Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x

May 2017

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

Text Part Number: OL-26137-01
CONTENTS

Preface ix
Overview of Cisco Identity Services Engine ix
Purpose x
Audience xi
Document Organization xi
Installation Reference xii
Document Conventions xii
Related Documentation xiii
Release-Specific Documents xiii
Platform-Specific Documents xiv
Documentation Updates xiv
Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1
Before Deploying Cisco ISE 1-1
  Understanding Node Types, Personas, Roles, and Services 1-1
  Cisco ISE Deployment Terminology 1-2
  Types of Nodes 1-2
  Understanding Distributed Deployment 1-4
  Guidelines for Setting Up a Distributed Deployment 1-7
  Cisco ISE Architecture Overview 1-8
Deployment Scenarios 1-9
  Small Cisco ISE Network Deployments 1-9
  Medium Cisco ISE Network Deployments 1-11
  Large Cisco ISE Network Deployments 1-12
Deployment Sizing and Scaling Recommendations 1-14
  Physical Appliance Sizing Recommendations 1-15
  VMware Appliance Sizing Recommendations 1-16
Configuration of a Cisco ISE Node 1-17
  Primary Node 1-17
  Secondary Node 1-17
  Logging Server 1-18
Switch Configurations Required to Support Cisco ISE Functions 1-18
Planning an Inline Posture Deployment 1-18
  Inline Posture Planning Considerations 1-19
CHAPTER 2  Cisco ISE Series Appliances  2-1
Cisco ISE 3300 Series Appliance Hardware Summary  2-1
Cisco ISE 3315 Serial Number Location  2-5
Cisco ISE 3315 Front and Rear Panels  2-5
Cisco ISE 3355 Serial Number Location  2-8
Cisco ISE 3355 Front and Rear Panels  2-8
Cisco ISE 3395 Serial Number Location  2-12
Cisco ISE 3395 Front and Rear Panels  2-12
Cisco SNS-3400 Series Appliance Hardware Summary  2-15
Cisco ISE SNS 3415/3495 Front and Rear Panels  2-16

CHAPTER 3  Before Configuring a Cisco ISE Series Appliance  3-1
Admin Rights Differences: CLI-Admin and Web-Based Admin Users  3-2
Understanding the Setup Program Parameters  3-3
Configuring a Cisco ISE 3300 Series Hardware Appliance  3-6
Downloading the Cisco ISE ISO Image  3-10
Cisco Integrated Management Interface  3-11
Configuring Cisco ISE on the Cisco SNS-3400 Series Appliance Using CIMC  3-11
Verifying the Configuration Process  3-17

CHAPTER 4  Virtual Machine Requirements  4-1
Disk Space Requirements  4-2
Evaluating the Cisco ISE Release 1.1.x  4-3
Configuring a VMware ESX or ESXi Server  4-4
Creating New Virtual File Size  4-5
Configuring VMware Server Interfaces for the Cisco ISE Profiler Service  4-6
Configuring the VMware Server  4-7
Preparing a VMware System for Cisco ISE Software Installation  4-14
Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD  4-14
Installing the Cisco ISE Software on a VMware System  4-16
Connecting to the Cisco ISE VMware Server Using Serial Console  4-17

CHAPTER 5  Installing a License  5-1
Types of Licenses  5-3
Obtaining a License  5-6
Autoinstallation of the Evaluation License  5-7
Accessing Cisco ISE Using a Web Browser  5-7
Contents

Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x

5-8
Logging In

5-9
Logging Out

5-10
Verifying the Cisco ISE Configuration

5-10
Verifying the Configuration Using a Web Browser

5-11
Verifying the Configuration Using the CLI

5-12
Verifying the Installation of VMware Tools

5-13
Upgrading VMware Tools

5-14
Resetting the Administrator Password

5-14
Lost, Forgotten, or Compromised Password

5-15
Password Negated Due to Administrator Lockout

5-16
Changing the IP Address of a Cisco ISE 3300 Series Appliance

5-16
Reimaging a Cisco ISE 3300 Series Appliance

5-17
Configuring the Cisco ISE System

5-18
Enabling System Diagnostic Reports in Cisco ISE

5-18
Installing New Cisco ISE Software

5-18
Configuring Certificates for Inline Posture Nodes

APPENDIX A
Preparing to Install the Cisco ISE 3300 Series Hardware

A-1
Safety Guidelines

A-1
General Precautions

A-3
Safety with Equipment

A-3
Safety with Electricity

A-5
Preventing ESD Damage

A-5
Lifting Guidelines

A-6
Preparing Your Site for Installation

A-6
Site Planning

A-11
Unpacking and Checking the Contents of Your Shipment

A-13
Required Tools and Equipment

A-14
Installation Checklist

A-14
Creating a Site Log

A-15
Ethernet Connector and Console Port Guidelines

APPENDIX B
Preparing to Install the Cisco SNS-3400 Series Hardware

B-1
Unpacking and Inspecting the Server

B-2
Safety Guidelines

B-3
Installing the Cisco SNS-3400 Series Appliance in a Rack

B-4
Rack Requirements

B-4
Equipment Requirements
Slide Rail Adjustment Range  B-4
Installing the Server In a Rack  B-4

CHAPTER C

Installing the Cisco ISE 3300 Series Hardware  C-1
Rack-Mounting Configuration Guidelines  C-1
Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack  C-2
Using a Four-Post Rack-Mount Hardware Kit  C-3
Installing the Slide Rails in a Rack  C-4
Installing the Appliance into the Slide Rails  C-6
Connecting Cables  C-8
Connecting the Network Interface  C-10
Connecting the Console  C-11
Connecting the Keyboard and Video Monitor  C-13
Cable Management  C-14
Powering Up the Cisco ISE 3300 Series Appliance  C-14
Power-Up Checklist  C-14
Power-Up Procedure  C-15
Checking the LEDs  C-16

CHAPTER D

Installing the Cisco SNS-3400 Series Hardware  D-1
Connecting and Powering On the Server  D-1
Checking the LEDs  D-2
Front Panel LEDs and Buttons  D-2
Rear Panel LEDs and Buttons  D-4
Configuring CIMC  D-4
Creating a Bootable USB Drive  D-6
Installing or Replacing Server Components  D-7

APPENDIX E

Maintaining the Cisco ISE 3300 Series Appliance  E-1
Maintaining Your Site Environment and Appliance  E-1
General Exterior Cleaning and Inspection  E-2
Cooling  E-3
Temperature  E-3
Humidity  E-4
Altitude  E-4
ESD  E-4
EMI and RFI  E-4
Magnetism  E-5
Power Source Interruptions  E-5
Maintaining Your Cisco ISE 3300 Series Appliance  E-6
Preparing to Transport the Rack Cabinet  E-6
Removing or Replacing the Cisco ISE 3300 Series Appliance  E-7

APPENDIX F  
Cisco SNS-3400 Series Server Specifications  F-1
Physical Specifications  F-1
Environmental Specifications  F-1
Power Specifications  F-2
450W Power Supply  F-2
650W Power Supply  F-2

APPENDIX G  
Troubleshooting the Cisco ISE Appliance  G-1
Troubleshooting Overview  G-1
Problem Solving  G-2
Troubleshooting the Power and Cooling Systems  G-3
Troubleshooting Adapter Cards, Cables, and Connections  G-4
Reading the LEDs  G-5
Front-Panel LEDs  G-5
Rear-Panel LEDs  G-5
Locating Appliance Serial Numbers  G-5

APPENDIX H  
Cisco ISE Appliance Ports Reference  H-1

APPENDIX I  
Installing Cisco ISE on Cisco NAC and Cisco Secure ACS Appliances  I-1
Installing Cisco ISE Software on a Reimaged Cisco Secure ACS Appliance  I-2
Installing Cisco ISE Software on a Reimaged Cisco NAC Appliance  I-2
Resetting the Existing RAID Configuration on a Cisco NAC Appliance  I-3

INDEX
Preface

Revised: May 2017, OL-26137-01

This preface provides the following information about the Cisco Identity Services Engine (ISE) 3300 Series appliance:

- **Overview of Cisco Identity Services Engine**, page 1
- **Purpose**, page 2
- **Audience**, page 3
- **Document Organization**, page 3
- **Document Conventions**, page 4
- **Related Documentation**, page 5
- **Documentation Updates**, page 6
- **Obtaining Documentation and Submitting a Service Request**, page 7

Overview of Cisco Identity Services Engine

Cisco Identity Services Engine (ISE), as a next-generation identity and access control policy platform enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE's unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices in order to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches.

Cisco ISE is a key component of the Cisco Security Group Access Solution. Cisco ISE is a consolidated policy-based access control solution that:

- Combines authentication, authorization, accounting (AAA), posture, profiler, and guest management services into one appliance
- Enforces endpoint compliance by checking the device posture of all endpoints accessing the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments allowing services to be delivered where they are needed
• Employs advanced enforcement capabilities including Security Group Access (SGA) through the use of Security Group Tags (SGTs) and Security Group (SG) Access Control Lists (ACLs)
• Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

The Cisco ISE software comes preinstalled on a range of physical appliances with various performance characterizations. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed. The Cisco ISE architecture supports standalone and distributed deployments, along with high-availability options. Cisco ISE allows you to configure and manage your network from a centralized portal for efficiency and ease of use.

Cisco ISE also incorporates distinct configurable roles and services, so that you can create and apply Cisco ISE services where they are needed in the network. The result being a comprehensive Cisco ISE deployment that operates as an fully functional and integrated system.

Purpose

This installation guide provides the following types of information about the Cisco ISE Release 1.1.x:
• Prerequisites for installation
• Procedures for installing the Cisco ISE software on a supported Cisco ISE appliance
• Procedures for installing the Cisco ISE software on a supported VMware virtual machine
• Procedures for installing the Cisco ISE software on a supported Cisco Network Admission Control (NAC) Appliance or Cisco Secure Access Control System (ACS) Appliance

Cisco ISE Release 1.1.x offers a choice of five appliance platforms, depending upon the size of your deployment:
• Small network—Cisco ISE 3315 and Cisco SNS 3415
• Medium network—Cisco ISE 3355, Cisco SNS 3415, and Cisco SNS 3495
• Large network—Cisco ISE 3395, Cisco SNS 3415, and Cisco SNS 3495

Note You can install the Cisco ISE version 1.1.4 on the Cisco SNS-3400 Series appliances and on any platform that is supported in the Cisco ISE Release 1.1.3.

The Cisco ISE software runs on the Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS). The Cisco ADE-OS and Cisco ISE software run on a dedicated Cisco ISE 3300 Series appliance, a dedicated Cisco SNS-3400 Series appliance, or on a VMware server (Cisco ISE VM).

For VMware-based installations, configure the VMware environment to meet a specific set of minimal system requirements and install the Cisco ISE Release 1.1.x software. The supported VMware versions include the following:
• VMware Elastic Sky X (ESX), version 4.0, 4.0.1, and 4.1
• VMware ESXi, version 4.0, 4.0.1, and 4.1
• VMware ESX 5.x

Note For more information about VMware-based installations, see Chapter 1, “Installing Cisco ISE in a VMware Virtual Machine”.
Note
VMware server, version 2.0, is only supported only for demonstrating the features of Cisco ISE Release 1.1.x, and is not supported for production environments.

Audience
This guide is designed for network administrators, system integrators, or network deployment personnel who install and configure the Cisco ISE software on Cisco ISE 3300 Series appliances or on VMware servers. As a prerequisite to using this hardware installation guide, you should be familiar with networking equipment and cabling and have a basic knowledge of electronic circuitry, wiring practices, and equipment rack installations.

Warning
Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Document Organization
Table 1 lists the organization of the Cisco ISE Hardware Installation Guide, Release 1.1.x.

Table 1 Cisco ISE Hardware Installation Guide Organization

<table>
<thead>
<tr>
<th>Chapter/Appendix and Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Understanding the Cisco ISE Network Deployment”</td>
<td>Provides an overview of the Cisco ISE 3300 Series appliance deployments and their components. Read this chapter before planning a new Cisco ISE 3300 Series deployment.</td>
</tr>
<tr>
<td>Chapter 1, “Introducing the Cisco ISE Hardware”</td>
<td>Provides an overview of the Cisco ISE 3300 Series hardware.</td>
</tr>
<tr>
<td>Chapter 1, “Configuring the Cisco ISE Appliances”</td>
<td>Describes how to perform an initial installation of the Cisco ISE software on the Cisco ISE 3300 Series hardware.</td>
</tr>
<tr>
<td>Chapter 1, “Installing Cisco ISE in a VMware Virtual Machine”</td>
<td>Describes how to install Cisco ISE software on the VMware ESX or ESXi virtual machines.</td>
</tr>
<tr>
<td>Chapter 1, “Performing Post-Installation Tasks”</td>
<td>Provides information on installing a Cisco ISE 3300 Series license and lists the configuration tasks that you need to perform following installation.</td>
</tr>
<tr>
<td>Appendix 1, “Preparing to Install the Cisco ISE 3300 Series Hardware”</td>
<td>Describes the necessary safety instructions, site requirements, and tasks that you need to perform before installing the Cisco ISE 3300 Series hardware.</td>
</tr>
<tr>
<td>Appendix 1, “Preparing to Install the Cisco SNS-3400 Series Hardware”</td>
<td>Describes the safety guidelines, site requirements, and guidelines that you must observe before installing the Cisco SNS-3400 Series appliances.</td>
</tr>
<tr>
<td>Appendix 1, “Installing the Cisco ISE 3300 Series Hardware”</td>
<td>Provides detailed instructions on performing the rack-mounting of a Cisco ISE 3300 Series appliance, connecting all cables, powering up the appliance, and removing or replacing the appliance.</td>
</tr>
</tbody>
</table>
Table 1  Cisco ISE Hardware Installation Guide Organization (continued)

<table>
<thead>
<tr>
<th>Chapter/Appendix and Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1, “Installing the Cisco SNS-3400 Series Hardware”</td>
<td>Describes how to install your Cisco SNS-3400 Series appliances and connect any of the supported appliances to the network.</td>
</tr>
<tr>
<td>Appendix 1, “Maintaining the Cisco ISE 3300 Series Appliance”</td>
<td>Provides recommendations for maintaining the Cisco ISE 3300 Series appliance following installation.</td>
</tr>
<tr>
<td>Appendix 1, “Cisco SNS-3400 Series Server Specifications”</td>
<td>Describes the technical specifications for the Cisco SNS-3400 Series server.</td>
</tr>
<tr>
<td>Appendix 1, “Troubleshooting the Cisco ISE Appliance”</td>
<td>Provides techniques for troubleshooting the initial start up of a Cisco ISE 3300 Series appliance.</td>
</tr>
<tr>
<td>Appendix A, “Cisco ISE Appliance Ports Reference”</td>
<td>Provides a reference list of ports that are used by the Cisco ISE 3300 Series appliance services, applications, and devices.</td>
</tr>
<tr>
<td>Appendix 1, “Installing Cisco ISE on Cisco NAC and Cisco Secure ACS Appliances”</td>
<td>Describes how to install Cisco ISE software on a supported Cisco NAC appliance or a Cisco Secure ACS Appliance.</td>
</tr>
</tbody>
</table>

Installation Reference

Table 2 lists reference material that may be useful to review before attempting to install the Cisco ISE 3300 Series Release 1.1.x software. For each of the installation processes, see the corresponding chapter, appendix, or guide.

Table 2  Cisco ISE 3300 Series Installation Scenarios

<table>
<thead>
<tr>
<th>Installation Process</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Introducing the Cisco ISE appliance and predeployment requirements | 1. Chapter 1, “Introducing the Cisco ISE Hardware”  
2. Appendix 1, “Preparing to Install the Cisco ISE 3300 Series Hardware” |
| Installing the initial Cisco ISE appliance and configuring the Cisco ISE software | 1. Appendix 1, “Installing the Cisco ISE 3300 Series Hardware”  
2. Chapter 1, “Configuring the Cisco ISE Appliances” |
| Installing the initial Cisco ISE software on the VMware server | 1. Chapter 1, “Installing Cisco ISE in a VMware Virtual Machine” |
| Licensing and using the web interface to log in | 1. Chapter 1, “Performing Post-Installation Tasks” |
| Installing Cisco ISE software on a Cisco NAC Appliance or on a Cisco Secure ACS Appliance | 1. Appendix 1, “Installing Cisco ISE on Cisco NAC and Cisco Secure ACS Appliances” |

Document Conventions

This guide uses the following conventions to convey instructions and information.
Note Means reader take note. Notes contain helpful suggestions or references to material that is not covered in this guide.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Release-Specific Documents


Table 3  Product Documentation for Cisco Identity Services Engine

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Location</th>
</tr>
</thead>
</table>
Table 3  Product Documentation for Cisco Identity Services Engine (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Location</th>
</tr>
</thead>
</table>

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco ISE
- Cisco Secure ACS
- Cisco NAC Appliance
- Cisco NAC Profiler
- Cisco NAC Guest Server

Documentation Updates

Table 4 lists the documentation updates for this Cisco ISE product release.
Table 4  Updates for Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/29/2013</td>
<td>Resolved CSCui72606</td>
</tr>
<tr>
<td>9/3/13</td>
<td>Resolved CSCui97432</td>
</tr>
<tr>
<td>4/25/13</td>
<td>Cisco Identity Services Engine, Release 1.1.4</td>
</tr>
<tr>
<td>2/28/13</td>
<td>Cisco Identity Services Engine, Release 1.1.3</td>
</tr>
<tr>
<td>10/31/13</td>
<td>Cisco Identity Services Engine, Release 1.1.2</td>
</tr>
<tr>
<td>1/31/13</td>
<td>Resolved CSCue27909</td>
</tr>
<tr>
<td>8/31/12</td>
<td>Resolved CSCua12292</td>
</tr>
<tr>
<td>7/10/12</td>
<td>Cisco Identity Services Engine, Release 1.1.1</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop by using a reader application. The RSS feeds are a free service, and Cisco currently supports RSS Version 2.0.
Understanding the Cisco ISE Network Deployment

This chapter provides information on how to deploy the Cisco Identity Services Engine (ISE) 3300 Series appliance and its related components, the Cisco SNS-3400 Series appliance and its related components, several network deployment scenarios, and describes the switch configurations that are needed to support Cisco ISE. This chapter contains the following topics:

- Before Deploying Cisco ISE, page 1-1
- Deployment Scenarios, page 1-9
- Deployment Sizing and Scaling Recommendations, page 1-14
- Configuration of a Cisco ISE Node, page 1-17
- Switch Configurations Required to Support Cisco ISE Functions, page 1-18
- Planning an Inline Posture Deployment, page 1-18

Before Deploying Cisco ISE

This section provides the following reference information that aids you in better understanding what is needed before you deploy the Cisco ISE appliances in your network environment:

- Understanding Node Types, Personas, Roles, and Services, page 1-1
- Types of Nodes, page 1-2
- Understanding Distributed Deployment, page 1-4
- Guidelines for Setting Up a Distributed Deployment, page 1-7
- Cisco ISE Architecture Overview, page 1-8

Understanding Node Types, Personas, Roles, and Services

Cisco ISE provides a highly available and scalable architecture that supports both standalone and distributed deployments. In a distributed environment, you configure one primary Administration ISE node and the rest are secondary nodes. The topics in this section provide information about Cisco ISE terminology, supported node types, distributed deployment, and the basic architecture.
Cisco ISE Deployment Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, and monitoring.</td>
</tr>
<tr>
<td>Node</td>
<td>A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on a</td>
</tr>
<tr>
<td></td>
<td>VMware server. Each instance (either running on a Cisco ISE appliance or on a VMware server) that runs the Cisco ISE software is called a node.</td>
</tr>
<tr>
<td>Node type</td>
<td>A node can be of two types: ISE node and Inline Posture node. The node type and persona determine the type of functionality provided by that node.</td>
</tr>
<tr>
<td>Persona</td>
<td>The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration,</td>
</tr>
<tr>
<td></td>
<td>Policy Service, and Monitoring.</td>
</tr>
<tr>
<td>Role</td>
<td>Determines if a node is a standalone, primary, or secondary node. Applies only to Administration ISE and Monitoring ISE nodes.</td>
</tr>
<tr>
<td>Node groups</td>
<td>Multiple Policy Service ISE nodes that are located behind a load balancer to distribute the requests evenly. To detect node failure and to reset sessions</td>
</tr>
<tr>
<td></td>
<td>in pending state on the failed node, two or more Policy Service ISE nodes can be placed in the same node group.</td>
</tr>
</tbody>
</table>

Types of Nodes

A Cisco ISE network has only two types of nodes:

- ISE node—An ISE node could assume any of the following three personas:
  - Administration—Allows you to perform all administrative operations on ISE. It handles all system-related configuration and configurations related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the Administration persona. The Administration persona can take on any one of the following roles: standalone, primary, or secondary. If the primary Administration ISE node goes down, then you must manually promote the secondary Administration ISE node. There is no automatic failover for the Administration persona.

  Note: At least one node in your distributed setup should assume the Administration persona.

  - Policy Service—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 assuming this persona. Typically, there would be more than one Policy Service persona in a distributed deployment. All Policy Service ISE nodes that reside behind a load balancer share a common multicast address and 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 pending sessions.
Before Deploying Cisco ISE

To promote device status replication and network profiling efficiency among Policy Service ISE nodes, Cisco recommends installing multiple Policy Service ISE nodes within local area network segments tangent to the Administrative ISE node, and avoid relying on wide-area network connections between Policy Service ISE nodes as much as possible.

Note

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

- Monitoring—Enables ISE to function as the log collector and store log messages from all the Administration and Policy Service personas on the ISE nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources.

A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring personas collect log messages. In case the primary Monitoring persona goes down, the secondary Monitoring persona automatically assumes the role of the primary Monitoring persona.

Note

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

- Inline Posture node—A gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLCs) and virtual private network (VPN) concentrators on the network. Inline Posture enforces access policies after a user has been authenticated and granted access, and handles Change of Authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows up to 10,000 Inline Posture nodes in a deployment. You can pair two Inline Posture nodes together for high availability as a failover pair.

An Inline Posture node is dedicated solely to that service, and cannot operate concurrently with other ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. Inline Posture nodes are not supported on VMware server systems.

Note

Inline Posture is not supported on the SNS 3495 platform. Ensure that you install Inline Posture on any one of the following supported platforms: ISE 3315, ISE 3355, ISE 3395, or SNS 3415.

Note

Each ISE node in a deployment can assume more than one of the three personas (Administration, Policy Service, or Monitoring) at a time. By contrast, each Inline Posture node operates only in a dedicated gatekeeping role.

In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration ISE nodes
- Primary and secondary Monitoring ISE nodes
- One or more Policy Service ISE nodes
- One or more Inline Posture nodes
Chapter 1      Understanding the Cisco ISE Network Deployment

Understanding Distributed Deployment

An ISE distributed deployment consists of one primary Administration ISE node and multiple secondary nodes. Each ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring.

Note
The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node. Inline Posture nodes are not supported on VMware server systems. For more information, see the Cisco Identity Services Engine User Guide, Release 1.1.x.

After you install ISE on all your nodes as described in this guide, the nodes come up in a standalone state. You must then define one node to be your primary Administration ISE node. After defining a primary Administration ISE node, you can choose to configure other personas on that node, such as Policy Service or Monitoring. After you define personas on the primary Administration ISE node, you can register other secondary nodes with the primary Administration ISE node and then define personas for the secondary nodes.

When you register an ISE node as a secondary node, ISE immediately creates a database link from the primary to the secondary node and begins the process of replicating or sharing ISE configuration data from the primary to the secondary nodes. This process ensures consistency between the configuration data that is present in all the ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. An incremental replication occurs after a full replication, and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the primary Administration ISE node are reflected in the secondary nodes. The process of replication ensures that all ISE nodes in a deployment are in sync. You can view the status of replication from the deployment pages of the ISE administrative user interface.

The Policy Service ISE nodes that reside in a single location behind a load balancer and share a common multicast address can be grouped together. In such scenarios, you can define node groups and assign the nodes to the particular group.

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary Administration ISE node, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered secondary node.

Note
You cannot deregister a primary Administration ISE node.

Note
You can detain the primary node as standalone from the Deployment page. Edit the primary node and click Make Standalone. You can do this only after deregistering all the secondary nodes in the deployment.

The application server in an ISE node restarts when you make any of the following changes:

- Register a node (standalone to secondary)
- Deregister a node (secondary to standalone)
- Primary node is changed to standalone (if no other nodes are registered with it; primary to standalone)
• Administration ISE node is promoted (secondary to primary)
• Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
• Modify the services in the Policy Service ISE node (enable or disable the session and profiler services)
• Restore a backup on the primary and a sync up operation is triggered to replicate data from the primary to secondary nodes

Note
For example, if your deployment has two nodes and you deregister the secondary node, both nodes in this primary-secondary pair are restarted. (The former primary and secondary nodes become standalone.)

Note
When you make any of these changes, the application services are restarted. You must expect a delay while these services restart.

Note
You can have only one primary node in your deployment. The other Cisco ISE nodes are secondary nodes that can be configured for one or more of the roles previously described. When the primary node is lost, you must promote one of the secondary nodes to become the primary. Cisco ISE supports the promotion of any secondary appliance to serve as the primary node.

When the Cisco ISE installation has been completed, you must configure one of your Cisco ISE instances as the primary node. You can edit the primary node and enable any service that you want to run on the primary.

Before Registering Secondary Nodes

Prerequisites:
• The fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, ise1.cisco.com must be Domain Name System (DNS)-resolvable from the primary Administration ISE node. Otherwise, node registration will fail. You must enter the IP addresses and FQDNs of the ISE nodes that are part of your distributed deployment in the DNS server.
• The primary Administration ISE node and the standalone node that you are about to register as a secondary node should be running the same version of Cisco ISE.
• Use the username and password that were created during the initial setup or the password if it was changed later.
• Database passwords of the primary and secondary nodes should be the same. If they are set differently during node installation, you can modify them by using the following commands:
  – application reset-passwd ise internal-database-admin
  – application reset-passwd ise internal-database-user
See the Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x for more details on how to use the CLI commands.
• You can alternatively create an administrator account on the node that is to be registered and use those credentials for registering that node. Every ISE administrator account is assigned one or more administrative roles. To register and configure a secondary node, you must have one of the following
roles assigned: Super Admin, System Admin, or RBAC Admin. See “Cisco ISE Admin Group Roles and Responsibilities” in Chapter 4 of theCisco Identity Services Engine User Guide, Release 1.1.x, for more information on the various administrative roles and the privileges that are associated with each of them.

- If you plan to register a secondary Administration ISE node for high availability, we recommend that you register the secondary Administration ISE node with the primary first before you register other Cisco ISE nodes. If Cisco ISE nodes are registered in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration ISE node as your primary.

- If you plan to register multiple Policy Service ISE nodes running Session services and you require mutual failover among those nodes, you must place the Policy Service ISE nodes in a node group. You must create the node group first before you register the nodes because you need to select the node group to be used on the registration page. See “Creating, Editing, and Deleting Node Groups” in Chapter 9 of theCisco Identity Services Engine User Guide, Release 1.1.x, for more information.

- Ensure that the Certificate Trust List (CTL) of the primary node is populated with the appropriate Certificate Authority (CA) certificates that can be used to validate the HTTPS certificate of the standalone node (that you are going to register as the secondary node). See “Creating Certificate Trust Lists in the Primary Cisco ISE Node” in Chapter 12 of theCisco Identity Services Engine User Guide, Release 1.1.x, for more information.

- After registering your secondary node to the primary node, if you change the HTTPS certificate on the registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node’s HTTPS certificate and import it to the CTL of the primary node. See “Creating Certificate Trust Lists in the Primary Cisco ISE Node” in Chapter 12 of theCisco Identity Services Engine User Guide, Release 1.1.x, for more information.

---

**Note**

We recommend that you set all Cisco ISE nodes to the UTC time zone. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

You can register the secondary nodes and edit their configuration profiles by using the user interface of the primary node. After you install a secondary node, Cisco ISE immediately creates a database link between the primary and the secondary node for replicating and synchronizing all changes. In addition, you can remove a node from the deployment by deregistering it. This action deletes it from the deployment.

When you deregister a node from the primary, the status of the deregistered node changes to standalone. Any connection between the primary and the secondary nodes is lost, no replication updates are sent to the secondary node.

**Next Steps:**

For more information on configuring Cisco ISE nodes, see:

- *Cisco Identity Services Engine User Guide, Release 1.1.x*
  - Chapter 9, “Setting Up ISE in a Distributed Environment” and “Registering and Configuring a Secondary Node”
Guidelines for Setting Up a Distributed Deployment

Observe the following guidelines before you attempt to set up Cisco ISE appliances in a distributed deployment:

- You must have a properly configured, working DNS for a distributed deployment to work correctly.
- Configure the Reverse DNS lookup for all Cisco ISE nodes in your distributed deployment in the DNS server. Otherwise, you may run into deployment related issues when registering Cisco ISE nodes, and restarting Cisco ISE nodes.
- A Cisco ISE node can run any of the ISE node personas at the same time.
- A Cisco ISE node can be designated to perform as a standalone node, or as either a primary or a secondary node in a primary-secondary pair, depending upon configuration and settings.
- You can have only one primary Cisco ISE node in your deployment.

**Note** Other Cisco ISE nodes are considered to be secondary nodes that can be configured for one or more other roles depending upon licenses and settings. When the primary node is lost, you need to promote a valid secondary node to become the primary. Cisco ISE only supports the promotion of a secondary node appliance with the Administration persona to serve as the “new” primary node. In addition, it must possess a valid license as a secondary node with an Administration persona.

- The primary Cisco ISE node must run the Administration persona.
- All Cisco ISE system-related configuration and configuration that is related to functionality should be made only on the primary Cisco ISE node.
- The configuration changes that you perform on the primary node are replicated to all the secondary nodes in your deployment.
- The Inline Posture node requires a dedicated Cisco ISE node. No other service can run on a node that is designated as an Inline Posture node.

**Note** The Inline Posture node is not supported on VMware server systems.

- To avoid time zone issues among the nodes, you must provide the same NTP server name during the setup mode of each node.

When the Cisco ISE installation is complete, you must configure one of your Cisco ISE nodes as the primary node. You can edit the primary node and enable any service that you want to run on the primary. You can register secondary nodes and edit their configuration by using the user interface of the primary node. After you install a secondary node, Cisco ISE immediately creates a database link between the primary and secondary nodes for replicating and synchronizing all changes.

When you deregister a node from the primary, the status of the deregistered node changes to standalone. To register a deregistered node back with the primary, you must first reset the database configuration on the node and bring it back to a freshly installed node state and then register it again.

For more information:

See the *Cisco Identity Services Engine User Guide, Release 1.1.x* for more information about:

- Cisco ISE Admin group roles and responsibilities
• Cisco ISE node services
• Resetting the configuration of a node

Cisco ISE Architecture Overview

Figure 1-1 illustrates a basic overview of the Cisco ISE architecture that includes the following components:

• Nodes and persona types
  – ISE node—Administration, Policy Service, Monitoring
  – Inline Posture node—Gatekeeping and access policy enforcer
• Network resources
• Endpoints

Note

Figure 1-1 shows ISE nodes and persona types (Administration, Policy Service, and Monitoring), an Inline Posture node, and a policy information point.

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.
Deployment Scenarios

This section describes three scenarios in which Cisco ISE can be deployed in a distributed deployment:

- Small Cisco ISE Network Deployments, page 1-9
- Medium Cisco ISE Network Deployments, page 1-11
- Large Cisco ISE Network Deployments, page 1-12

Small Cisco ISE Network Deployments

The smallest Cisco ISE deployment consists of two Cisco ISE nodes as shown in Figure 1-2, with one Cisco ISE node functioning as the primary appliance in a small network.

Note

Concurrent endpoints represent the total number of supported users and devices. This can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

The primary node provides all the configuration, authentication, and policy capabilities that are required for this network model, while 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 secondary network appliances, network resources, or RADIUS.
RADIUS is where the centralized AAA operations are performed between clients and the primary Cisco ISE node. As a result, the key requirement is to ensure that you can synchronize or replicate all of the content that resides on the primary Cisco ISE node with the secondary Cisco ISE node(s).

Being able to synchronize between the primary and secondary node makes it possible to keep the secondary node 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 node on all RADIUS clients by using this type of deployment or a similar approach.

**Figure 1-2  Small Cisco ISE Network Deployment**

![Small Cisco ISE Network Deployment Diagram](image)

As the number of devices, network resources, users, and AAA clients increases in your network environment, we recommend that you change your deployment configuration from the basic small model and use more of a split or distributed deployment model, as shown in Figure 1-3.

**Note**

Figure 1-2 shows the secondary Cisco ISE node acting as a Policy Service persona performing AAA functions. The secondary Cisco ISE node could also be acting as a Monitoring or Administration persona.

**Split Cisco ISE Deployments**

In the case of split Cisco ISE deployments, you will continue to maintain primary and secondary nodes as described in the small Cisco ISE deployment. However, the AAA load is split between these 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. When running under normal network operations, neither the primary or secondary node carries the full load of handling AAA requests 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 also provides better loading while still maintaining the functional status of the secondary node during the course of normal network operations.
Another advantage is that 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. Figure 1-3 shows the secondary Cisco ISE node in this role.

**Figure 1-3  Split Cisco ISE Network Deployment**

In addition, the split Cisco ISE node deployment design provides an advantage because it also allows for growth, as shown in Figure 1-4.

**Medium Cisco ISE Network Deployments**

As small, local networks grow, you can keep pace and manage network growth by adding additional Cisco ISE nodes to create a medium-sized network. In medium network deployments, consider promoting one Cisco ISE node to perform as the primary to handle all the configuration services, and secondary Cisco ISE nodes to manage all your AAA functions.

As the amount of log traffic increases in the network, you can choose to either use the primary Cisco ISE node as your centralized log collector or dedicate one of the secondary Cisco ISE nodes to serve in this capacity for your network.
Figure 1-4  Medium Cisco ISE Network Deployment

Large Cisco ISE Network Deployments

We recommend that you use centralized logging (as shown in Figure 1-5) for larger Cisco ISE networks. To use centralized logging, you must 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. See Understanding the Setup Program Parameters, page 1-3 when configuring the Cisco ISE software to support a dedicated logging server.

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.

In large centralized networks, you should use a load balancer (as shown in Figure 1-5), 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 Cisco ISE 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 or distant locations.

To optimize AAA performance, each remote site should have its own AAA infrastructure (as shown in Figure 1-6). 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.
Some factors to consider when planning a network that has several remote sites include the following:

- Verify if a central or external database is used, such as Microsoft Active Directory or LDAP. For optimizing the process, each remote site should have a synchronized instance of the external database that is available for Cisco ISE to access.
- Locating the AAA clients is important. You should locate your 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.
- DNS should be properly configured on all Cisco ISE nodes to ensure access to the external databases.

**Deployment Sizing and Scaling Recommendations**

This section provides guidance on the size of the physical and virtual machine appliances that you would need for your deployment based on the number of endpoints that connect to your network. This section contains the following topics:

- Physical Appliance Sizing Recommendations, page 1-15
• VMware Appliance Sizing Recommendations, page 1-16

Physical Appliance Sizing Recommendations

Table 1-2 provides guidance on the type of deployment, number of Cisco ISE nodes, and the type of appliance (small, medium, large) that you need based on the number of endpoints that connect to your network.

Table 1-2  Cisco ISE Deployment—Sizing and Scaling Recommendations

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Number of Nodes/Personas</th>
<th>Appliance</th>
<th>Number of Active Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Standalone or 2 nodes</td>
<td>ISE-3315/ISE-3355/ISE-3395/SNS-3415/SNS-3495</td>
<td>Maximum of 2000 endpoints for the entire deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The Cisco SNS-3400 Series hardware is supported only on ISE 1.1.4.</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>• Administration and Monitoring personas colocated on single or redundant nodes. Maximum of 2 Administration and Monitoring nodes. • Dedicated Policy Service nodes. Maximum of 5 Policy Service nodes.</td>
<td>ISE-3355/SNS-3415/SNS-3495 appliances for Administration and Monitoring personas</td>
<td>Maximum of 5000 endpoints</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISE-3395/SNS-3415/SNS-3495 appliances for Administration and Monitoring personas</td>
<td>Maximum of 10000 endpoints</td>
</tr>
<tr>
<td>Large</td>
<td>• Dedicated Administration node/nodes. Maximum of 2 Administration nodes. • Dedicated Monitoring node/nodes. Maximum of 2 Monitoring nodes. • Dedicated Policy Service nodes. Maximum of 36 Policy Service nodes.</td>
<td>ISE-3395 or SNS 3495 appliances for Administration and Monitoring personas</td>
<td>Maximum of 100,000 endpoints</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The SNS-3400 Series hardware is supported only on ISE 1.1.4.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-3 provides guidance on the type of appliance needed for a dedicated Policy Service node based on the number of active endpoints the node services.
Chapter 1  Understanding the Cisco ISE Network Deployment

Table 1-3  Policy Service Node Sizing Recommendations

<table>
<thead>
<tr>
<th>Form Factor</th>
<th>Platform Size</th>
<th>Appliance</th>
<th>Maximum Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Small</td>
<td>ISE-3315</td>
<td>3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNS-3415</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>ISE-3355</td>
<td>6000</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>ISE-3395</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNS-3495</td>
<td></td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Small/Medium/Large</td>
<td>Comparable to Physical Appliance</td>
<td>3000 to 10,000</td>
</tr>
</tbody>
</table>

Table 1-4 provides the maximum throughput and the maximum number of endpoints that a single Inline Posture node can support.

Table 1-4  Inline Posture Node Sizing Recommendations

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of endpoints per any physical appliance</td>
<td>3,000 to 10,000 (gated by Policy Service nodes)</td>
</tr>
<tr>
<td>Maximum throughput per any physical appliance</td>
<td>936 Mbps</td>
</tr>
</tbody>
</table>

VMware Appliance Sizing Recommendations

The VMware appliance specification should be comparable with the physical appliances. Table 1-5 lists the recommended VMware specification comparable to the physical appliances for a production environment.

Refer to “Minimum VMware Production Disk Space Requirements” to determine the total disk space needed for the various personas.

Table 1-5  VMware Appliance Specifications for a Production Environment

<table>
<thead>
<tr>
<th>Platform</th>
<th>NAC-3315</th>
<th>NAC-3355</th>
<th>NAC-3395</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor¹</td>
<td>Single QuadCore</td>
<td>Single QuadCore</td>
<td>2 x QuadCore</td>
</tr>
<tr>
<td></td>
<td>2.66 GHz</td>
<td>2.00 GHz</td>
<td>2.00 GHz</td>
</tr>
<tr>
<td></td>
<td>4 total cores</td>
<td>4 total cores</td>
<td>8 total cores</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Total Disk Space²</td>
<td>500 GB</td>
<td>600 GB</td>
<td>600 GB</td>
</tr>
<tr>
<td>Ethernet NICs³</td>
<td>4 x Integrated Gigabit NICs</td>
<td>4 x Integrated Gigabit NICs</td>
<td>4 x Integrated Gigabit NICs</td>
</tr>
</tbody>
</table>

¹. Virtual machine resources should be dedicated. The VM resources should not be shared or oversubscribed across multiple VMs.

². Policy Service nodes on virtual machines can be deployed with less disk space than Administration or Monitoring nodes. Recommendation is 100 to 200 GB disk space for Policy Service nodes.

³. Virtual machines can be configured with 1 to 4 NICs. A minimum of 1 NIC is required. Recommendation is to allow for 2 or more NICs. Additional interfaces can be used to support various services such as profiling or RADIUS. Refer to Appendix E, “Cisco ISE 3300 Series Appliance Ports Reference” for details about the services that are supported on each of the ports.
Configuration of a Cisco ISE Node

This section briefly describes the roles that various Cisco ISE appliances play in a network deployment and how to configure them:

- **Primary Node, page 1-17**
- **Secondary Node, page 1-17**
- **Logging Server, page 1-18**

See the “Setting Up Cisco ISE in a Distributed Environment” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x*, for more information on:

- Configuring a Cisco ISE Node
- Configuring Administration Cisco ISE Nodes for High Availability
- Viewing Nodes in a Deployment
- Managing Node Groups
- Changing Node Personas and Services
- Configuring Monitoring ISE Nodes for Automatic Failover
- Removing a Node from Deployment
- Replacing the Cisco ISE Appliance Hardware

All Cisco ISE appliances have a similar installation procedure. For specific details, see the following sections:

- Chapter 1, “Configuring the Cisco ISE Appliances,” for installing Cisco ISE software on the Cisco ISE 3300 Series appliance.
- Chapter 1, “Installing Cisco ISE in a VMware Virtual Machine,” for installing Cisco ISE software on a VMware ESX server.
- Appendix 1, “Installing the Cisco SNS-3400 Series Hardware,” for installing Cisco ISE software on the Cisco SNS-3400 Series appliance.

---

**Note**

For any Cisco ISE network deployment, your first hardware installation must be performed on the node that is designated as the primary node in your network.

---

**Primary Node**

In a Cisco ISE deployment, only one appliance can serve as a Cisco ISE primary node. This primary node provides configuration capabilities and is the source for all replication operations.

When in a primary-secondary pair, only the primary and secondary nodes that operate as the Administration persona need to be configured in the license file. When you install the license file on the primary, the license requirements for the secondary node are met.

**Secondary Node**

Because the network can only have a single primary Cisco ISE node, all other Cisco ISE nodes function as secondary nodes. Although the Cisco ISE secondary nodes receive all the system configurations from the primary node, you must configure the following on each secondary node:
License—When the base license is installed on the primary, replication copies the license onto each of the Cisco ISE secondary nodes in the deployment.

New local certificates—You can either configure the local certificates on the secondary nodes or import the local certificates from the primary node onto each secondary node.

Logging server—You can configure either the primary or the secondary node to serve as the dedicated logging server for your Cisco ISE network. We strongly recommend that you configure a secondary Cisco ISE node as the dedicated logging server.

In a primary-secondary node pair, the secondary node is registered and it begins to receive the full synchronization of the configuration and replication updates from the primary node in the network.

Logging Server

You can configure to use either a primary node or one of the secondary nodes as the dedicated logging server for your network. In this role, the logging server receives logs from the primary node and all the secondary nodes deployed in the Cisco ISE network. We recommend that you designate one of the Cisco ISE secondary nodes as the Monitoring persona and exclude this particular secondary node from any of the AAA activities. Three main logging categories are captured:

- Audit
- Accounting
- Diagnostics

For a complete description that provides more details on logging categories and best practices for configuring the logging server, see Chapter 13, “Logging” in the Cisco Identity Services Engine User Guide, Release 1.1.x.

Switch Configurations Required to Support Cisco ISE Functions

To ensure that Cisco ISE is able to interoperate with network switches, and functions from Cisco ISE are successful across the network segment, you must configure your network switches with certain required NTP, RADIUS/AAA, 802.1X, MAB, and other settings.

For more information:

- For more switch configuration requirements, see Appendix C, “Switch Configuration Required to Support Cisco ISE Functions” in the Cisco Identity Services Engine User Guide, Release 1.1.x.

Planning an Inline Posture Deployment

This section is only intended to provide a brief overview of what is needed to plan and deploy Inline Posture in a Cisco ISE network. It is the responsibility of your network or system architect to research the issues involved in Inline Posture deployment to determine what best suits your network needs and requirements.
Before you start any planning for deploying or configuring Inline Posture for your network, you must first understand what types of Inline Posture operating modes and deployment options are supported.

**Caution**
The Inline Posture node’s untrusted interface should be disconnected at the time the Inline Posture node is being configured. If the Inline Posture node’s trusted and untrusted interfaces are connected to the same VLAN during initial configuration, and the Inline Posture node initially boots up after changing its persona, multicast packet traffic gets flooded out of the untrusted interface. This multicast storm can potentially bring down devices that are connected to the same subnet or VLAN. The Inline Posture node at this time is in the maintenance mode.

For more details about Inline Posture operating modes, filters, managed subnets, and Inline Posture high availability as these topics correspond to the Cisco ISE network, see Chapter 10, “Setting Up an Inline Posture Node,” in the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

### Inline Posture Planning Considerations

This section poses some basic questions and considerations that must be addressed by your network or system architect when planning to deploy Inline Posture nodes. Ensure that you have understood the following planning and deployment issues prior to starting any Inline Posture node configuration in a distributed Cisco ISE network deployment:

- How do you plan to deploy your Inline Posture node?
- How will you deploy your Inline Posture node(s)?
- Will the Inline Posture node be run as a standalone node, or as part of a primary-secondary pair of Inline Posture nodes?

**Note**
Cisco ISE networks support up to two Inline Posture nodes configured on your network at any one time. If you plan to deploy an Inline Posture high-availability primary-secondary pair, then two Inline Posture nodes must be configured. In this mode, one node is designated as the primary and the other as the secondary node. The primary node assumes the primary role when both nodes come up at the same time.

- Will your deployment plans include an Inline Posture primary-secondary pair configuration? If so, be aware that all configuration related to functionality can only be done from the primary node of this pair (the Cisco ISE user interface only shows basic configuration tables for the secondary node in this configuration).
- Note that you can synchronize an Inline Posture primary node configuration with its peer secondary node using the Failover tab of the primary node in this Inline Posture pair. For more information, see Chapter 10, “Setting Up an Inline Posture Node,” in the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

The following topics in this section provide some basic information on Inline Posture nodes, but these topics are not intended to provide you with all the information needed to complete a comprehensive deployment plan for your network.
Choosing an Inline Posture Operating Mode

Which Inline Posture operating mode you choose largely depends on your existing network architecture. The choice you make limits many of the other configuration options you may want in your Cisco ISE deployment. Therefore, you need to fully understand each of the following primary Inline Posture operating modes:

- **Routed mode**—This mode acts as a Layer 3 “hop” in the network connections. The routed mode selectively forwards packets to specified addresses. The routed mode ensures it can segregate network traffic, which allows you to specify access to users who can access selected destination addresses.

- **Bridged mode**—This mode acts as a Layer 2 “bump in the wire” in the network connections. The bridged mode forwards packets regardless of the destination address.

**Note**
Inline Posture nodes also support a maintenance mode, which takes the node offline so that you can perform administrative procedures. This mode is also the default when an Inline Posture node is initially brought online in the network.

**Inline Posture Routed Mode**

In the routed mode, an Inline Posture node operates as a Layer 3 router and functions as the default gateway for an untrusted (outside Cisco ISE) network with its managed clients. All traffic between an untrusted and trusted network passes through this Inline Posture routed mode. The routed mode applies IP filtering rules, the configured access policies, and other traffic-based policies you have set up for your network.

When you configure an Inline Posture node in its routed mode, specify the IP addresses of its two interfaces:

- Trusted (Eth0)
- Untrusted (Eth1)

The trusted and untrusted addresses should be on different subnets. An Inline Posture node can manage one or more subnets, and the untrusted interface acts as a gateway for the managed subnets. Figure 1-7 illustrates an example of an Inline Posture routed mode configuration.
Inline Posture Bridged Mode

When operating in a bridged mode, the Inline Posture node operates like a standard Ethernet bridge. This configuration is used most often when the untrusted network already contains a gateway, and you do not want or plan to make any changes to the existing configuration.

Figure 1-8 shows the Inline Posture node acting as a bridge for the Layer 2 client traffic from the WLC into the Cisco ISE network. While in this configuration, the Inline Posture node requires subnet entries for the subnets to be able to respond to and send ARP broadcasts to the correct VLANs.

The Layer 2 flow of traffic from the three example subnets (10.20.80.0/24, 10.20.90.0/24, and 10.20.60.0/24) all reflect the use of the bridged mode on the Inline Posture node using VLAN mapping. The only difference between the three subnet examples is that for the 10.20.60.0/24 subnet, the Inline Posture main interfaces reside within this subnet.
Deploying Inline Posture as Standalone or High Availability

The most important decision you may make about your Inline Posture deployment is whether to deploy it as a single, standalone Inline Posture node, or as a primary-secondary pair to ensure high availability and provide redundancy for network reliability.

A standalone Inline Posture node is a single Inline Posture node that provides Inline Posture services, while working independently of all other nodes in your Cisco ISE network. You may decide to deploy a single standalone Inline Posture node for a network that serves a smaller facility or for a small network where network redundancy is not a major concern.

When you configure a pair of Inline Posture nodes for high availability, they act as primary-secondary pair to provide additional redundancy and reliability. This primary-secondary pair ensures that your network continues functioning even if one node in the pair fails. If the primary node fails, the secondary node takes over and provides the needed Inline Posture functionality.

About Inline Posture High Availability

Inline Posture high availability consists of two Inline Posture nodes that are configured as a primary-secondary pair. In this configuration, the primary node acts as the RADIUS proxy and forwards all network packets. If the primary node fails, the secondary Inline Posture node in this pair takes over.
In an Inline Posture stateless high-availability deployment that has a primary-secondary pair configuration, the secondary node acts as a backup unit and does not forward any packets between the interfaces. Stateless means that sessions that have been authenticated and authorized by the primary node are automatically authorized again once a failover occurs.

The secondary node monitors the primary node using the heartbeat protocol (on the eth2 and eth3 interfaces). The heartbeat protocol requires that messages are sent at regular intervals between the two nodes. If the heartbeat stops or does not receive a response back in the allotted time, failover occurs and recovery action takes place.

When the heartbeat protocol is active in an Inline Posture high-availability configuration, it requires a network connection between the eth2 and eth3 interfaces of the Inline Posture primary-secondary pair. The eth2 and eth3 interfaces of each node in an Inline Posture high-availability pair (primary and secondary) are configured to use heartbeat protocol exchanges between the two nodes. For this reason, you must make a direct cable connection between the eth2 interfaces of both Inline Posture nodes, and likewise, there must also be a direct cable connection between the eth3 interfaces of both nodes to ensure redundancy.

**Note**  The heartbeat protocol requires a direct cable connection between the eth2 interfaces of both nodes in a high-availability pair, as well as a direct cable connection between the eth3 interfaces of the two nodes. You can use any Ethernet cable to make these connections. **Figure 1-9** illustrates this cable requirement.
Introducing the Cisco ISE Hardware

This chapter introduces the Cisco Identity Services Engine (ISE) 3300 Series appliance and Cisco SNS-3400 Series appliance hardware and provides descriptions of the support appliance hardware, the major components, controls, connectors, and front-panel and rear-panel LED indicators. This chapter contains information about the following topics:

- Cisco ISE Series Appliances, page 1-1
- Cisco ISE 3300 Series Appliance Hardware Summary, page 1-1
- Cisco SNS-3400 Series Appliance Hardware Summary, page 1-15

Cisco ISE Series Appliances

The Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS) and Cisco ISE software run on either a dedicated Cisco ISE 3300 Series appliance or on a VMware server (Cisco ISE VM). The Cisco ISE Release 1.1.x software does not support the installation of any other packages or applications on this dedicated platform. See the Release Notes for Cisco Identity Service Engine, Release 1.1.x for additional hardware compatibility information.

Cisco ISE 3300 Series Appliance Hardware Summary

Table 1-1, Table 1-2, and Table 1-3 summarize the hardware specifications for each of the supported Cisco ISE appliances. See the Diagrams column for hyperlinks to detailed diagrams that show network interface card (NIC) ports, power supply sockets, LEDs, and important controls or buttons on the corresponding panel.
Table 1-1    Cisco ISE 3315 Appliance Hardware Summary

<table>
<thead>
<tr>
<th>Hardware and Support Specifications</th>
<th>Diagrams</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco ISE concurrent endpoint support:¹</td>
<td>• Figure 1-2 on page 1-6, “Cisco ISE 3315 Front-Panel Features”</td>
</tr>
<tr>
<td>− Policy Service node only—up to 3,000</td>
<td>• Figure 1-3 on page 1-6, “Cisco ISE 3315 Front-Panel LEDs and Buttons”</td>
</tr>
<tr>
<td>− Any other node type or combination—up to 2,000</td>
<td>• Figure 1-4 on page 1-7, “Cisco ISE 3315 Rear-Panel Features”</td>
</tr>
<tr>
<td>• Single processor: Quad-core Intel Xeon (Core 2 quad)</td>
<td>• Figure 1-5 on page 1-7, “Cisco ISE 3315 Rear-Panel LEDs”</td>
</tr>
<tr>
<td>• 4 gigabyte (GB) RAM</td>
<td></td>
</tr>
<tr>
<td>• 2 x 250 GB SATA² hard disk drive (HDD)</td>
<td></td>
</tr>
<tr>
<td>• Four 10/100/1000 LAN ports [two integrated NICs; 2 gigabit (Gb) NICs (PCI-E)]</td>
<td></td>
</tr>
<tr>
<td>• CD/DVD-ROM drive</td>
<td></td>
</tr>
<tr>
<td>• Four USB ports (two on the front panel, two on the rear panel)</td>
<td></td>
</tr>
<tr>
<td>• Two Gb Ethernet ports on rear panel</td>
<td></td>
</tr>
<tr>
<td>• One serial port on the rear panel</td>
<td></td>
</tr>
<tr>
<td>• One Video Graphics Array (VGA) port on the front panel</td>
<td></td>
</tr>
<tr>
<td>• Weight—From 24.25 lb (11.0 kg) to 28.0 lb (12.7 kg), depending on what options are installed.</td>
<td></td>
</tr>
<tr>
<td>• Dimensions—1.75 in. H 17.3 in. W x 22.0 in. D (44.5 mm x 440.0 mm x 559.0 mm); these dimensions do not include the rack handles.</td>
<td></td>
</tr>
<tr>
<td>• Cooling fans—Five (plus two on the power supply).</td>
<td></td>
</tr>
<tr>
<td>• Rack mounting—Uses slide rails (see Installing the Slide Rails in a Rack, page 1-4); mounts in a standard 19-inch (48.3 cm), four-post equipment rack (by using the provided rack-mount brackets).</td>
<td></td>
</tr>
<tr>
<td>• Maximum operating altitude—7000 feet (2133 meters).</td>
<td></td>
</tr>
<tr>
<td>• Operating temperature range—50 to 90° F (10 to 35° C) up to 3,000 feet (914.4 meters); 50 to 90° F (10 to 32° C) 3000 to 7000 feet (914.4 to 2133 meters).</td>
<td></td>
</tr>
<tr>
<td>• Power—Configured for AC-input power; has a single autoranging AC-input power supply (350 Watts).</td>
<td></td>
</tr>
</tbody>
</table>

Note  The Cisco ISE 3315 appliance is normally shipped with a rack-mount hardware kit that includes brackets or rails for mounting it in a four-post equipment rack. For more information, see Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack, page 1-2.

---

1. Concurrent endpoints represent the total number of supported users and devices. This can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

2. SATA = serial advanced technology attachment.
Table 1-2 Cisco ISE 3355 Appliance Hardware Summary

<table>
<thead>
<tr>
<th>Hardware and Support Specifications</th>
<th>Diagrams</th>
</tr>
</thead>
</table>
| - Cisco ISE concurrent endpoint support: 
  - Policy Service node only—up to 6,000
  - Any other node type or combination—up to 2,000
- Single processor: Quad-core Intel Xeon (Nehalem)
- 4 GB RAM
- 2 x 300 GB SAS² RAID³ HDD
- Four 10/100/1000 LAN ports [two integrated NICs; 2 Gb NICs (PCI-E)]
- CD/DVD-ROM drive
- Four USB ports (one on the front panel, one internal, two on the rear panel)
- Two Gb Ethernet ports on the rear panel
- One serial port on the rear panel
- Two VGA ports (one on front panel and one on rear panel)
- Cavium CN-1620-400-NHB-G accelerator card
- Weight—From 28 lb (12.7 kg) to 34.5 lb (15.6 kg) depending on what options are installed.
- Dimensions—1.7 in. H x 17.3 in. W x 28.0 in. D (43 mm x 440.0 mm x 711.4 mm); these dimensions do not include the rack handles.
- Cooling fans—Six for single-processor (Cisco ISE 3355) or dual-processor (Cisco ISE 3395).
- Rack mounting—Uses slide rails (see Installing the Slide Rails in a Rack, page 1-4); mounts in a standard 19-inch (48.3 cm), four-post equipment rack (by using the provided rack-mount brackets).
- Maximum operating altitude—7000 feet (2133 meters).
- Operating temperature range—50 to 90° F (10 to 35° C) up to 3000 feet (914.4 meters); 50 to 90° F (10 to 32° C) 3000 to 7000 feet (914.4 to 2133 meters).
- Power—Configured for AC-input power; has dual redundant auto-switching power supplies (675 Watts).

Note The Cisco ISE 3355 and Cisco ISE 3395 appliances are normally shipped with a rack-mount hardware kit that includes brackets or rails for mounting it in a four-post equipment rack. For more information, see Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack, page 1-2. The rack-mount hardware kits for Cisco ISE 3300 Series appliances do not include a two-post equipment rack.
1. Concurrent endpoints represent the total number of supported users and devices. This can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

2. SAS = single-attachment station.

3. RAID = redundant array of independent disks.

Table 1-3  Cisco ISE 3395 Appliance Hardware Summary

<table>
<thead>
<tr>
<th>Hardware and Support Specifications</th>
<th>Diagrams</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco ISE concurrent endpoint support:</td>
<td>• Figure 1-12 on page 1-12, “Cisco ISE 3395 Front-Panel Features”</td>
</tr>
<tr>
<td>– Policy Service node only—up to 10,000</td>
<td>• Figure 1-13 on page 1-13, “Cisco ISE 3395 Front-Panel LEDs and Buttons”</td>
</tr>
<tr>
<td>– Any other node type or combination—up to 2,000</td>
<td>• Figure 1-14 on page 1-14, “Cisco ISE 3395 Rear-Panel Features”</td>
</tr>
<tr>
<td>• Dual processor: 2 x Quad-core Intel Xeon (Nehalem)</td>
<td>• Figure 1-15 on page 1-15, “Cisco ISE 3395 Rear-Panel LEDs”</td>
</tr>
<tr>
<td>• 4 GB RAM</td>
<td></td>
</tr>
<tr>
<td>• 4 x 300 GB SAS RAID HDD</td>
<td></td>
</tr>
<tr>
<td>• 4 10/100/1000 LAN ports [two integrated NICs; 2 Gb NICs (PCI-E)]</td>
<td></td>
</tr>
<tr>
<td>• CD/DVD-ROM drive</td>
<td></td>
</tr>
<tr>
<td>• Four USB ports (one on the front panel, one internal, two on the rear panel)</td>
<td></td>
</tr>
<tr>
<td>• Two Gb Ethernet ports on the rear panel</td>
<td></td>
</tr>
<tr>
<td>• One serial port on the rear panel</td>
<td></td>
</tr>
<tr>
<td>• Two VGA ports (one on front panel and one on rear panel)</td>
<td></td>
</tr>
<tr>
<td>• Cavium CN-1620-400-NHB-G accelerator card</td>
<td></td>
</tr>
<tr>
<td>• Weight—From 28 lb (12.7 kg) to 34.5 lb (15.6 kg) depending on what options are installed.</td>
<td></td>
</tr>
<tr>
<td>• Dimensions—1.7 in. H x 17.3 in. W x 28.0 in. D (43 mm x 440.0 mm x 711.4 mm); these dimensions do</td>
<td></td>
</tr>
<tr>
<td>not include the rack handles.</td>
<td></td>
</tr>
<tr>
<td>• Cooling fans—Six for single-processor (Cisco ISE 3355) or dual-processor (Cisco ISE 3395).</td>
<td></td>
</tr>
<tr>
<td>• Rack mounting—Uses slide rails (see Installing the Slide Rails in a Rack, page 1-4); mounts in a</td>
<td></td>
</tr>
<tr>
<td>standard 19-inch (48.3 cm), four-post equipment rack (by using the provided rack-mount brackets).</td>
<td></td>
</tr>
<tr>
<td>• Maximum operating altitude—7000 feet (2133 meters).</td>
<td></td>
</tr>
<tr>
<td>• Operating temperature range—50 to 90° F (10 to 35° C) up to 3000 feet (914.4 meters); 50 to</td>
<td></td>
</tr>
<tr>
<td>90° F (10 to 32° C) 3000 to 7000 feet (914.4 to 2133 meters).</td>
<td></td>
</tr>
<tr>
<td>• Power—Configured for AC-input power; has dual redundant auto-switching power supplies (675 Watts).</td>
<td></td>
</tr>
</tbody>
</table>
1. Concurrent endpoints represent the total number of supported users and devices. This can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

**Cisco ISE 3315 Serial Number Location**

The serial number label is located at the lower left of the front panel of the Cisco ISE 3315 (see Figure 1-1).

*Figure 1-1   Cisco ISE 3315 Appliance Serial Number Location*

- The serial number for the Cisco ISE 3315 is defined by and observes the Cisco unique device identifier (UDI) specifications.

**Cisco ISE 3315 Front and Rear Panels**

The Cisco ISE 3315 platform is recommended for deployments that manage up to three additional appliances or three high-availability pairs. The Cisco ISE 3315 comes equipped with four network interfaces that provide flexibility in NIC interface selection and also enables it for use in high-availability configurations. For additional details, see *Cisco ISE Series Appliances, page 1-1.*

- Concurrent endpoints represent the total number of supported users and devices. This can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.
Cisco ISE 3315 Front-Panel Features

Figure 1-2, Figure 1-3, and the accompanying tables illustrate and describe the Cisco ISE 3315 front-panel features, LEDs, and buttons.

Figure 1-2   Cisco ISE 3315 Front-Panel Features

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Front USB port 1</td>
</tr>
<tr>
<td>2</td>
<td>Front USB port 2</td>
</tr>
<tr>
<td>3</td>
<td>Hard disk drive (HDD) bay 0</td>
</tr>
<tr>
<td>4</td>
<td>HDD bay 1</td>
</tr>
<tr>
<td>5</td>
<td>CD-ROM/DVD drive</td>
</tr>
</tbody>
</table>

Figure 1-3   Cisco ISE 3315 Front-Panel LEDs and Buttons

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power status LED</td>
</tr>
<tr>
<td>2</td>
<td>Power button (Recessed.)</td>
</tr>
<tr>
<td>3</td>
<td>Reset button (Recessed.)</td>
</tr>
<tr>
<td>4</td>
<td>HDD activity LED</td>
</tr>
<tr>
<td>5</td>
<td>Locator button or LED</td>
</tr>
<tr>
<td>6</td>
<td>System health LED</td>
</tr>
</tbody>
</table>

1. Power status LED: Green = Appliance has AC power and is powered on. Off = Appliance is powered off (AC power disconnected).
2. Power button: (Recessed.)
3. Reset button: (Recessed.)
5. Locator button or LED: Flashing blue = Locator button has been pressed.
6. System health LED: Off = System health is normal. Amber = Prefailure system threshold has been reached, which can be caused by any of the following conditions:
   - At least one fan failure (system or processor fan).
   - At least one of the temperature sensors reached critical level (system or processor thermal sensors).
   - At least one memory module failed.
   - A power supply unit error has occurred.
Cisco ISE 3315 Rear-Panel Features

Figure 1-4, Figure 1-5, and the accompanying tables illustrate and describe the Cisco ISE 3315 rear-panel features and LEDs.

Figure 1-4  Cisco ISE 3315 Rear-Panel Features

1. AC Power supply cable socket
2. NIC 3 (eth2) add-on card
3. NIC 4 (eth3) add-on card
4. Serial port
5. Video port
6. NIC 2 (eth1) Gigabit Ethernet interface
7. NIC 1 (eth0) Gigabit Ethernet interface
8. Rear USB port 4
9. Rear USB port 3

Figure 1-5  Cisco ISE 3315 Rear-Panel LEDs

1. NIC 1 (eth0) activity LED
   - Green = Activity exists.
   - Flashing green = Activity exists.
   - Off = No activity exists.
2. NIC 1 (eth0) link LED
   - Green = Link exists.
   - Off = No link exists.
3. NIC 2 (eth1) activity LED
   - Green = Activity exists.
   - Flashing green = Activity exists.
   - Off = No activity exists.
4. NIC 2 (eth1) link LED
   - Green = Link exists.
   - Off = No link exists.
Cisco ISE 3355 Serial Number Location

The serial number label is located at the lower left of the front panel of the Cisco ISE 3355 (see Figure 1-6).

![Cisco ISE 3355 Appliance Serial Number Location](image)

**Note**
The serial number for the Cisco ISE 3355 is defined by and observes the Cisco UDI specifications.

Cisco ISE 3355 Front and Rear Panels

The Cisco ISE 3355 platform provides enhanced capability for enterprise-wide deployments that manage up to 20 other appliances or high-availability pairs. Similar to the Cisco ISE 3315, the Cisco ISE 3355 comes equipped with four network interfaces that provide flexibility in NIC interface selection and also make it capable for use in high-availability configurations.

The Cisco ISE 3355 also provides 4 GB of RAM, two SAS drives that are configured in RAID 0 and 1, dual power supplies, and a Cavium CN-1620-400-NHB-G accelerator card that supports Secure Sockets Layer (SSL) for larger network deployments and provides added reliability for centralized management of the deployment in the network core. For details, see Cisco ISE Series Appliances, page 1-1.

Cisco ISE 3355 Front-Panel Features

Figure 1-7, Figure 1-8, and the accompanying tables illustrate and describe the Cisco ISE 3355 front-panel features, LEDs, and buttons.

![Cisco ISE 3355 Front-Panel Features](image)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDD bay 0</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Empty (unused) HDD bay¹</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Empty (unused) HDD bay¹</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Power button with LED indicator (bi-color: green</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>or amber)</td>
<td></td>
</tr>
</tbody>
</table>

¹: This bay is designated for future use or expansion.
### Chapter 1      Introducing the Cisco ISE Hardware

Cisco ISE 3300 Series Appliance Hardware Summary

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Operator information panel</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>Operator information panel release switch</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Video port</td>
<td></td>
</tr>
</tbody>
</table>

1. We do not support installing additional hard drives in the Cisco ISE 3355 appliance.

### Figure 1-8    Cisco ISE 3355 Front-Panel LEDs and Buttons

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDD activity LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green = Hard disk drive activity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flashing Green = Hard disk drive activity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = Hard disk drive is idle or disabled.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HDD status LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amber = Hard disk drive is in error state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = Hard disk drive is functioning or disconnected from power.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Power switch button cover</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cover slides left or right to expose or protect the power switch.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Ethernet icon LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green = Ethernet interfaces are configured and up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = No Ethernet interfaces are currently configured or Ethernet interfaces are all down.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Ethernet interface activity LEDs (NIC 1 and NIC 2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green = Activity exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flashing green = Activity exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = No activity exists.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Information LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amber = A noncritical system event has occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = System is functioning normally.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>System health LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = System health is normal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amber = A prefailure system threshold has been reached, which can be caused by any of the following conditions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>At least one fan failure (system or processor fan).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>At least one of the temperature sensors reached critical level (system or processor thermal sensors).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>At least one memory module failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A power supply unit error has occurred.</td>
<td></td>
</tr>
</tbody>
</table>
Cisco ISE 3300 Series Appliance Hardware Summary

Chapter 1      Introducing the Cisco ISE Hardware

Cisco ISE 3355 Rear-Panel Features

Figure 1-9, Figure 1-10, and the accompanying tables illustrate and describe the Cisco ISE 3355 rear-panel features and LEDs.

Figure 1-9    Cisco ISE 3355 Rear-Panel Features

<table>
<thead>
<tr>
<th></th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Front locator button or LED</td>
</tr>
<tr>
<td></td>
<td>Flashing blue = Locator button has been pressed.</td>
</tr>
<tr>
<td>9</td>
<td>Ethernet interface activity LEDs (NIC 3 and NIC 4)</td>
</tr>
<tr>
<td></td>
<td>Green = Activity exists.</td>
</tr>
<tr>
<td></td>
<td>Flashing green = Activity exists.</td>
</tr>
<tr>
<td></td>
<td>Off = No activity exists.</td>
</tr>
<tr>
<td>10</td>
<td>Power button with LED</td>
</tr>
<tr>
<td></td>
<td>Green = The appliance has AC power and is powered up.</td>
</tr>
<tr>
<td></td>
<td>Rapidly flashing green = The appliance is turned off and</td>
</tr>
<tr>
<td></td>
<td>not yet ready to be turned on. The appliance typically</td>
</tr>
<tr>
<td></td>
<td>remains in this state for 1 to 3 minutes.</td>
</tr>
<tr>
<td></td>
<td>Slowly flashing green = The appliance is currently turned</td>
</tr>
<tr>
<td></td>
<td>off and ready to be turned on.</td>
</tr>
<tr>
<td></td>
<td>Slowly fading on or off green = The appliance is in</td>
</tr>
<tr>
<td></td>
<td>power-save mode and is ready to be turned on.</td>
</tr>
<tr>
<td></td>
<td>Off = The appliance is turned off (AC power is</td>
</tr>
<tr>
<td></td>
<td>disconnected).</td>
</tr>
</tbody>
</table>

1   Empty (unused) PCI Express slot
2   Video port
3   Rear USB port 4
4   AC Power supply cable sockets
5   Rear USB port 3
6   Serial port (serial console, DB9 connection)
7   NIC 2 (eth1) Gigabit Ethernet interface
8   NIC 1 (eth0) Gigabit Ethernet interface
9   NIC 4 (eth3) add-on card
10  NIC 3 (eth2) add-on card
### Cisco ISE 3355 Rear-Panel LEDs

<table>
<thead>
<tr>
<th>Number</th>
<th>LED Description</th>
<th>Status Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NIC 1 (eth0) activity LED</td>
<td>Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.</td>
</tr>
<tr>
<td>2</td>
<td>NIC 1 (eth0) link LED</td>
<td>Green = Link exists. Off = No link exists.</td>
</tr>
<tr>
<td>3</td>
<td>AC power LED</td>
<td>Green = AC power source is connected to power supply. Off = No AC power source is connected to power supply.</td>
</tr>
<tr>
<td>4</td>
<td>DC power LED</td>
<td>Green = DC power source is connected to power supply. Off = No DC power source is connected to power supply.</td>
</tr>
<tr>
<td>5</td>
<td>Power supply error LED</td>
<td>Amber = Power source to power supply is present, but power supply is in error state. Off = Power supply is functioning normally (if AC and DC power indicators are green) or power supply is disconnected.</td>
</tr>
<tr>
<td>6</td>
<td>System error LED</td>
<td>Amber = Indicates that a system error has occurred. Off = The system is functioning normally.</td>
</tr>
<tr>
<td>7</td>
<td>Rear locator LED</td>
<td>Flashing blue = Front locator button has been pressed.</td>
</tr>
<tr>
<td>8</td>
<td>Power LED</td>
<td>Green = The appliance has AC power and is turned on. Rapidly flashing green = The appliance is turned off and is not yet ready to be turned on. The appliance typically only remains in this state for 1 to 3 minutes. Slowly flashing green = The appliance is currently turned off and ready to be turned on. Slowly fading on or off green = The appliance is in power-save mode and is ready to be turned on. Off = The appliance is turned off (AC power is disconnected).</td>
</tr>
</tbody>
</table>
Cisco ISE 3395 Serial Number Location

The serial number label is located at the lower left of the front panel of the Cisco ISE 3395 (see Figure 1-11).

**Figure 1-11  Cisco ISE 3395 Appliance Serial Number Location**

![Cisco ISE 3395 Appliance Serial Number Location](image)

**Note**
The serial number for the Cisco ISE 3395 is defined by and observes the Cisco UDI specifications.

Cisco ISE 3395 Front and Rear Panels

The Cisco ISE 3395 appliance provides the enhanced processing, memory, and power necessary for an enterprise-wide deployment managing up to 40 additional appliances or HA pairs.

The Cisco ISE 3395 features dual processors, dual power supplies, 4 GB of RAM, four HDDs, four network interfaces, and a Cavium CN-1620-400-NHB-G accelerator card that supports SSL for larger network deployments and provides added reliability for centralized management of the deployment in the network core. For details, see Cisco ISE Series Appliances, page 1-1.

Cisco ISE 3395 Front-Panel Features

**Figure 1-12, Figure 1-13, and the accompanying tables illustrate and describe the Cisco ISE 3355 front-panel features, LEDs, and buttons.**

**Figure 1-12  Cisco ISE 3395 Front-Panel Features**

![Cisco ISE 3395 Front-Panel Features](image)
Cisco ISE 3395 Series Appliance Hardware Summary

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDD bay 0</td>
</tr>
<tr>
<td>2</td>
<td>HDD bay 2</td>
</tr>
<tr>
<td>3</td>
<td>Empty (unused) HDD bay</td>
</tr>
<tr>
<td>4</td>
<td>Power button with LED indicator (bi-color: green or amber)</td>
</tr>
<tr>
<td>5</td>
<td>Operator information panel</td>
</tr>
<tr>
<td>6</td>
<td>Operator information panel release switch</td>
</tr>
<tr>
<td>7</td>
<td>Video port</td>
</tr>
<tr>
<td>8</td>
<td>Front USB port 1</td>
</tr>
<tr>
<td>9</td>
<td>Front USB port 2</td>
</tr>
<tr>
<td>10</td>
<td>CD-ROM/DVD drive</td>
</tr>
<tr>
<td>11</td>
<td>Empty (unused) HDD bay</td>
</tr>
<tr>
<td>12</td>
<td>HDD bay 3</td>
</tr>
<tr>
<td>13</td>
<td>HDD bay 1</td>
</tr>
</tbody>
</table>

1. We do not support installing additional hard drives in the Cisco ISE 3395 appliance.

**Figure 1-13  Cisco ISE 3395 Front-Panel LEDs and Buttons**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDD activity LED</td>
</tr>
<tr>
<td>2</td>
<td>HDD status LED</td>
</tr>
<tr>
<td>3</td>
<td>Power switch button cover</td>
</tr>
<tr>
<td>4</td>
<td>Ethernet icon LED</td>
</tr>
<tr>
<td>5</td>
<td>Ethernet interface activity LEDs (NIC 1 and NIC 2)</td>
</tr>
<tr>
<td>6</td>
<td>Information LED</td>
</tr>
</tbody>
</table>

1. Green = Hard disk drive activity.  
Flashing Green = Hard disk drive activity.  
Off = Hard disk drive is idle or disabled.

2. Amber = Hard disk drive is in an error state.  
Off = Hard disk drive is functioning or disconnected from power.

3. Cover slides left or right to expose or protect power switch.

4. Green = Ethernet interfaces are configured and up.  
Off = No Ethernet interfaces are currently configured or the Ethernet interfaces are all down.

5. Green = Activity exists.  
Flashing green = Activity exists.  
Off = No activity exists.

6. Amber = A noncritical system event has occurred.  
Off = System is functioning normally.
Cisco ISE 3395 Rear-Panel Features

Figure 1-14, Figure 1-15, and the accompanying tables illustrate and describe the Cisco ISE 3395 rear-panel features and LEDs.

### Figure 1-14  Cisco ISE 3395 Rear-Panel Features

<table>
<thead>
<tr>
<th>Number</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Empty (unused) PCI Express slot</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Video port</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Rear USB port 4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>AC Power supply cable sockets</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Rear USB port 3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Serial port (serial console, DB9 connection)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>NIC 2 (eth1) Gigabit Ethernet interface</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NIC 1 (eth0) Gigabit Ethernet interface</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>NIC 4 (eth3) add-on card</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>NIC 3 (eth2) add-on card</td>
<td></td>
</tr>
</tbody>
</table>

**Cisco ISE 3300 Series Appliance Hardware Summary**

<table>
<thead>
<tr>
<th>Number</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>System health LED</td>
<td>Off = System health is normal. Amber = A prefailure system threshold has been reached, which can be caused by any of the following conditions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At least one fan failure (system or processor fan).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At least one of the temperature sensors reached critical level (system or processor thermal sensors).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At least one memory module failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A power supply unit error has occurred.</td>
</tr>
<tr>
<td>8</td>
<td>Locator button or LED</td>
<td>Flashing blue = Locator button has been pressed.</td>
</tr>
<tr>
<td>9</td>
<td>Ethernet interface activity LEDs (NIC 3 and NIC 4)</td>
<td>Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.</td>
</tr>
<tr>
<td>10</td>
<td>Power button or LED</td>
<td>Green = The appliance has AC power and is turned on. Rapidly flashing green = The appliance is turned off and is not yet ready to be turned on. The appliance typically only remains in this state for 1 to 3 minutes. Slowly flashing green = The appliance is currently turned off and ready to be turned on. Slowly fading on or off green = The appliance is in power-save mode and is ready to be turned on. Off = The appliance is turned off (AC power is disconnected).</td>
</tr>
</tbody>
</table>
Cisco SNS-3400 Series Appliance Hardware Summary

The Cisco SNS-3400 Series appliance hardware consists of the Secure Network Server (SNS) 3415 and 3495 appliances.

Table 1-4 summarizes the hardware specifications for the SNS 3415 and 3495 appliances. See the Diagrams column for hyperlinks to diagrams that show power supply sockets, LEDs, and important controls or buttons on the corresponding panel.
Chapter 1  Introducing the Cisco ISE Hardware

Cisco SNS-3400 Series Appliance Hardware Summary

Table 1-4  Cisco ISE SNS 3415/3495 Appliance Hardware Summary

<table>
<thead>
<tr>
<th>Cisco ISE Appliance</th>
<th>Hardware Specifications</th>
<th>Diagrams</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNS 3415</td>
<td>• Cisco UCS C220 M3</td>
<td>• SNS 3415/3495 Front Panel</td>
</tr>
<tr>
<td></td>
<td>• Single socket Intel E5-2609 2.4Ghz CPU, 4 total cores, 4 total threads</td>
<td>• SNS 3415/3495 Rear Panel</td>
</tr>
<tr>
<td></td>
<td>• 16-GB RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 x 600-GB disk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Embedded Software RAID 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4 GE network interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For physical, environmental, and power specifications, see Cisco SNS-3400 Series Server Specifications.</td>
<td></td>
</tr>
<tr>
<td>SNS 3495</td>
<td>• Cisco UCS C220 M3</td>
<td>• SNS 3415/3495 Front Panel</td>
</tr>
<tr>
<td></td>
<td>• Dual socket Intel E5-2609 2.4Ghz CPU, 8 total cores, 8 total threads</td>
<td>• SNS 3415/3495 Rear Panel</td>
</tr>
<tr>
<td></td>
<td>• 32-GB RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 x 600-GB disk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RAID 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4 GE network interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For physical, environmental, and power specifications, see Cisco SNS-3400 Series Server Specifications.</td>
<td></td>
</tr>
</tbody>
</table>

Cisco ISE SNS 3415/3495 Front and Rear Panels

Front Panel

Figure 1-16 shows the SNS 3415/3495 front panel.

Figure 1-16  SNS 3415/3495 Front Panel
Chapter 1      Introducing the Cisco ISE Hardware

Cisco SNS-3400 Series Appliance Hardware Summary

Rear Panel

Figure 1-17 shows the SNS 3415/3495 rear panel.

Figure 1-17      SNS 3415/3495 Rear Panel

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power button/power status LED</td>
</tr>
<tr>
<td>2</td>
<td>Identification button LED</td>
</tr>
<tr>
<td>3</td>
<td>System status LED</td>
</tr>
<tr>
<td>4</td>
<td>Fan status LED</td>
</tr>
<tr>
<td>5</td>
<td>Temperature status LED</td>
</tr>
<tr>
<td>6</td>
<td>Power supply status LED</td>
</tr>
<tr>
<td>7</td>
<td>Network link activity LED</td>
</tr>
<tr>
<td>8</td>
<td>Asset tag (serial number)</td>
</tr>
<tr>
<td>9</td>
<td>Keyboard, video, mouse (KVM) connector (used with the KVM cable that provides two USB, one Video Graphics Adapter (VGA), and one serial connector)</td>
</tr>
<tr>
<td>10</td>
<td>Drives (up to eight hot-swappable 2-5-inch drives)</td>
</tr>
</tbody>
</table>

Serial Number Location

The serial number for the server is printed on a label on the top of the server, near the front.
CHAPTER 1

Configuring the Cisco ISE Appliances

This chapter describes how to perform an initial configuration of a Cisco Identity Services Engine (ISE) 3300 Series appliance, and it contains the following topics:

- Before Configuring a Cisco ISE Series Appliance, page 1-1
- Understanding the Setup Program Parameters, page 1-3
- Configuring a Cisco ISE 3300 Series Hardware Appliance, page 1-6
- Downloading the Cisco ISE ISO Image, page 1-10
- Cisco Integrated Management Interface, page 1-11
- Configuring Cisco ISE on the Cisco SNS-3400 Series Appliance Using CIMC, page 1-11
- Verifying the Configuration Process, page 1-17

Note
Cisco requires you to review the configuration prerequisites listed in this chapter before you attempt to configure the Cisco ISE software on a Cisco ISE 3300 Series appliance.

Before Configuring a Cisco ISE Series Appliance

The Cisco ISE 3300 Series appliances are preinstalled with the Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS) and the Cisco ISE Release 1.1.x software.

The Cisco SNS-3400 Series appliances are preinstalled with the Cisco Application Deployment Engine (ADE) Release 2.0.5 operating system (ADE-OS) and the Cisco ISE Release 1.1.x software.

The Cisco ADE-OS and the Cisco ISE software are preinstalled on a dedicated Cisco ISE appliance (Cisco ISE 3300 Series) or can be installed on a VMware server in this release.

Make sure that you identify all of the following configuration settings for each appliance or VMware instance before proceeding:

- Hostname
- IP address for the Gigabit Ethernet 0 (eth0) interface
- Netmask
- Default gateway
- DNS domain
- Primary name server
Before Configuring a Cisco ISE Series Appliance

Chapter 1      Configuring the Cisco ISE Appliances

Before Configuring a Cisco ISE Series Appliance

- Primary Network Time Protocol (NTP) server
- System time zone
- Username (username for CLI-admin user)
- Password (password for CLI-admin user)
- Database administrator password and database user password (one-time entry only)

Note

If Cisco ISE is not able to reach the DNS or NTP server, the ISE configuration will fail. In case of DNS failure, the workaround is to correct the DNS from the ISE configuration CLI and then run application reset-config ise to re-prime the ISE database. NTP sync is a requirement during initial setup. If you are not providing a valid NTP server during the initial setup, then you need to reimagine the Cisco ISE appliance.

For details about the differences between the CLI-admin user and web-based admin user rights, see Admin Rights Differences: CLI-Admin and Web-Based Admin Users, page 1-2.

Installation Modes for Cisco ISE 3300 Series Appliance

After you download the Cisco ISE 1.1.4 ISO image, you can use any one of the following options to configure the Cisco ISE 1.1.4 software on your appliance:

- Burn the Cisco ISE 1.1.4 ISO image on a DVD and use it to install Cisco ISE 1.1.4 on the ISE 3300 Series and legacy NAC and ACS appliances. See Appendix 1, “Installing Cisco ISE on Cisco NAC and Cisco Secure ACS Appliances” for the supported ACS and NAC platforms.

Installation Modes for Cisco SNS-3400 Series Appliance

After you download the Cisco ISE 1.1.4 ISO image, you can use any one of the following options to configure the Cisco ISE 1.1.4 software on your appliance:

- Configure the Cisco Integrated Management Interface (CIMC) and use it to install Cisco ISE 1.1.4. See Appendix 1, “Configuring CIMC.”.
- Create a bootable USB Drive and use it to install Cisco ISE 1.1.4. See Appendix 1, “Creating a Bootable USB Drive.”.

Admin Rights Differences: CLI-Admin and Web-Based Admin Users

The username and password that you configure by using the Cisco ISE Setup program is 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 as 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 in sync, so that you can use the same user name and password for both admin roles.

You can add additional web-based admin users through the user interface itself. See the “Configuring Cisco ISE Administrators” section of the Cisco Identity Services Engine User Guide, Release 1.1.x for additional details.
Chapter 1 Configuring the Cisco ISE Appliances

Understanding the Setup Program Parameters

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

Tasks Performed by CLI-Admin and Web-Based Admin Users
The CLI-admin user and the web-based admin user can perform the following Cisco ISE system-related tasks:

- Back up the Cisco ISE application data.
- Display any system, application, or diagnostic logs on the Cisco ISE appliance.
- Apply Cisco ISE software patches, maintenance releases, and upgrades.
- Set the NTP server configuration.

Tasks Performed Only by the CLI-Admin User
Only the CLI-admin user can perform the following Cisco ISE system-related tasks:

- Start and stop the Cisco ISE application software.
- Reload or shut down the Cisco ISE appliance.
- Reset the web-based admin user in case of a lockout. For additional details, see Password Negated Due to Administrator Lockout, page 1-15.

Cisco recommends that you protect the CLI-admin user credentials by explicitly creating only those users that you want to access the Cisco ISE CLI.

Note

Web-based admin users that are created by using the Cisco ISE user interface cannot automatically log into the Cisco ISE CLI. Only CLI-admin users that were explicitly created to have these privileges can access the Cisco ISE CLI.

Refer to Accessing Cisco ISE Using a Web Browser, page 1-7 for additional details.

To create other CLI-admin users, you must first log into the Cisco ISE CLI as the CLI-admin user and complete the following tasks:

| Step 1 | Log in by using the CLI-admin username and password that you created during the setup process. |
| Step 2 | Enter the Configuration mode. |
| Step 3 | Run the username command. |

Note

For details, see the Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x.

Understanding the Setup Program Parameters

When you run the Cisco ISE Setup program to configure the Cisco ISE software, it launches an interactive CLI that prompts you to enter required parameters to configure the system (see Table 1-1).

Ensure that the DNS and NTP servers are reachable after you run Setup and whenever a Cisco ISE node reboots in the deployment.
There are several ways you can make a connection to the supported hardware appliances to run the Setup program:

- Using a network-based console connection to the hardware appliance.
- Using a local serial console cable connection to the rear panel of the appliance.
- Using a local keyboard and video (VGA) connection to the appliance.

These methods let you configure the initial network settings that create the initial set of administrator credentials for the appliance. Using the Setup program is a one-time configuration task.

**Note**

The following procedure assumes that you have properly installed, connected, and powered up the supported appliance by following the recommended procedures. For configuring VMware servers, see Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD, page 1-14.

### Table 1-1  Identity Services Engine Network Configuration Parameters for Setup

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Must not exceed 15 characters. Valid characters include alphanumeric (A-Z, a-z, 0-9), hyphen (-), with a requirement that the first character must be an alphabetic character.</td>
<td>isebeta1</td>
</tr>
<tr>
<td>(eth0) Ethernet interface address</td>
<td>Must be a valid IPv4 address for the Gigabit Ethernet 0 (eth0) interface.</td>
<td>10.12.13.14</td>
</tr>
<tr>
<td>Netmask</td>
<td>Must be a valid IPv4 netmask.</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Must be a valid IPv4 address for the default gateway.</td>
<td>10.12.13.1</td>
</tr>
<tr>
<td>DNS domain name</td>
<td>Cannot be an IP address. Valid characters include ASCII characters, any numbers, hyphen (-), and period (.).</td>
<td>mycompany.com</td>
</tr>
<tr>
<td>Primary name server</td>
<td>Must be enabled with a valid IPv4 address for the primary name server.</td>
<td>10.15.20.25</td>
</tr>
<tr>
<td>Add/Edit another name server</td>
<td>Must be a valid IPv4 address for an additional name server. (Optional) Allows you to configure multiple Name servers. To do so, enter y to continue.</td>
<td></td>
</tr>
<tr>
<td>Primary NTP server</td>
<td>Must be enabled with a valid IPv4 address or hostname of an NTP server.</td>
<td>clock.nist.gov</td>
</tr>
<tr>
<td>Add/Edit another NTP server</td>
<td>Must be a valid NTP domain.</td>
<td></td>
</tr>
<tr>
<td>System Time Zone</td>
<td>Must be a valid time zone. For details, see Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x, which provides a list of time zones that Cisco ISE supports. For example, for Pacific Standard Time (PST) it is PST8PDT (or UTC-8 hours).</td>
<td>UTC (default)</td>
</tr>
</tbody>
</table>

**Note** The time zones referenced in this hyperlink are the most frequently used time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones.
### Table 1-1  
**Identity Services Engine Network Configuration Parameters for Setup (continued)**

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be from 3 to 8 characters in length, and be composed of valid alphanumeric characters (A-Z, a-z, or 0-9).</td>
<td>admin (default)</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password (there is no default). The password must be a minimum of six characters in length and include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). The administrative password supports only the following special characters:</td>
<td>MyIseYP@@ss</td>
</tr>
<tr>
<td></td>
<td>• ~, !, @, $, &amp;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• *, ~, __, +=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• , ’, , ;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;, &gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Database Administrator Password</strong></td>
<td>Identifies the Cisco ISE database system-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and must include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). The allowed list of characters also include underscore (_) and pound (#) keys.</td>
<td>ISE4adbp_ss</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  All nodes in a distributed environment require the same password, so you must be sure to configure all of them by using the same entry. After you configure this password, Cisco ISE uses it “internally”; that is, you do not have to enter it when logging into the system.</td>
<td></td>
</tr>
<tr>
<td><strong>Database User Password</strong></td>
<td>Identifies the Cisco ISE database access-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and must include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). The allowed list of characters also includes underscore (_) and pound (#) keys.</td>
<td>ISE5udbp#ss</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  All nodes in a distributed environment require the same password, so you must be sure to configure all of them using the same entry. After you configure this password, Cisco ISE uses it “internally”; that is, you do not have to enter it when logging into the system.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Cisco ISE 3300 Series Hardware Appliance

This section describes running the Cisco ISE Setup program to configure the Cisco ISE 3300 Series software for the supported hardware appliances.

To configure a Cisco ISE 3300 Series appliance by using the Setup program, complete the following steps:

**Step 1** Connect a keyboard and a VGA monitor to the Cisco ISE 3300 Series appliance.

**Step 2** Ensure that a power cord is connected to the Cisco ISE 3300 Series and turn on the appliance. 

**Note** The Cisco ISE software is already preinstalled on the appliance. Do not insert the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx)* DVD. The DVD is provided only for performing appliance reimage or for CLI password recovery.

In about 2 minutes, the following prompt is displayed, which means that the boot sequence is complete:

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

**Step 3** At the prompt, type `setup` to start the Setup program. You are prompted to enter networking parameters and first credentials. The following illustrates a sample Setup program and default prompts:

**Note** Cisco ISE appliances track time internally using UTC time zones. If you do not know your own specific time zone, you can enter one based on the city, region, or country where your Cisco ISE appliance is located. See Tables *Table 1-2, Table 1-3, and Table 1-4* for sample time zones. It is recommended to configure the preferred time zone (the default is UTC) during installation when Setup prompts you to configure this setting.

```plaintext
Enter hostname[]: ise-server-1
Enter IP address[]: 10.1.1.10
Enter Netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.10.10.10
Enter default DNS domain[]: cisco.com
```

**Caution** Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable. For details about the impact of changing time zones, see “clock time zone” in Appendix A in the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.
Enter Primary nameserver[]: 200.150.200.150
Add/Edit another nameserver? Y/N: n
Enter primary NTP domain[]: clock.cisco.com
Add/Edit another NTP domain? Y/N: n
Enter system time zone[]: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Virtual machine detected, configuring VMware tools...
Appliance is configured
Installing applications...
Installing ISE...
Application bundle (ise) installed successfully

===Initial Setup for Application: ise===

Welcome to the ISE initial setup. The purpose of this setup is to provision the internal ISE database. This setup requires you to create database administrator password and also create a database user password.

Please follow the prompts below to create the database administrator password.

Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:
Confirm new database user password:
Successfully created database user password.

Running database cloning script...
Generating configuration...
Rebooting...

Welcome to the ISE initial setup. The purpose of this setup is to provision the internal database. This setup is non-interactive and will take roughly 15 minutes to complete. Please be patient.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

---

Note

Virtual machine detected, configuring VMware tools... message will display only if Cisco ISE is installed on a virtual machine. This message is not displayed if Cisco ISE is installed on a physical machine.
After the Cisco ISE software is configured, the Cisco ISE system reboots automatically. To log back into the Cisco ISE CLI, you must enter the CLI-admin user credentials that you configured during setup.

**Step 4**

After Cisco ISE reboots, you are prompted to enter and confirm the new database administrator and database user passwords. (All nodes in a distributed environment require the same password, so be sure to configure all of them by using the same entry.) You will see this prompt:

Welcome to the ISE initial setup. The purpose of this setup is to provision the internal database. This setup requires you to create a database administrator password and also create a database user password.

Please follow the prompts below to create the database administrator password.

Enter new database admin password:

Confirm new database admin password:

Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:

Confirm new database user password:

Successfully created database user password.

Running database cloning script...

Running database network config assistant tool...

Extracting ISE database contents...

Starting ISE database processes...

...

**Step 5**

After you log into the Cisco ISE CLI shell, you can run the following CLI command to check the status of the Cisco ISE application processes:

```
ise-server/admin# show application status ise
ISE Database listener is running, PID: 4845
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 6344
ISE M&T Session Database is running, PID: 4502
ISE M&T Log Collector is running, PID: 6652
ISE M&T Log Processor is running, PID: 6738
ISE M&T Alert Process is running, PID: 6542
ise-server/admin#
```

**Step 6**

After you confirm that the Cisco ISE Application Server is running, you can log into the Cisco ISE user interface by using one of the supported web browsers (see Accessing Cisco ISE Using a Web Browser, page 1-7).

To log into the Cisco ISE user interface by using a web browser, enter the following in the Address field:

https://<your-ise-hostname or IP address>/admin/

Here “your-ise-hostname or IP address” represents the hostname or IP address that you configured for the Cisco ISE 3300 Series appliance during setup.

**Step 7**

At the Cisco ISE Login window, you are prompted to enter the web-based admin login credentials (username and password) to access the Cisco ISE user interface. 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.

After you log into the Cisco ISE user interface, you can then configure your devices, user stores, policies, and other components.
The username and password credentials that you use for web-based access to the Cisco ISE user interface are not the same as the CLI-admin user credentials that you created during setup for accessing the Cisco ISE CLI interface. For an explanation of the differences between these two types of admin users, see Admin Rights Differences: CLI-Admin and Web-Based Admin Users, page 1-2.

Supported Time Zones
This section provides three tables that provide more information on common UTC time zones for Europe, the United States and Canada, Australia, and Asia.

Note
The format for time zones is POSIX or System V. POSIX time zone format syntax looks like America/Los_Angeles, while System V time zone syntax looks like PST8PDT.

- For time zones in Europe, the United States, and Canada, see Table 1-2.
- For time zones in Australia, see Table 1-3.
- For time zones in Asia, see Table 1-4.

Table 1-2 Common Time Zones

<table>
<thead>
<tr>
<th>Acronym or name</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td></td>
</tr>
<tr>
<td>GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu</td>
<td>Greenwich Mean Time, as UTC</td>
</tr>
<tr>
<td>GB</td>
<td>British</td>
</tr>
<tr>
<td>GB-Eire, Eire</td>
<td>Irish</td>
</tr>
<tr>
<td>WET</td>
<td>Western Europe Time, as UTC</td>
</tr>
<tr>
<td>CET</td>
<td>Central Europe Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>EET</td>
<td>Eastern Europe Time, as UTC + 2 hours</td>
</tr>
<tr>
<td>United States and Canada</td>
<td></td>
</tr>
<tr>
<td>EST, EST5EDT</td>
<td>Eastern Standard Time, as UTC -5 hours</td>
</tr>
<tr>
<td>CST, CST6CDT</td>
<td>Central Standard Time, as UTC -6 hours</td>
</tr>
<tr>
<td>MST, MST7MDT</td>
<td>Mountain Standard Time, as UTC -7 hours</td>
</tr>
<tr>
<td>PST, PST8PDT</td>
<td>Pacific Standard Time, as UTC -8 hours</td>
</tr>
<tr>
<td>HST</td>
<td>Hawaiian Standard Time, as UTC -10 hours</td>
</tr>
</tbody>
</table>

Table 1-3 Australia Time Zones

Australia

<table>
<thead>
<tr>
<th>Acronym</th>
<th>City 1</th>
<th>City 2</th>
<th>City 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>Adelaide</td>
<td>Brisbane</td>
<td>Broken_Hill</td>
</tr>
<tr>
<td>Canberra</td>
<td>Currie</td>
<td>Darwin</td>
<td>Hobart</td>
</tr>
</tbody>
</table>
Chapter 1 Configuring the Cisco ISE Appliances

Downloading the Cisco ISE ISO Image

You can download the Cisco ISE 1.1.4 ISO image from Cisco.com.

Step 1 Go to http://www.cisco.com/go/ise. You must already have valid Cisco.com login credentials to access this link.

Step 2 Click Download Software.

Table 1-3 Australia Time Zones (continued)

<table>
<thead>
<tr>
<th>Australia¹</th>
<th>Lindeman</th>
<th>LHI³</th>
<th>Melbourne</th>
</tr>
</thead>
<tbody>
<tr>
<td>North</td>
<td>NSW⁴</td>
<td>Perth</td>
<td>Queensland</td>
</tr>
<tr>
<td>South</td>
<td>Sydney</td>
<td>Tasmania</td>
<td>Victoria</td>
</tr>
<tr>
<td>West</td>
<td>Yancowinna</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Enter the country and city together with a forward slash (/) between them; for example, Australia/Currie.
2. ACT = Australian Capital Territory
3. LHI = Lord Howe Island
4. NSW = New South Wales

Table 1-4 Asia Time Zones

<table>
<thead>
<tr>
<th>Asia¹</th>
<th>Aden²</th>
<th>Aqtau</th>
<th>Baghdad</th>
<th>Beirut</th>
<th>Choihalsan</th>
<th>Dhakar</th>
<th>Gazer</th>
<th>Irkutsck</th>
<th>Jerusalem</th>
<th>Kashgar</th>
<th>Kuwait</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Almaty</td>
<td>Aqtobe</td>
<td>Bahrain</td>
<td>Bishkek</td>
<td>Chongqing</td>
<td>Dili</td>
<td>Harbi</td>
<td>Istanbul</td>
<td>Kabul</td>
<td>Katmandu</td>
<td>Krasnoyarsk</td>
</tr>
<tr>
<td></td>
<td>Amman</td>
<td>Ashgabat</td>
<td>Baku</td>
<td>Brunei</td>
<td>Columbo</td>
<td>Dubai</td>
<td>Hong_Kong</td>
<td>Jakarta</td>
<td>Kamchatka</td>
<td>Kuala_Lumpur</td>
<td>Kuching</td>
</tr>
<tr>
<td></td>
<td>Anadyr</td>
<td>Ashkhabad</td>
<td>Bangkok</td>
<td>Kolkata</td>
<td>Damascus</td>
<td>Dushanbe</td>
<td>Hovd</td>
<td>Jayapura</td>
<td>Karachi</td>
<td>Kuching</td>
<td></td>
</tr>
</tbody>
</table>

1. The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia.
2. Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

Note

Additional time zones are available if you use the Cisco ISE CLI **show timezones** command. This CLI command displays a list of all time zones available to you. Choose the most appropriate one for your network location.
Cisco Integrated Management Interface

You can monitor the server inventory, health, and system event logs by using the built-in Cisco Integrated Management Controller (CIMC) GUI or CLI interfaces. See the user documentation for your release at the following URL:


Configuring Cisco ISE on the Cisco SNS-3400 Series Appliance Using CIMC

After you have configured the CIMC for your appliance, you can use it to manage your Cisco SNS-3400 series appliance. You can perform all operations including BIOS configuration on your Cisco SNS-3400 series appliance through the CIMC.

Note

For configuring VMware servers, see Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD, page 1-14.

Before You Begin

- Ensure that you have configured the CIMC on your appliance. See Configuring CIMC, page 1-4 for more information.
- Ensure that you have properly installed, connected, and powered up the supported appliance by following the recommended procedures. See Connecting and Powering On the Server, page 1-1 and Checking the LEDs, page 1-2.
- Ensure that you have the Cisco ISE 1.1.4 ISO image on the client machine from which you are accessing the CIMC or you have a bootable USB with the Cisco ISE 1.1.4 ISO for installation. See Creating a Bootable USB Drive, page 1-6.
- Cisco ISE appliances track time internally using UTC time zones. If you do not know your own specific time zone, you can enter one based on the city, region, or country where your Cisco ISE appliance is located. See Table 1-2, Table 1-3, and Table 1-4 for sample time zones. We recommend that you configure the preferred time zone (the default is UTC) during installation when Setup prompts you to configure this setting.

Step 1

Connect to the CIMC for server management. Connect Ethernet cables from your LAN to the server, using the ports that you chose by your Network Interface Card (NIC) Mode setting. The Active-active and Active-passive NIC redundancy settings require you to connect to two ports.

Step 2

Use a browser and the IP address of the CIMC to log in to the CIMC Setup Utility. The IP address is based upon the CIMC configuration that you made (either a static address or the address assigned by your Dynamic Host Configuration Protocol (DHCP) server).
Step 3  Click **Launch KVM Console**.

Step 4  Use your CIMC credentials to log in.

Step 5  Click the **Virtual Media** tab.

Step 6  Click **Add Image** to choose the ISE 1.1.4 ISO from the system running your client browser.

Step 7  Check the **Mapped** check box against the virtual CD/DVD drive that you have created.

Step 8  Click the **KVM** tab.

Step 9  Choose **Macros > Ctrl-Alt-Del** to boot the Cisco SNS-3400 series appliance using the ISO image. A screen similar to the one shown in the following figure appears.

Step 10  Press F6 to bring up the boot menu. A screen similar to the following one appears.
Step 11  Choose the CD/DVD that you mapped and press Enter. A screen similar to the following one appears.

Step 12  At the boot prompt, enter 1 and press Enter.

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

Step 13  At the prompt, type setup to start the Setup program. You are prompted to enter networking parameters and first credentials. The following illustrates a sample Setup program and default prompts:

Enter hostname[]: ise-server-1
Enter IP address[]: 10.1.1.10
Enter Netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.10.10.10
Enter default DNS domain[]: cisco.com
Enter Primary nameserver[]: 200.150.200.150
Add/Edit another nameserver? Y/N: n
Enter primary NTP domain[]: clock.cisco.com
Add/Edit another NTP domain? Y/N: n
Enable SSH?: Y/N
Enter system time zone[]: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Virtual machine detected, configuring VMware tools...
Appliance is configured
Installing applications...
Installing ISE...
Application bundle (ise) installed successfully

Welcome to the ISE initial setup. The purpose of this setup is to provision the internal ISE database. This setup is non-interactive, and will take roughly 15 minutes to complete.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

Note An “Installing ISE-IPEP” message appears when you install the IPN 1.1.4 ISO image and you will see an “Application bundle (ISE-IPEP) installed successfully” message.

Note A “Virtual machine detected, configuring VMware tools...” message appears only if Cisco ISE is installed on a virtual machine. This message is not displayed if Cisco ISE is installed on a physical machine.

After the Cisco ISE or IPN software is configured, the Cisco ISE system reboots automatically. To log back in to the CLI, you must enter the CLI-admin user credentials that you configured during setup.

Step 14 If you installed the IPN ISO, go to Configuring Certificates for Inline Posture Nodes, page 1-18.

Step 15 If you installed the Cisco ISE 1.1.4 ISO, after you log in to the Cisco ISE CLI shell, you can run the following CLI command to check the status of the Cisco ISE application processes:

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

ISE Database listener is running, PID: 4845
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 6344
ISE M&T Session Database is running, PID: 4502
ISE M&T Log Collector is running, PID: 6652
ISE M&T Log Processor is running, PID: 6738
ISE M&T Alert Process is running, PID: 6542
ise-server/admin#

Step 16 After you confirm that the Cisco ISE Application Server is running, you can log in to the Cisco ISE user interface by using one of the supported web browsers (see Accessing Cisco ISE Using a Web Browser, page 1-7).
To log in to the Cisco ISE user interface by using a web browser, enter `https://<your-ise-hostname or IP address>/admin/` in the Address field:

Here “your-ise-hostname or IP address” represents the hostname or IP address that you configured for the Cisco SNS-3400 Series appliance during setup.

**Step 17**

At the Cisco ISE Login window, you are prompted to enter the web-based admin login credentials (username and password) to access the Cisco ISE user interface. 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.

After you log in to the Cisco ISE user interface, you can then configure your devices, user stores, policies, and other components.

The username and password credentials that you use for web-based access to the Cisco ISE user interface are not the same as the CLI-admin user credentials that you created during setup for accessing the Cisco ISE CLI interface. For an explanation of the differences between these two types of admin users, see [Admin Rights Differences: CLI-Admin and Web-Based Admin Users](#), page 1-2.

---

**Caution**

Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable. For details about the impact of changing time zones, see “clock time zone” in Appendix A in the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.

**Supported Time Zones**

This section provides three tables that provide more information about common UTC time zones for Europe, the United States and Canada, Australia, and Asia.

**Note**

We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports, logs, and posture agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

The format for time zones is POSIX or System V. POSIX time zone format syntax looks like America/Los_Angeles, and System V time zone syntax looks like PST8PDT.

- For time zones in Europe, the United States, and Canada, see Table 1-2.
- For time zones in Australia, see Table 1-3.
- For time zones in Asia, see Table 1-4.

**Table 1-5 Europe, United States, and Canada Time Zones**

<table>
<thead>
<tr>
<th>Acronym or Name</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Europe</strong></td>
<td></td>
</tr>
<tr>
<td>GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu</td>
<td>Greenwich Mean Time, as UTC</td>
</tr>
<tr>
<td>GB</td>
<td>British</td>
</tr>
<tr>
<td>GB-Eire, Eire</td>
<td>Irish</td>
</tr>
</tbody>
</table>
### Table 1-5  Europe, United States, and Canada Time Zones (continued)

<table>
<thead>
<tr>
<th>Acronym or Name</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WET</td>
<td>Western Europe Time, as UTC</td>
</tr>
<tr>
<td>CET</td>
<td>Central Europe Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>EET</td>
<td>Eastern Europe Time, as UTC + 2 hours</td>
</tr>
</tbody>
</table>

#### United States and Canada

| EST, EST5EDT    | Eastern Standard Time, as UTC -- 5 hours |
| CST, CST6CDT   | Central Standard Time, as UTC – 6 hours |
| MST, MST7MDT   | Mountain Standard Time, as UTC – 7 hours |
| PST, PST8PDT   | Pacific Standard Time, as UTC – 8 hours |
| HST            | Hawaiian Standard Time, as UTC – 10 hours |

### Table 1-6  Australia Time Zones

**Australia**

<table>
<thead>
<tr>
<th>ACT²</th>
<th>Adelaide</th>
<th>Brisbane</th>
<th>Broken_Hill</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canberra</td>
<td>Currie</td>
<td>Darwin</td>
<td>Hobart</td>
</tr>
<tr>
<td>Lord_Howe</td>
<td>Lindeman</td>
<td>LHI³</td>
<td>Melbourne</td>
</tr>
<tr>
<td>North</td>
<td>NSW⁴</td>
<td>Perth</td>
<td>Queensland</td>
</tr>
<tr>
<td>South</td>
<td>Sydney</td>
<td>Tasmania</td>
<td>Victoria</td>
</tr>
<tr>
<td>West</td>
<td>Yancowinna</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

1. Enter the country and city together with a forward slash (/) between them; for example, Australia/Carrie.
2. ACT = Australian Capital Territory
3. LHI = Lord Howe Island
4. NSW = New South Wales

### Table 1-7  Asia Time Zones

**Asia**

<table>
<thead>
<tr>
<th>Aden²</th>
<th>Almaty</th>
<th>Amman</th>
<th>Anadyr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aqtau</td>
<td>Aqtobe</td>
<td>Ashgabat</td>
<td>Ashkhabad</td>
</tr>
<tr>
<td>Baghdad</td>
<td>Baku</td>
<td></td>
<td>Bangkok</td>
</tr>
<tr>
<td>Beirut</td>
<td>Bishkek</td>
<td>Brunei</td>
<td>Kolkata</td>
</tr>
<tr>
<td>Choisalsan</td>
<td>Chongqing</td>
<td>Columbo</td>
<td>Damascus</td>
</tr>
<tr>
<td>Dhakar</td>
<td>Dili</td>
<td>Dubai</td>
<td>Dushanbe</td>
</tr>
<tr>
<td></td>
<td>Harbin</td>
<td>Hong_Kong</td>
<td>Hovd</td>
</tr>
<tr>
<td>Irkutsk</td>
<td>Istanbul</td>
<td>Jakarta</td>
<td>Jayapura</td>
</tr>
<tr>
<td>Jerusalem</td>
<td>Kabul</td>
<td>Kamchatka</td>
<td>Karachi</td>
</tr>
</tbody>
</table>
Verifying the Configuration Process

To verify that you have correctly completed the configuration process, use one of the following two methods to log into the Cisco ISE 3300 Series appliance:

- Web browser
- Cisco ISE CLI

To perform post-installation verification of configuration, see Chapter 1, “Performing Post-Installation Tasks.”

Table 1-7  Asia Time Zones (continued)

<table>
<thead>
<tr>
<th>Asia¹</th>
<th>Kashgar</th>
<th>Katmandu</th>
<th>Kuala Lumpur</th>
<th>Kuching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kuwait</td>
<td>Krasnoyarsk</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>

1. The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia.
2. Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

The Cisco ISE CLI show timezones command displays a list of all time zones available to you. Choose the most appropriate one for your network location.
Performing Post-Installation Tasks

This chapter describes several tasks that you must perform after successfully completing the installation and configuration of the Cisco Identity Services Engine (ISE) 3300 Series appliance. This chapter contains information about the following topics:

- Installing a License, page 1-1
- Accessing Cisco ISE Using a Web Browser, page 1-7
- Verifying the Cisco ISE Configuration, page 1-10
- Verifying the Installation of VMware Tools, page 1-12
- Resetting the Administrator Password, page 1-14
- Reimaging a Cisco ISE 3300 Series Appliance, page 1-16
- Configuring the Cisco ISE System, page 1-17
- Enabling System Diagnostic Reports in Cisco ISE, page 1-18
- Installing New Cisco ISE Software, page 1-18
- Configuring Certificates for Inline Posture Nodes, page 1-18

Installing a License

To manage a Cisco ISE system, you must have a valid license. Licensing provides the ability to restrict the use of the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

Concurrent endpoints represent the total number of supported users and devices. Endpoints can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

Cisco ISE software feature support is split into two functional sets:

- Base Package—Enables basic services of network access, guest, and link encryption
- Advanced Package—Enables more advanced services like Profiler, Posture, and Security Group Access
Each license package supports a specific number of concurrent endpoints that can connect and use the corresponding services. Services for each package type are enabled by installing corresponding licenses. There are two possible license-installation approaches:

- **Base and Advanced Licenses**: Base and Advanced licenses can be installed to enable corresponding feature support, depending on your installation. Each license may be installed separately, and you can also choose to install multiple licenses of the same type to cumulatively increase the number of endpoints for the corresponding package.

- **Wireless License**: The Wireless license enables the same number of endpoints on both the base and advanced package. However, the devices that are supported with this type of license are restricted to wireless devices. It is possible to subsequently remove this restriction by installing an Wireless Upgrade license that enables the base and advanced package feature support for all types of devices.

The following sections provide information about these topics:

- Types of Licenses, page 1-3
- Obtaining a License, page 1-6
- Autoinstallation of the Evaluation License, page 1-7

**Built-In License**

The Cisco ISE system includes an evaluation license that features both Base and Advanced package services, is valid for a 90-day period, and restricts the number of system base and advanced package users to 100. The Cisco ISE system prompts you before the evaluation license expires to download and install a valid production license.

When the evaluation license expires at the end of its 90-day period, the Administration web application will prompt you to install a valid production license for Base, Base and Advanced, or Wireless. (Although the evaluation license allows you to provide support for both wired and wireless users, purchasing and applying a Wireless License option cuts off support for any wired users that you may have been supporting during the evaluation period.) For specific details on using the administrator user interface to add and modify license files, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

**License Management**

When you deploy only one Administration ISE node in your network, licenses are centrally managed by the Administration ISE node and are automatically distributed among all other nodes (except Inline Posture nodes) in the deployment. When you have installed primary and secondary Administration ISE nodes in your network in a distributed deployment, however, each of the Administration ISE nodes in the deployment must have the same license files. In addition, in order to install license files on your Cisco ISE, the node must be in standalone mode or deployed as the primary Administration ISE node for the period of time it takes to install the required licenses.

**Note** Cisco ISE licenses are generated based on the Administration ISE node hardware ID, *not* the MAC address.

**Concurrent Endpoint Counts**

Each Cisco ISE license includes a count value for the Base, Base and Advanced, or Wireless packages that restricts the number of concurrent endpoints that can use Cisco ISE services. The count includes the total number of endpoints across the entire deployment that are concurrently connected to the network and accessing its services. License enforcement within Cisco ISE if the number of endpoints increases...
beyond the supported license count is a soft one, with the endpoint remaining unblocked from accessing services. For information about the alarms that are generated when endpoints exceed the licensed values, see License Enforcement, page 1-3.

License Enforcement
Cisco ISE tracks concurrent endpoints on the network and generates alarms when endpoint counts exceed the licensed amounts:
- 80% Info
- 90% Warning
- 100% Critical

Caution
Accurate endpoint accounting relies on RADIUS accounting.

License Expiration
Alarms will not be sent for license expiration notification. Upon logging into a Cisco ISE node with an expired license, administrators are not able to access the Cisco ISE dashboard or other services, and instead, are redirected to a license page on www.cisco.com.

Cisco ISE License Application Behavior
- When you install a Wireless License over the default Evaluation License, the Wireless License overrides the Evaluation License parameters with the specific duration and user count associated with the Wireless License.
- When you install a Base License over the default Evaluation License, the Base License overrides only the “Base” portion of the Evaluation License; thus keeping the Advanced License capabilities available only for the remainder of time allowed by the default Evaluation License duration.
- When you install an Advanced License over the default Evaluation License, the Advanced License overrides only the “Advanced” portion of the Evaluation License; thus keeping the Base License capabilities available only for the remainder of time allowed by the default Evaluation License duration.

Note
To avoid expiration issues that are associated with Base or Advanced features in the Cisco ISE, we recommend replacing the default Evaluation License with both a Base and Advanced License at the same time.

Types of Licenses
This section describes the four types of licenses that are supported for use with Cisco ISE 3300 Series appliances:
- Evaluation License, page 1-4
- Base License, page 1-5
- Advanced License, page 1-5
- Wireless License, page 1-5
Generally speaking, Base and Advanced licenses are primarily focused on providing Cisco ISE services, and Wireless license options are focused on ensuring that you are able to deploy Cisco ISE more quickly and easily in a purely wireless endpoint environment.


**License Guidelines**

The following are some license guidelines that you need to observe:

- Licenses are applied on Administration ISE nodes only.
- Deployments cannot have an Advanced license without the Base license.
- Wireless Licenses cannot coexist on an Administration ISE node with Base or Base and Advanced Licenses.
- Administration ISE nodes should ensure that networks cannot add more Advanced endpoint licenses than Base endpoint licenses.
- Inline Posture nodes do not require a separate license.
  - Inline Posture nodes are only supported on Cisco ISE 3300 Series appliances. They are not supported on VMware server systems.
  - Only certain wireless LAN controller (WLC) versions are supported by Inline Posture. (See Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x for details.)

**Note**

Inline Posture nodes are not supported on VMware server systems.

- When you launch the Cisco ISE before a license has been applied, only a bootstrap configuration that includes a license page appears.
- When the evaluation license approaches expiration, you are prompted to download and install a production license (Base, Base and Advanced, or Wireless) when you attempt web-based access with the Cisco ISE system.
- When a Base license is applied, Cisco ISE user interface screens and tabs are displayed for basic network access and Guest access.
- When an Advanced license is applied, Cisco ISE user interface screens and tabs are displayed for Profiler, Posture, and Security Group Access.

**Evaluation License**

The evaluation license consists of both the Base and Advanced license packages. An evaluation license is limited to support only 100 endpoints, and it expires in 90 days. This duration is not based on a real-time clock, but on the Cisco ISE system clock. The evaluation license comes preinstalled, and it does not require a separate installation.

As the evaluation license approaches the end of its 90-day period, the Cisco ISE system prompts the user to download and install a valid product license (Base or Advanced) by generating an alarm to upgrade the license. Upon installing a regular license, the services are continued as per the chosen package.
Base License

Base licenses are installed by using the Cisco ISE administrative interface on the device. Like the evaluation license, the Base license usage is also recorded on the device. The Base licenses are perpetual licenses. The Base package includes Authentication, Authorization, Guest, and Sponsor services, and this license package never expires.

Advanced License

Advanced licenses can be installed only on top of the Base license. You cannot upgrade the evaluation license to an Advanced license without first installing the Base license. In addition to the features that are available in the Base license package, the Advanced license activates the Profiler, Posture, and Security Group Access services of the Cisco ISE.

At any time, the total number of endpoints supported by the Advanced package cannot be higher than the Base license count (it can be equal to or less than Base license count).

Note
The Advanced Licenses are subscription-based and there are two valid subscription terms: three-year or five-year.

Wireless License

Wireless Licenses are designed to provide a flexible option to exclusively wireless service providers that not only offers the essential Base License functions like basic network access (authentication and authorization), Guest services, and link encryption, but also all Advanced License services, including Profiler, Posture, and Security Group Access services. The Cisco ISE ensures that only exclusively wireless customers are able to take advantage of the Wireless License options by only allowing RADIUS Wireless authentication requests that come from a wireless LAN controller (WLC) (Other authentication request methods are dropped.) In addition, the LiveLogs entries also indicate reasons for the dropped requests by indicating, “Request from a non-wireless device was dropped due to installed Wireless license.”

Note
Like Advanced License packages, Wireless Licenses are subscription-based.

If you currently subscribe to a Wireless License model for your deployment and then decide you want to offer Cisco ISE support for non-wireless endpoints on your network, rather than revert to a Base and Advanced License scheme as described earlier, you can move to a Wireless Upgrade License. These licenses are designed to provide the full range of Cisco ISE functions and policy management capabilities for all wireless and non-wireless client access methods, including wired and VPN concentrator access.

Note
You can only install a Wireless Upgrade license option on top of an existing Wireless license with the same allowable endpoint count. You cannot install a Wireless Upgrade on top of a Base plus Advanced license package.
Obtaining a License

To continue to use Cisco ISE services after the 90-day evaluation license expires, and to support more than 100 concurrent endpoints on the network, you must obtain and install your own Base or Base and Advanced license packages in the Cisco ISE. License files are based on a combination of the Cisco ISE hardware ID and Product Authorization Key (PAK). At the time you purchase your Cisco ISE, or before the 90-day license expires, you can access Cisco.com and order your Base or Base and Advanced licenses.

Within an hour of ordering your license files from Cisco.com, you should receive an email with the Cisco Supplemental End-User License Agreement and a Claim Certificate containing a PAK for each license that you order. After receiving the Claim Certificate, you can log in and access the Cisco Product License Registration site at http://www.cisco.com/go/license and provide the appropriate hardware ID information and PAK to generate your license.

You must supply the following specific information to generate your license file:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)
- Product Authorization Key (PAK)

Remember, if you are installing primary and secondary Administration ISE nodes in your network in a distributed deployment, each of the Administration ISE nodes in the deployment must have the same license files. In addition, in order to install license files on your Cisco ISE, the node must be in standalone mode or deployed as the primary Administration ISE node for the period of time it takes to install the required licenses. The day after you submit your license information in the Cisco Product License Registration site, you will receive an email with your license file as an attachment. Save the license file to a known location on your local machine and use the instructions in Managing Licenses in the “Managing Licenses” chapter of the Cisco Identity Services Engine User Guide, Release 1.1.x to add and update your product licenses in the Cisco ISE.

To determine your primary Administration ISE node hardware ID, complete the following:

**Step 1**
Access the direct-console CLI and enter the `show inventory` command. The output includes a line that is similar to the following:

```
PID: NAC3315, VID: V01, SN: ABCDEFG
```

**Step 2**
(Optional) If the license has not expired, you can view the primary Administration ISE node hardware ID by completing the following steps:

a. Choose Administration > System > Licensing.
   The License Operations navigation pane and Current Licenses page appears.

b. In the License Operations navigation pane, click Current Licenses.
   The Current Licenses page appears.

c. Select the button corresponding to the Cisco ISE node that you want to check for the primary Administration ISE node hardware ID, and click Administration Node.
   The product identifier, version identifier, and serial number appear.
For detailed information and license part numbers that are available for Cisco ISE, including licensing options for new installations as well as migration from an existing Cisco security product like Cisco Secure Access Control System, see the Cisco Identity Services Engine Ordering Guidelines at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html.

### Autoinstallation of the Evaluation License

If you are using a virtual machine for Cisco ISE with disk space between 60 and 600 GB, the Cisco ISE automatically installs the evaluation license. All Cisco ISE 3300 Series appliances ship with an evaluation license that is limited to 90 days and 100 endpoints.

After you have installed the Cisco ISE software and initially configured the appliance as the primary Administration ISE node, you must obtain and apply a license for your Cisco ISE as described in Obtaining a License, page 1-6. You apply all licenses to the Cisco ISE primary Administration ISE node by using the primary Administration ISE node hardware ID. The primary Administration ISE node then centrally manages all the licenses that are installed for your deployment.

Cisco ISE licenses are generated based on the primary Administration ISE node hardware ID, not the MAC address. The process of managing the licenses is the same for dual Administration ISE nodes as it is for a single Administration ISE node.

**Next Steps:**

To manage your licenses by using the Cisco ISE user interface, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x* and complete the following tasks:

- Adding and upgrading a license
- Editing a license

### Accessing Cisco ISE Using a Web Browser

The Cisco ISE 3300 Series appliances support a web interface using the following HTTPS-enabled browsers:

- Mozilla Firefox version 3.6
- Mozilla Firefox version 9
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9 (in Internet Explorer 8 compatibility mode)

**Note**

The Cisco ISE user interface does not support using the Microsoft IE8 browser in its IE7 compatibility mode (the Microsoft IE8 is supported in its IE8-only mode).
This section provides information about the following topics:

- Logging In, page 1-8
- Logging Out, page 1-9

Logging In

When you login to the Cisco ISE web-based interface for the first time, you will be using the preinstalled Evaluation license. You must use only the supported HTTPS-enabled browsers listed in the previous section. After you have installed Cisco ISE as described in this guide, you can log into the Cisco ISE web-based interface.

**To log into Cisco ISE using the web-based interface, complete the following steps:**

**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.

http://<IP address or host name>/admin/

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

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

**Step 4**
Click **Login**, and the Cisco ISE dashboard appears.
To recover or reset the Cisco ISE CLI-admin username or password, see the Re
setting the Administrator Password, page 1-14.

If you forget your CLI-admin username or password, use the Cisco Identity
Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, and
choose Password Recovery. This option allows you to reset the CLI-admin
username and password.

The minimum required screen resolution to view the Cisco ISE GUI and
for better user experience is 1280*800 pixels.

CLI-based and web-based username and password values are not the same when
logging into the Cisco ISE. For more information about the differences
between the Cisco ISE CLI-admin user and the Cisco ISE web-based admin user,
see Admin Rights Differences: CLI-Admin and Web-Based Admin Users,
page 1-2.

The license page appears only the first time that you log into Cisco ISE after
the evaluation license has expired.

We recommend that you use the Cisco ISE user interface to periodically
reset your administrator login password after you successfully log into the Cisco
ISE system. To reset your administrator password, see “Configuring Cisco ISE
Administrators” in the Cisco Identity Services Engine User Guide, Release 1.1.x
for details.

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID
enough times, the Cisco ISE user interface “locks you out” of the system, adds a
log entry in the Monitor > Reports > Catalog > Server Instance > Server
Administrator Logins report, and suspends the credentials for that
administrator ID until you have an opportunity to reset the password
associated with that administrator ID, as described in Password Negated
Due to Administrator Lockout, page 1-15. The number of failed attempts
required to disable the administrator account is configurable according to
the guidelines that are described in the “Managing Identities” chapter
administrator user account gets locked out, an email is sent to the
associated admin user.

Logging Out

To log out of the Cisco ISE web-based web interface, click Log Out in the Cisco
ISE main window toolbar. This act ends your administrative session and logs you
out.

For security reasons, we recommend that you log out of the Cisco ISE 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.
Verifying the Cisco ISE Configuration

This section provides two methods that each use a different set of username and password credentials for logging into and verifying your Cisco ISE configuration:

- Verifying the Configuration Using a Web Browser, page 1-10
- Verifying the Configuration Using the CLI, page 1-11

Note

For first time web-based access to the Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup. For CLI-based access to the Cisco ISE system, the administrator username by default is **admin** and the administrator password (which is user-defined because there is no default) represents the values that you configured during setup.

To better understand the rights differences between the CLI-admin user and the web-based admin user, see **Admin Rights Differences: CLI-Admin and Web-Based Admin Users, page 1-2.**

Verifying the Configuration Using a Web Browser

To verify that you successfully configured your Cisco ISE 3300 Series appliance, complete the following steps 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**.

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

For example, entering **http://10.10.10.10/admin/** displays the Cisco ISE Login page.
Step 3 In the Cisco ISE Login page, enter the username and password that you have defined during setup, and click **Login**.

The Cisco ISE dashboard appears.

**Note**

We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password after you have successfully logged into the Cisco ISE system. To reset your administrator password, see “Configuring Cisco ISE Administrators” in the *Cisco Identity Services Engine User Guide, Release 1.1.x* for details.

---

**Verifying the Configuration Using the CLI**

To verify that you successfully configured your Cisco ISE 3300 Series appliance, use the Cisco CLI and complete the following steps:

---

**Step 1** After the Cisco ISE appliance reboot has completed, launch a supported product for establishing a Secure Shell (SSH) connection to the ISE appliance (for example, by using PuTTY, an open source Telnet/SSH client).

**Step 2** In the Host Name (or IP Address) field, type in the hostname (or the IP address of the Cisco ISE appliance by using dotted decimal formation), and click **Open** to display the system prompt for the Cisco ISE appliance.

**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** To verify that the application has been installed properly, at the system prompt enter **show application version ise** and press **Enter**.
The console displays the following screen.

```
ise-4/admin# show application version ise
Cisco Identity Services Engine
------------------------------------------------
Version : 1.0.2.303
Build Date : Mon Oct 4 04:44:16 2010
Install Date : Mon Oct 4 22:51:55 2010
```

**Note**
The build number reflects the currently installed version of the Cisco ISE software.

**Step 6**
To check the status of the Cisco ISE processes, at the system prompt enter `show application status ise` and press **Enter**.

The console displays the following screen.

```
ise-4/admin# show application status ise
ISE Database listener is running, PID: 4014
ISE Database is running, number of processes: 29
ISE Application Server is running, PID: 4310
ISE Monitoring Session Database is running, PID: 3815
ISE Monitoring Log Collector is running, PID: 4369
ISE Monitoring Log Processor is running, PID: 4325
ISE Monitoring Alert Process is running, PID: 4331
```

**Note**
To get the latest Cisco ISE patches and to keep your Cisco ISE up-to-date, visit the following web site: http://software.cisco.com/download/navigator.html

**Step 7**
To check the Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS) version, at the system prompt, enter `show version` and press **Enter**.

The console displays the following output:

```
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.2.083
ADE-OS System Architecture: i386
```

---

**Verifying the Installation of VMware Tools**

You can verify the Installation of the VMware tools in the following two ways:

- Using Summary Tab in the vSphere Client
- Using the CLI

**Using Summary Tab in the vSphere Client**

Go to the Summary tab of the vSphere Client. The value for VMware Tools should be “OK”. The red arrow in Figure 1-1 indicates that the VMware tools are installed since the value is “OK”.

---
Verifying the Installation of VMware Tools

Using the CLI

You can also verify if the VMware tools are installed with the use of the `show inventory` CLI command. This command lists the NIC driver information. On a virtual machine with VMware tools installed, the driver information will be listed as “VMware Virtual Ethernet driver.” Refer to the following example:

```
vm36/admin# show inv
NAME: "ISE-VM-K9          chassis", DESCR: "ISE-VM-K9          chassis"
PID: ISE-VM-K9         , VID: V01 , SN: 8JDCELIDLJ0A
Total RAM Memory: 4016564 kB
CPU Core Count: 1
   CPU 0: Model Info: Intel(R) Xeon(R) CPU           E5504  @ 2.00GHz
Hard Disk Count(*): 1
   Disk 0: Device Name: /dev/sda
   Disk 0: Capacity: 64.40 GB
   Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
   NIC 0: Device Name: eth0
   NIC 0: HW Address: 00:0C:29:BA:C7:82
   NIC 0: Driver Descr: VMware Virtual Ethernet driver

(*) Hard Disk Count may be Logical.

vm36/admin#
```

Upgrading VMware Tools

Cisco ISE software contains the supported VMware tools. Although you can upgrade VMware tools through the VMware client user interface, that action does not update the tools on Cisco ISE. The VMware tools are only updated upon installing a new Cisco ISE software version via an ISO installation package, applying an upgrade bundle, or applying a patch. (Patches only have updates for VMware tools if there is a critical need.)
Resetting the Administrator Password

There are two ways to reset the administrator password in Cisco ISE. Depending on the nature of your particular password loss, use one of the following sets of instructions:

- **Lost, Forgotten, or Compromised Password, page 1-14** — Use this procedure if no one is able to log into the Cisco ISE system because the administrator password has been lost, forgotten, or compromised.

- **Password Negated Due to Administrator Lockout, page 1-15** — Use this procedure if your password has been rendered unusable because login failed the specified number of times in a row for the administrator ID.

Lost, Forgotten, or Compromised Password

If no one is able to log into the Cisco ISE system because the administrator password has been lost, forgotten, or compromised, you can use the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to reset the administrator password.

Prerequisites:

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to start up a Cisco ISE appliance:

- An error may occur if you attempt to start up a Cisco ISE appliance by using the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD under the following conditions:
  - You have a terminal server associated with the serial console connection to the Cisco ISE appliance that includes the `exec` line setting (you are not using the `no exec` line setting).
  - 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).

  and

  - You have a serial console connection to the Cisco ISE appliance.

  **Note**

  You can prevent these connection-related problems when using the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to start up a Cisco ISE appliance by setting the terminal server setting for the serial console line to use the “no exec” setting. This allows you to use both a KVM connection and a serial console connection.

Resetting the Administrator Password for a Cisco ISE Appliance

To reset the administrator password, complete the following steps:

- **Step 1** Ensure that the Cisco ISE appliance is powered up.
- **Step 2** Insert the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD in the appliance CD/DVD drive.
- **Step 3** Reboot the Cisco ISE appliance to boot from the DVD.
The console displays the following message (this example shows a Cisco ISE 3355):

```
Welcome to Cisco Identity Services Engine - ISE 3355
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
```

**Step 4**
To reset the administrator password, at the system prompt, enter 3 if you use a keyboard and video monitor connection to the appliance, or enter 4 if you use a local serial console port connection.

The console displays a set of parameters.

**Step 5**
Enter the parameters by using the descriptions that are listed in Table 1-1.

### Table 1-1 Password Reset Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin username</td>
<td>Enter the number of the corresponding administrator whose password you want to reset.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the new password for the designated administrator.</td>
</tr>
<tr>
<td>Verify password</td>
<td>Enter the password again.</td>
</tr>
<tr>
<td>Save change and reboot</td>
<td>Enter Y to save.</td>
</tr>
</tbody>
</table>

The console displays:

Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot? [Y/N]:

See the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*, for commands to reset DB passwords and other CLI commands.

### Password Negated Due to Administrator Lockout

You might enter an incorrect password for your administrator user ID enough times to disable the administrator password. The minimum and default number is five. The Cisco ISE user interface “locks you out” of the system and suspends the credentials for that administrator ID until you have an opportunity to reset the password that is associated with that administrator ID.
Changing the IP Address of a Cisco ISE 3300 Series Appliance

To change the IP address of a Cisco ISE 3300 series appliance, complete the following steps:

**Step 1** Log into the Cisco ISE CLI.

**Step 2** Enter the following:

```
configure terminal
interface GigabitEthernet 0
ip address <new_ip_address> <new_subnet_mask>
exit
```

**Note** Do not use the `no ip address` command when you change the Cisco ISE appliance IP address.

**Note** All the Cisco ISE services have to be restarted after changing the Cisco ISE appliance IP address.

Reimaging a Cisco ISE 3300 Series Appliance

You might need to reimage a Cisco ISE 3300 Series appliance, or you might want to reimage an appliance that was previously used for a Cisco Secure ACS Release 5.1 installation. For example, you plan to migrate Cisco Secure ACS data to Cisco ISE and want to re-use the appliance.
To reimage a Cisco ISE 3300 Series appliance, complete the following steps:

**Step 1** If the Cisco Secure ACS appliance is turned on, turn off the appliance.

**Step 2** Turn on the Cisco Secure ACS appliance.

**Step 3** Press F1 to enter the BIOS setup mode.

**Step 4** Use the arrow key to navigate to **Date and Time** and press **Enter**.

**Step 5** Set the time for your appliance to the UTC/GMT time zone.

**Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

**Step 6** Press Esc to exit to main BIOS menu.

**Step 7** Press Esc to exit from the BIOS Setup mode.

**Step 8** Perform the instructions described in Before Configuring a Cisco ISE Series Appliance, page 1-1.

**Step 9** Perform the instructions described in Understanding the Setup Program Parameters, page 1-3.

**Step 10** Insert the **Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)** DVD in the appliance CD/DVD drive.

The console displays (this example shows a Cisco ISE 3315):

```
Welcome to Cisco Identity Services Engine - ISE 3315
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

**Step 11** At the console prompt, enter 1 if you use a keyboard and video monitor, or enter 2 if you use a serial console port, and press **Enter**.

The reimage process uninstalls the existing Cisco ADE-OS and software versions, and installs the latest Cisco ADE-OS and Cisco ISE software versions.

For details about the installation and configuration process, see Before Configuring a Cisco ISE Series Appliance, page 1-1 and Understanding the Setup Program Parameters, page 1-3.

For details about migrating Cisco Secure ACS Release 5.1/5.2 data to a Cisco ISE Release 1.0 appliance, see the **Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x**.

---

**Configuring the Cisco ISE System**

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 authentication policies, authorization, policies, and using all the features, menus, and options, see the **Cisco Identity Services Engine User Guide, Release 1.1.x**.
Enabling System Diagnostic Reports in Cisco ISE

After installing Cisco ISE the first time or reimaging an appliance, you can choose to enable the system-level diagnostic reports using the Cisco ISE CLI (the logging function that reports on system diagnostics is not enabled in Cisco ISE by default).

To enable system diagnostic reports, do the following:

**Step 1**
Log into the Cisco ISE CLI console using your default administrator user ID and password.

**Step 2**
Enter the following commands:

```
admin# configure terminal
admin# logging 127.0.0.1:20514
admin# end
admin# write memory
```

You can configure system diagnostic settings through the Cisco ISE UI (Administration > System > Logging > Logging Categories > System Diagnostics).

Installing New Cisco ISE Software

Each Cisco ISE 3300 Series appliance comes preinstalled with Cisco ISE software. We recommend that should it be necessary to upgrade the preinstalled Cisco ISE ADE-OS and Cisco ISE software with a new version, that you make sure to preserve your existing system configuration information. Performing a new installation of Cisco ISE software on your appliance can take from between 10 minutes to 60 or more minutes (per deployed Cisco ISE node) depending on how much configuration data needs to be restored.

**Note**
After the new software installation is complete, clear the cache of any active browsers that have been used to access Cisco ISE before this installation process.

**For more information**
For details on installing the Cisco 3300 Series appliances with new Cisco ISE Release 1.0 software, see “Installing Cisco ISE Software” in the Release Notes for Cisco Identity Service Engine, Release 1.1.x.

Configuring Certificates for Inline Posture Nodes

After you have installed the IPN 1.1.4 ISO image on any of the supported appliance platforms and run the setup program, you must configure certificates for Inline Posture nodes before you can add them to the deployment.
Before You Begin

- Your Inline Posture node must be certified from the same CA that has certified your primary Administration ISE node.
- You can configure Inline Posture node certificates only from the command-line interface (CLI).
- If you wish to deploy an active-standby pair of Inline Posture nodes, you must configure the certificates on both the active and standby Inline Posture nodes.

**Step 1**
Log in to the Inline Posture node through the CLI.

**Step 2**
Enter the following command:
`pep certificate server generatecsr`

**Step 3**
Enter `n` to use an existing private key file to use with the certificate signing request or enter `y` to generate a new one.

**Step 4**
Enter your desired key size.

**Step 5**
Enter the type of digest that you want to sign the certificate with.

**Step 6**
Enter your country code name (2 letter code).

**Step 7**
Enter values for your state, city, organization, organizational unit.

**Step 8**
Enter the Common Name. The Common Name is the same as your hostname. You must enter the fully qualified domain name (FQDN). For example, if your hostname is `IPEP1` and your DNS domain name is `cisco.com`, you must enter `IPEP1.cisco.com` as your Common Name.

**Step 9**
Enter your e-mail address.

**Step 10**
Copy the entire block of text including the blank line after the END CERTIFICATE REQUEST tag (to include the carriage return).

**Step 11**
Send this CSR to the Certificate Authority that signed your primary Administration ISE node’s certificate.

*Note* Only server authentication is supported in the 1.1.4 release. If you use other CAs to sign your certificate, ensure that the extended key usage specifies server authentication alone.

**Step 12**
Download your signed certificate in the DER or base64 format, and copy it to an ftp server.

**Step 13**
Enter the following command from the Inline Posture node CLI:
`copy ftp://a.b.c.d/ipep1.cer disk:`
where `a.b.c.d` is the ip address of the ftp server and `ipep1.cer` is the CA-signed certificate that you are adding to the Inline Posture node.

**Step 14**
Enter the username and password for the ftp server.

**Step 15**
Enter the following command from the Inline Posture node CLI:
`pep certificate server add`

**Step 16**
Enter `y` for the application to restart.

**Step 17**
Enter `y` to bind the certificate to the last certificate signing request.
Step 18  Enter the name of the CA-signed certificate. The Inline Posture application restarts. You can now register this Inline Posture node with your primary Administration ISE node. Refer to the *Cisco Identity Services Engine User Guide, Release 1.1.x* for more information.
Installing Cisco ISE in a VMware Virtual Machine

This chapter describes the system requirements for installing the Cisco Identity Services Engine (ISE) 3300 Series appliance software in a VMware virtual machine. The following topics provides information about the installation process:

- Virtual Machine Requirements, page 1-1
- Disk Space Requirements, page 1-2
- Evaluating the Cisco ISE Release 1.1.x, page 1-3
- Configuring a VMware ESX or ESXi Server, page 1-4
- Configuring the VMware Server, page 1-7
- Preparing a VMware System for Cisco ISE Software Installation, page 1-14
- Installing the Cisco ISE Software on a VMware System, page 1-16
- Connecting to the Cisco ISE VMware Server Using Serial Console, page 1-17

The Inline Posture node is supported only on Cisco ISE 3300 Series appliances. It is not supported on VMware server systems. All the other designated roles are supported for use on VMware virtual machines.

### Virtual Machine Requirements

Table 1-1 lists the minimum system requirements to install Cisco ISE 3300 Series software on a VMware virtual machine to support 100 endpoints for evaluation purposes only.

<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Quad-Core; 2.13 GHz or faster</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB RAM</td>
</tr>
</tbody>
</table>

Note

The Inline Posture node is supported only on Cisco ISE 3300 Series appliances. It is not supported on VMware server systems. All the other designated roles are supported for use on VMware virtual machines.
Disk Space Requirements

The minimum system requirements for the virtual machine must be similar to the Cisco ISE 3300 Series appliance hardware configuration. Refer to the Identity Services Engine 3300 Series Appliances Data Sheet for the hardware configuration. See “Deployment Sizing and Scaling Recommendations” section on page 1-14 for virtual machine specifications for a production environment.

Table 1-2 lists the minimum Cisco ISE hard disk space allocation requirements for running on a VMware server in a production deployment. Use the supported VMware ESX and ESXi server versions listed in Table 1-1 for running Cisco ISE software in a production deployment.
Chapter 1      Installing Cisco ISE in a VMware Virtual Machine

Evaluating the Cisco ISE Release 1.1.x

The Cisco ISE software will only use up to 600 GB of disk space regardless of how much more disk space you allocate to the virtual machine.

On any node that has the Monitoring persona enabled, 30% of the VM disk space is allocated for log storage. For a Monitoring node with 600 GB VM disk space, 180 GB is allocated for log storage. A deployment with 100,000 user endpoints generates 2 GB of logs approximately per day. In this case, you can store 30 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 30 GB more for log storage. Depending on your requirements, you can increase the VM disk size up to a maximum of 600 GB or 180 GB log storage. The 30% disk space allotment is applicable only for fresh installations. If you upgrade to 1.1.x, a maximum of 150 GB is allocated for the MnT node irrespective of the VM disk size.

The Cisco ISE must be installed on a single disk in VMware.

Table 1-2   Minimum VMware Production Disk Space Requirements

| ISE Persona                                      | Minimum Disk Space Requirements for Production
|--------------------------------------------------|--------------------------------------------------
| Standalone ISE                                   | 600 GB                                           |
| Administration                                   | 200 GB                                           |
| Monitoring                                       | 500 GB                                           |
| Administration and Monitoring                    | 600 GB                                           |
| Administration, Monitoring, and Policy Service   | 600 GB                                           |
| Policy Service                                   | 100 GB                                           |

1. Additional disk space is required to support local logging, and to store the backup and upgrade files in the local disk.

Evaluating the Cisco ISE Release 1.1.x

For evaluation purposes, Cisco ISE Release 1.1.x can be installed in any of the supported VMware server virtual machines that meet the Virtual Machine Requirements, page 1-1. When evaluating Cisco ISE Release 1.1.x, you can configure less disk space in the virtual machine, but you still are required to allocate a minimum disk space of 60 GB.

To download the Cisco ISE Release 1.1.x software for evaluation, complete the following steps:

**Step 1** Go to the following link:

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

**Step 2** Click Download Software.
The Cisco ISE Release 1.1.x software image comes with a 90-day evaluation license already installed, so you can begin testing all Cisco ISE services once your installation and initial configuration are complete.

To migrate a Cisco ISE configuration from an evaluation system to a fully licensed production system, you need to complete the following tasks:

- Back up the configuration of the evaluation version
- Install a production deployment license
- Restore the configuration to the production system
- Increase disk space for installation

**Note**

The minimum Cisco ISE hard disk space allocation requirements for running on a VMware servers in an evaluation environments that support only 100 users is 60 GB. When you move your VMware server to a production environment that support a larger number of users, however, be sure to reconfigure your Cisco ISE installation to the recommended minimum disk size that is listed in Table 1-2 or higher (up to the allowed maximum of 600 GB). See “Deployment Sizing and Scaling Recommendations” section on page 1-14 for information on virtual machine requirements for a production environment.

---

**Configuring a VMware ESX or ESXi Server**

This section describes how to configure a VMware ESX or ESXi server on the VMware virtual machine. This section provides procedures for performing some important configuration-related tasks.

To perform the following procedures, you must log in to the ESXi server as a user with administrative privileges (root user). The values that are provided in the following procedures and illustrations are examples only. Actual values depend on your deployment requirements.

**Before You Begin**

Before you configure your VMware ESX or ESXi server, read the following:

- Cisco ISE 1.1.4 is a 32-bit system. Ensure that your virtual machine’s guest operating system is set to 32 bits. See [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870) for information on how to set your guest operating system type.

- Ensure that you allocate the recommended amount of disk space on the VMware virtual machine. See Table 1-2 on page 1-3 for more details.

- The VMware virtual file system (VMFS) is set for each of the storage volumes configured on the VMware host. You must choose a VMFS block size based on the largest virtual disk size hosted on the VMware host. Once you configure the VMFS block size, you cannot change it without reformattting the VMFS partitions. Your VMware VMFS block size should be based on the size of the largest virtual disk:
  - 1 MB—256 GB
  - 2 MB—512 GB
  - 4 MB—1 TB
  - 8 MB—2 TB
Ensure that you have read and performed the task described in Creating New Virtual File Size, page 1-5.

- Do not choose VMware thin provisioning as a storage type. This release of the Cisco ISE software does not support using VMware thin provisioning as a storage type on any of the supported VMware servers. Thin provisioning is not a default setting and Cisco advises against choosing the check box for thin provisioning in Step 13 (as shown in Figure 1-13).

- If you are enabling the Profiler service, ensure that you have read and performed the tasks described in Configuring VMware Server Interfaces for the Cisco ISE Profiler Service, page 1-6.

Creating New Virtual File Size

To create a new virtual file size, perform the following steps:

**Step 1** Choose Configuration > Storage > Add Storage Wizard.

You can find the Add Storage wizard at the upper-right corner of the configuration window.

**Step 2** From the Storage Type drop-down list, choose Disk/LUN and click Next.

**Step 3** Choose 200 GB for disk space size, choose 2 MB as the VMFS block size, and click Next.

100 GB is the minimum disk space size that is required for installing VMware with Cisco ISE. However, Cisco ISE will only use up to a maximum of 600 GB even if you assign extra space in your VMware system. The value that you set should be from 100 to 600 GB, depending on your deployment.
Chapter 1      Installing Cisco ISE in a VMware Virtual Machine

Configuring a VMware ESX or ESXi Server

Note
It is important to note that the VMware virtual file system (VMFS) is set for each of the storage volumes configured in the VMware host. This means that your choice of the VMFS block size will need to take into account the largest virtual disk sizes hosted on the VMware host. Once the block size is set it cannot be changed without having to reformat the VMFS partitions.

If you specify the default VMFS 1-MB block size, you will not be able to create a 600-GB disk space for your virtual machine on the VMware host. Only by specifying a VMFS block size of 2 MB when the VMFS file system is being created, will you be able to configure up to 600 GB of disk space for your virtual machine.

Step 4 Click Finish.
The new VMware system with a 200-GB virtual disk size and a 2-MB block size is created successfully.

Step 5 Verify the new file size, choose Configuration > Memory, and click Properties.
Figure 1-2 displays the properties of a disk space created with the name ds1.

Figure 1-2  Disk Space Properties Window

Configuring VMware Server Interfaces for the Cisco ISE Profiler Service

To configure the VMware server interfaces to support the collection of SPAN or mirrored traffic to a dedicated probe interface for the Cisco ISE Profiler service, perform the following steps:

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 under the Security tab, check the Promiscuous Mode check box.
**Step 3** In the adjacent drop-down list, choose **Accept**, and click **OK**.

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

*Figure 1-3 VMNetwork Properties Window*

---

**Configuring the VMware Server**

This section describes how to configure VMware servers by using the VMware vSphere Client.

**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**.

The New Virtual Machine Wizard appears.

**Step 3** In the Configuration dialog box, choose **Custom** as the VMware configuration, as shown in *Figure 1-4*, and click **Next**.
Figure 1-4  Virtual Machine Configuration Dialog Box

The Name and Location dialog box appears (see Figure 1-5).

Step 4  Enter a name that you want for referencing the VMware system, and click Next.

Figure 1-5  Name and Location Dialog Box

Tip  Use the hostname that you want to use for your VMware host.
Chapter 1 Installing Cisco ISE in a VMware Virtual Machine

Configuring a VMware ESX or ESXi Server

The Datastore dialog box appears (see Figure 1-6).

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

*Figure 1-6 Datastore Dialog Box*

The Virtual Machine Version dialog box appears.

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

The Guest Operating System dialog box appears (see Figure 1-7).

**Step 7** Choose **Linux** and **Red Hat Enterprise Linux 5 (32-bit)** from the Version drop-down list.
Step 8 From the Number of Virtual Processors drop-down list, choose 4. Click Next.
In some versions of ESX server, the following screen appears. Choose 2 from the Number of virtual sockets and the Number of cores per virtual socket drop-down list (see Figure 1-9). Click Next.

**Figure 1-9 Number of Virtual Sockets and Cores Dialog Box**

The Memory Configuration dialog box appears (see Figure 1-10).

**Step 9** Enter a value based on the recommendations in Table 1-1, and click Next.

**Figure 1-10 Memory Configuration Dialog Box**

The Network Interface Card (NIC) Configuration dialog box appears (see Figure 1-11).

**Step 10** Choose a NIC and Adapter, and click Next.
The SCSI controller dialog box appears.

**Step 11** Choose an SCSI controller and click **Next**.

The Select a Disk dialog box appears (see Figure 1-12).

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

![Figure 1-11 NIC Configuration Dialog Box](image1)

![Figure 1-12 Select a Disk](image2)
The Virtual Disk Size and Provisioning Policy dialog box appears.

**Step 13** Do not check the *Allocate and commit space on demand* (Thin Provisioning) check box and *Support clustering features such as Fault Tolerance* check box in the Disk Provisioning dialog box (see Figure 1-13). Click Next to continue.

*Figure 1-13   Disk Provisioning Dialog Box* 

The Advanced Options dialog box appears.

**Step 14** Choose the Advanced Options, and click Next.

The Ready to Complete New Virtual Machine dialog box appears (see Figure 1-14).

**Step 15** Verify the configuration details, such as Name, Guest OS, Virtual CPU, Memory, and Virtual Disk Size of the newly created VMware system.
Preparing a VMware System for Cisco ISE Software Installation

After configuring the VMware system, you are ready to install the Cisco ISE software. To install the Cisco ISE software from your Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, you need to configure the VMware system to boot from this Cisco ISE DVD. This requires that the VMware system be configured with a virtual DVD drive to boot from the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD.

You can do this by using different methods that are dependent upon your network environment. See Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD, page 1-14 to configure the VMware system by using the DVD drive of your VMware ESX server host.

Preparing a VMware System for Cisco ISE Software Installation

After configuring the VMware system, you are ready to install the Cisco ISE software. To install the Cisco ISE software from your Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, you need to configure the VMware system to boot from this Cisco ISE DVD. This requires that the VMware system be configured with a virtual DVD drive to boot from the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD.

You can do this by using different methods that are dependent upon your network environment. See Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD, page 1-14 to configure the VMware system by using the DVD drive of your VMware ESX server host.

Configuring a VMware System Using the Cisco Identity Services Engine ISE Software DVD

This section describes how to configure a VMware system to boot from the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD by using the DVD drive of the VMware ESX server host.
To configure the VMware system by using the DVD drive, complete the following steps:

---

**Step 1**

In the VMware Infrastructure Client, highlight the newly created VMware system, and choose **Edit Virtual Machine Settings**.

The Virtual Machine Properties window appears. **Figure 1-15** displays the properties of a VMware system created with the name Cisco ISE Release 1.0.

**Figure 1-15  Virtual Machine Properties Dialog Box**

---

**Step 2**

In the Virtual Machine Properties dialog box, choose **CD/DVD Drive 1**.

The CD/DVD Drive1 properties dialog box appears.

**Step 3**

Choose the **Host Device** option, and from the drop-down list, choose your DVD host device.

**Step 4**

Choose the **Connect at Power On** option, and click **OK** to save your settings.

You can now use the DVD drive of the VMware ESX server to install the Cisco ISE software.

---

When you complete the configuration, click the **Console** tab, right-click **VM** in the left pane, choose **Power**, and choose **Reset** to restart the VMware system.
Installing the Cisco ISE Software on a VMware System

This section describes the installation process for the Cisco ISE software on a VMware.

To install the Cisco ISE software on a VMware system, complete the following steps:

Step 1
Log into the VMware Infrastructure Client.

Step 2
Ensure that Universal Time Coordinated (UTC) is set in BIOS:

- If the VMware system is turned on, turn the system off.
- Turn on the VMware system.
- Press F1 to enter the BIOS Setup mode.
- Using the arrow key, navigate to Date and Time and press Enter.
- Enter the time for your appliance to the UTC/Greenwich Mean Time (GMT) time zone.

Note
We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

- Press Esc to exit to the main BIOS menu.
- Press Esc to exit from the BIOS Setup mode.

Note
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 3
Insert the Cisco ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD into the VMware ESX host CD/DVD drive, and turn on the virtual machine.

Note
If you do not have access to this DVD, you can download the Cisco ISE Release 1.1.x software from the Cisco Software Download Site at http://software.cisco.com/download/navigator.html?a=a&i=rpm. You will be required to provide your Cisco.com credentials.

When the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD boots, the console displays:

Welcome to Cisco ISE
To boot from the hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Monitor/Keyboard)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot: 1

You can choose either the monitor and keyboard port, or the console port to perform the initial setup.

Step 4
At the system prompt, type 1 to choose a monitor and keyboard port, or type 2 to choose a console port, and press Enter.
This starts the installation of the Cisco ISE software on the VMware system.

**Note**

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 5** At the system prompt, type `setup`, and press **Enter**.

The Setup Wizard appears and guides you through the initial configuration. For more information on the setup process, see Understanding the Setup Program Parameters, page 1-3.

---

**Connecting to the Cisco ISE VMware Server Using Serial Console**

To connect to Cisco ISE VMware server using the serial console, complete the following steps:

**Step 1** Power off the particular VMware server (for example ISE-120).

**Step 2** Right click on the VMware server and choose **Edit**.

**Step 3** Choose the **Hardware** tab and click **Add**.
Step 4  Choose **Serial Port** and click **Next**.

![Add Hardware window](image1)

Step 5  For Serial Port Output choose **Use physical serial port on the host**. Click **Next**.

![Add Hardware window](image2)
Step 6  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 7  Click Next.

Step 8  Check the device status. It will be shown as Connected.
Preparing to Install the Cisco ISE 3300 Series Hardware

This appendix briefly describes safety guidelines, site requirements, and Ethernet connector and console port guidelines that you must observe before installing the Cisco Identity Services Engine (ISE) 3300 Series appliance. This information is provided in the following topics:

- Safety Guidelines, page 1-1
- Preparing Your Site for Installation, page 1-6
- Ethernet Connector and Console Port Guidelines, page 1-15

Safety Guidelines

Before you begin installing the Cisco ISE 3300 Series appliance, review the safety guidelines in this appendix and Rack-Mounting Configuration Guidelines, page 1-1 to avoid injuring yourself or damaging the equipment.

In addition, before replacing, configuring, or maintaining the appliance, review the safety warnings that are listed in Related Documentation, page 5. This section contains the following topics:

- General Precautions, page 1-1
- Safety with Equipment, page 1-3
- Safety with Electricity, page 1-3
- Preventing ESD Damage, page 1-5
- Lifting Guidelines, page 1-5

General Precautions

Observe the following general precautions for using and working with your appliance:

- Observe and follow service markings. Do not service any Cisco product except as explained in your appliance documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock. Components that are inside these compartments should be serviced only by an authorized service technician.
Appendix 1      Preparing to Install the Cisco ISE 3300 Series Hardware

Safety Guidelines

If any of the following conditions occur, unplug the product from the electrical outlet and replace
the part, or contact your authorized service provider:

– The power cable, extension cord, or plug is damaged.
– An object has fallen into the product.
– The product has been exposed to water.
– The product has been dropped or damaged.
– The product does not operate correctly when you follow the operating instructions.

Keep your appliance away from radiators and heat sources. Also, do not block cooling vents.

Do not spill food or liquids on your appliance, and never operate the product in a wet environment.

Do not push any objects into the openings of your appliance. Doing so can cause fire or electric
shock by shorting out interior components.

Use the product only with other equipment that is approved by Cisco.

Allow the product to cool before removing covers or touching internal components.

Use the correct external power source. Operate the product only from the type of power source that
is indicated on the electrical ratings label of the product. If you are not sure of the type of power
source required, consult your service representative or local power company.

Use only approved power cables. If you have not been provided with a power cable for your
appliance or for any AC-powered option that is intended for your appliance, purchase a power cable
that is approved for use in your country.

The power cable must be rated for the product and for the voltage and current that is marked on the
product’s electrical ratings label. The voltage and current rating of the cable should be greater than
the ratings that are marked on the product.

To help prevent electric shock, plug the appliance and power cables into properly grounded
electrical outlets. These cables are equipped with three-prong plugs to help ensure proper
grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use
an extension cord, use a three-wire cord with properly grounded plugs.

Observe extension cord and power strip ratings. Make sure that the total ampere rating of all
products that are plugged into the extension cord or power strip does not exceed 80 percent of the
extension cord or power strip ampere ratings limit.

Do not use appliance voltage converters, or kits that are sold for appliances with your product.

To help protect your appliance from sudden, transient increases and decreases in electrical power,
use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).

Position cables and power cords carefully; route cables and the power cord and plug so that they
cannot be stepped on or tripped over. Be sure that nothing rests on your appliance cables or
power cord.

Do not modify power cables or plugs. Consult a licensed electrician or your power company for site
modifications. Always follow your local or national wiring rules.
Safety with Equipment

The following guidelines help ensure your safety and protect the equipment. However, this list does not include all potentially hazardous situations, so be alert.

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

- Always disconnect all power cords and interface cables before moving the appliance.
- Never assume that power is disconnected from a circuit; *always* check.
- Keep the appliance chassis area clear and dust-free before and after installation.
- Keep tools and assembly components away from walk areas where you or others could trip over them.
- Do not work alone if potentially hazardous conditions exist.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not wear loose clothing that may get caught in the appliance chassis.
- Wear safety glasses when working under conditions that may be hazardous to your eyes.

Safety with Electricity

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors.** Statement 1021

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12
Safety Guidelines

**Warning**

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Statement 1001

**Warning**

This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Statement 39

**Warning**

When installing or replacing the unit, the ground connection must always be made first and disconnected last.

Statement 1046

Follow these guidelines when working on equipment powered by electricity:

- Locate the room’s emergency power-off switch. Then, if an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before performing the following tasks:
  - Working on or near power supplies
  - Installing or removing an appliance
  - Performing most hardware upgrades
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Never assume that power is disconnected from a circuit; always check.
- Never perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never work alone when potentially hazardous conditions exist.
- If an electrical accident occurs, proceed as follows:
  - Use caution, and do not become a victim yourself.
  - Turn off power to the appliance.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing, external cardiac compressions, or other medical attention; then take appropriate action.

In addition, use the following guidelines when working with any equipment that is disconnected from a power source but still connected to telephone wiring or network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
Preventing ESD Damage

ESD can damage equipment and impair electrical circuitry. ESD can occur when electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow ESD-prevention procedures when removing and replacing modules:

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your appliance. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.
- Ensure that the Cisco ISE 3300 Series appliance is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the appliance to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the appliance.

Caution

For the safety of your equipment, periodically check the resistance value of the antistatic wrist strap. It should be between 1 and 10 Mohm.

Lifting Guidelines

The Cisco ISE 3300 Series appliance weighs between 15 lb (9.071 kg) and 33 lb (14.96 kg) depending on what hardware options are installed in the appliance. The appliance is not intended to be moved frequently. Before you install the appliance, ensure that your site is properly prepared so that you can avoid having to move the appliance later to accommodate power sources and network connections.

Whenever you lift the appliance or any heavy object, follow these guidelines:

- Always disconnect all external cables before lifting or moving the appliance.
- Ensure that your footing is solid, and balance the weight of the object between your feet.
- Lift the appliance slowly; never move suddenly or twist your body as you lift.
- Keep your back straight and lift with your legs, not your back. If you must bend down to lift the appliance, bend at the knees, not at the waist, to reduce the strain on your lower back muscles.
- Lift the appliance from the bottom; grasp the underside of the appliance exterior with both hands.
Preparing Your Site for Installation

This section contains information about site planning, site preparation, and preparing to install the Cisco ISE 3300 Series appliance in the following topics:

- Site Planning, page 1-6
- Unpacking and Checking the Contents of Your Shipment, page 1-11
- Required Tools and Equipment, page 1-13
- Installation Checklist, page 1-14
- Creating a Site Log, page 1-14

Before you install the Cisco ISE 3300 Series appliance, complete the following steps:

Step 1 Prepare the site (see Site Planning, page 1-6) and review any installation plans or deployment site survey documentation.

Step 2 Unpack and inspect the appliance.

Step 3 Gather the tools and test equipment that are required to properly install the appliance.

Site Planning

Warning This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

Statement 1017

Typically, you should have prepared the installation site beforehand. As part of your preparation, obtain a floor plan of the site and the equipment rack where the Cisco ISE 3300 Series appliance will be housed.

Determine the location of any existing appliances and their interconnections, including communications and power. Follow the airflow guidelines (see Airflow Guidelines, page 1-8) to ensure that adequate cooling air is provided to the appliance.

All personnel who are involved in the installation of the appliance, including installers, engineers, and supervisors, should participate in the preparation of a method of procedure (MOP) for approval by the customer. For more information, see Method of Procedure, page 1-10.

The following sections provide the site requirement guidelines that you must consider before installing the appliance:

- Rack Installation Safety Guidelines, page 1-7
- Site Environment, page 1-8
- Airflow Guidelines, page 1-8
- Temperature and Humidity Guidelines, page 1-9
- Power Considerations, page 1-9
- Method of Procedure, page 1-10
Rack Installation Safety Guidelines

The Cisco ISE 3300 Series appliance can be mounted in most four-post telephone company (telco-type), 19-inch equipment racks that comply with the EIA standard for equipment racks (EIA-310-D). The distance between the center lines of the mounting holes on the two mounting posts must be 18.31 inches +/- 0.06 inch (46.50 cm +/- 0.15 cm). The rack-mounting hardware that is included with the appliance is suitable for most 19-inch equipment racks or telco-type frames.

Note Cisco strongly recommends using four-post racks whenever possible, but your rack must have at least two posts that provide mounting flanges for mounting an appliance.

Figure 1-1 shows a couple of common examples of four-post equipment racks.

**Figure 1-1  Four-Post Equipment Rack Types**

![Four-Post Equipment Rack Types](image)

**Four-Post (Partially-Enclosed) Rack**

Image “1” in Figure 1-1 shows a freestanding, partially-enclosed rack with two mounting posts in the front and two more at the rear. The Cisco ISE 3300 Series appliance may be installed in this type of enclosed rack, because the appliance only requires an unobstructed flow of cooling air into the front of the chassis and pushed out of the rear to maintain acceptable operating temperatures for its internal components.

**Four-Post (Open) Rack**

Image “2” Figure 1-1 shows a freestanding, four-post open rack with two mounting posts in front and two mounting posts at the back. The mounting posts in this type of rack are often adjustable so that you can position the rack-mounted unit within the depth of the rack rather than flush-mount it with the front of the rack.

Before installing your Cisco ISE 3300 Series appliance in a rack, review the following guidelines:

- Two or more people are required to install the appliance in a rack.
- Ensure that the room air temperature is below 95°F (35°C).
- Do not block any air vents; usually, 6 inches (15 cm) of space provides proper airflow.
• Plan the appliance installation starting from the bottom of the rack.
• Do not extend more than one appliance out of the rack at the same time.
• Connect the appliance to a properly grounded outlet.
• Do not overload the power outlet when installing multiple devices in the rack.
• Do not place any object weighing more than 110 lb (50 kg) on top of rack-mounted devices.

Site Environment

The location of your appliance and the layout of your equipment rack or wiring room are extremely important considerations for proper operation. Equipment that is placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. Plan for access to front panel and rear panel of the appliance.

The following precautions will help you plan an acceptable operating environment for your appliance and will help you avoid environmentally caused equipment failures:

• Ensure that the room in which your appliance operates has adequate circulation. Electrical equipment generates heat. Without adequate circulation, ambient air temperature may not cool equipment to acceptable operating temperatures. For more information, see Airflow Guidelines, page 1-8.
• Ensure that the site of the rack includes provisions for source AC power, grounding, and network cables.
• Allow sufficient space to work around the rack during the installation. You need:
  – At least 3 feet (9.14 m) adjacent to the rack to move, align, and insert the appliance.
  – At least 24 inches (61 cm) of clearance in front of and behind the appliance for maintenance after installation.
• To mount the appliance between two posts or rails, the usable aperture (the width between the inner edges of the two mounting flanges) must be at least 17.7 inches (45.0 cm).

Note

The rack-mount kit does not include a two-post equipment rack.

• Use appropriate strain-relief methods to protect cables and equipment connections.
• To avoid noise interference in network interface cables, do not route them directly across or along power cables.
• Always follow ESD-prevention procedures as described in Preventing ESD Damage, page 1-5 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

Airflow Guidelines

To ensure adequate airflow through the equipment rack, we recommend that you maintain a clearance of at least 6 inches (15.24 cm) at the front and the rear of the rack. If airflow through the equipment rack and the appliances that occupy it is blocked or restricted, or if the ambient air that is being drawn into the rack is too warm, the temperature within the equipment rack can get too high and the appliance(s) may overheat.
The site should also be as dust-free as possible. Dust tends to clog the appliance fans, which reduces the flow of cooling air through the equipment rack and the appliances that occupy it. This type of airflow reduction increases the risk that the temperature will get too high and the appliance(s) may overheat.

Additionally, the following guidelines will help you plan your equipment rack configuration:

- Besides airflow, you must allow clearance around the rack for maintenance.
- When mounting an appliance in an open rack, ensure that the rack frame does not block the front intakes or the rear exhausts.

### Temperature and Humidity Guidelines

Table 1-1 lists the operating and nonoperating environmental site requirements for the Cisco ISE 3300 Series appliance. The appliance normally operates within the ranges that are listed; however, a temperature measurement that approaches a minimum or maximum parameter indicates a potential problem.

Maintain normal operation by anticipating and correcting environmental anomalies before they approach critical values by properly planning and preparing your site before you install the appliance.

#### Table 1-1 Operating and Nonoperating Environmental Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature, ambient operating</td>
<td>50°F (10°C)</td>
<td>95°F (35°C)</td>
</tr>
<tr>
<td>Temperature, ambient nonoperating and storage</td>
<td>-40°F (°C)</td>
<td>158°F (70°C)</td>
</tr>
<tr>
<td>Humidity, ambient (noncondensing) operating</td>
<td>10%</td>
<td>90%</td>
</tr>
<tr>
<td>Humidity, ambient (noncondensing) nonoperating and storage</td>
<td>5%</td>
<td>95%</td>
</tr>
<tr>
<td>Vibration, operating</td>
<td>5–500 Hz, 2.20 g RMS random</td>
<td>—</td>
</tr>
</tbody>
</table>

### Power Considerations

You configure the Cisco ISE 3300 Series appliance with AC-input power only. Ensure that all power connections conform to the rules and regulations in the National Electrical Codes, as well as local codes. While planning power connections to your appliance, the following precautions and recommendations must be followed:

- Check the power at your site before installation and periodically after installation to ensure that you are receiving clean power (free of spikes and noise). Install a power conditioner if necessary.

- The AC power supply includes the following features:
  - Autoselect feature for 110 V or 220 V operation.
  - An electrical cord for all appliances. (A label near the power cord indicates the correct voltage, frequency, current draw, and power dissipation for the appliance.)

**Warning** This product relies on the building installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15 Amp U.S. (240 VAC, 10 Amp international) is used on the phase conductors (all current-carrying conductors). Statement 13

- Install proper grounding to your host equipment rack to avoid damage from lightning and power surges.
Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

- Ensure that the AC-input power supply operates on input voltage and frequency within the ranges of 100 to 240 VRMS and 50 to 60 Hz without the need for operator adjustments. Table 1-2 provides additional information on electrical inputs.

**Table 1-2 Electrical Input Specifications**

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sine-wave input</td>
<td>50 Hz</td>
<td>60 Hz</td>
</tr>
<tr>
<td>Input voltage low range</td>
<td>100 VAC</td>
<td>127 VAC</td>
</tr>
<tr>
<td>Input voltage high range</td>
<td>200 VAC</td>
<td>240 VAC</td>
</tr>
<tr>
<td>Approximate input kilovolt-amperes (kVA)</td>
<td>0.102 kVA</td>
<td>0.55 kVA</td>
</tr>
</tbody>
</table>

**Method of Procedure**

As described previously, part of your preparation includes reviewing installation plans or MOPs. A MOP is a preinstallation checklist or list of tasks, guidelines, or considerations that need to be addressed and agreed upon before you proceed with the installation. The following example MOP serves as a guideline:

---

**Step 1** Assign personnel.

**Step 2** Determine protection requirements for personnel, equipment, and tools.

**Step 3** Evaluate potential hazards that may affect service.

**Step 4** Schedule time for installation.

**Step 5** Determine any space requirements.

**Step 6** Determine any power requirements.

**Step 7** Identify any required procedures or tests.

**Step 8** In an equipment plan, make a preliminary decision that locates each Cisco ISE 3300 Series appliance that you plan to install.

**Step 9** Read this hardware installation guide.

**Step 10** Verify the list of replaceable parts for installation (screws, bolts, washers, and so on) so that the parts are identified.

**Step 11** Check the required tools list to make sure the necessary tools and test equipment are available. For more information, see Required Tools and Equipment, page 1-13.

**Step 12** Perform the installation.
Unpacking and Checking the Contents of Your Shipment

The shipping package for the Cisco ISE 3300 Series appliance is designed to reduce the possibility of product damage that is associated with routine material handling that is experienced during shipment. To reduce the potential for damage to the product, transport the appliance in its original Cisco packaging. Failure to do so may result in damage to the appliance. Also, do not remove the appliance from its shipping container until you are ready to install it.

The appliance, cables, and any optional equipment that you ordered may be shipped in more than one container. A Notes section has been provided to record damaged or missing items. Figure 1-2 displays the shipment items with the Cisco ISE 3300 Series appliance.

Note
Do not discard the packaging materials that are used in shipping your Cisco ISE 3300 Series appliance. You will need the packaging materials in the future if you move or ship your appliance.

Figure 1-2   Items Shipped with the Cisco ISE 3300 Series Appliance

Inspect all items for shipping damage. If anything appears to be damaged, or if you encounter problems installing or configuring your appliance, contact your customer service representative.

Note
The rack-mount kit does not include a two-post equipment rack.

Cisco Information Packet and Warranty

The Cisco Information Packet provides warranty, service, and support information. To access and download the Cisco Information Packet and your warranty and license agreements from Cisco.com, point your browser at the following location:


The Warranties and License Agreements page appears.

To read the Cisco Information Packet, complete the following steps:

Step 1
Click the Information Packet Number field, and ensure that the part number 78-5235-03D0 is highlighted.
Step 2 Choose the language in which you would like to read the document.

Step 3 Click Go.

The Cisco Limited Warranty and Software License page from the Information Packet appears.

Step 4 Read the document online, or click the PDF icon to download and print the document.

You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from the Adobe website.

To read translated and localized warranty information about your product, complete the following steps:

Step 1 Enter this part number in the Warranty Document Number field:
78-5236-01C0

Step 2 Choose the language in which you would like to read the document.

Step 3 Click Go.

The Cisco warranty page appears.

Step 4 Review the document online, or click the PDF icon to download and print the document in PDF.

You can also contact the Cisco Service and Support website for assistance at:

Duration of Hardware Warranty
Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware
Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the Return Materials Authorization (RMA) request. Actual delivery times can vary depending on the customer location.

Note Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive an RMA Number
Contact the company from which you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.
Complete the following information, and keep it for reference:

<table>
<thead>
<tr>
<th>Product Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company product was purchased from</td>
<td></td>
</tr>
<tr>
<td>Company telephone number/website location</td>
<td></td>
</tr>
<tr>
<td>Product model number</td>
<td></td>
</tr>
<tr>
<td>Product serial number¹</td>
<td></td>
</tr>
<tr>
<td>Maintenance contact number</td>
<td></td>
</tr>
</tbody>
</table>

¹. See the “Cisco ISE 3300 Series Appliance Hardware Summary” section on page 1-1, “Cisco ISE 3355 Serial Number Location” section on page 1-8, “Cisco ISE 3395 Serial Number Location” section on page 1-12, and the “Locating Appliance Serial Numbers” section on page 1-5 for more information.

**Required Tools and Equipment**

**Caution**
The fastener pack in the rack-mount kit contains eight rack screws. You must check these screws to ensure that they are the appropriate size for the holes in your rack. Using the wrong-sized screws for your threaded rack holes can damage the rack.

You need the following tools and equipment to install the Cisco ISE 3300 Series appliance in a four-post rack:

**Warning**
Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Statement 1030

- ESD-preventive cord and wrist strap.
- Number 2 Phillips screwdriver.
- Flat-blade screwdrivers (small, 3/16-in [0.476 cm] and medium, 1/4-inch [0.625 cm]) to remove the cover if you are upgrading memory or other components.
- Rack-mount kit. For more information on kit contents, see Using a Four-Post Rack-Mount Hardware Kit, page 1-3.
- Cables for connection to the LAN ports (depending on the configuration).
- Ethernet switch for connection to the Ethernet (LAN) port or ports.

You must have either of the following for the initial configuration of the Cisco ISE 3300 Series appliance:

- USB keyboard and VGA monitor.
  or
- Console terminal (an ASCII terminal or a PC that is running terminal-emulation software) that is configured for 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.
- Console cable for connection to the serial (console) port. A null-modem cable is recommended.
Installation Checklist

To assist you with your installation and to provide a historical record of what was done, and by whom, use the following installation checklist. Make a copy of this checklist and mark the entries as you complete each task.

When the checklist is complete, include a copy of it for each Cisco ISE 3300 Series appliance in your site log along with other records for your new appliance. (See Creating a Site Log, page 1-14 for information about creating a site log.)

<table>
<thead>
<tr>
<th>Task</th>
<th>Verified by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation checklist copied</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background information placed in site log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site power voltages verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation site power check completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required tools availability verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional equipment availability verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ISE 3300 Series appliance received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Information Packet publication received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appliance components verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial electrical connections established</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASCII terminal (for local configuration) verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signal distance limits verified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Startup sequence steps completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial operation verified</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Creating a Site Log

You can maintain a site log that serves as a record of all installation, maintenance, upgrade, replacement, and changes that are made to the Cisco ISE 3300 Series appliance. Keep the log in an accessible place near the appliance so that anyone who performs tasks has access to it.

Use the installation checklist (see Installation Checklist, page 1-14) to verify the steps in the installation and maintenance of your appliance. Site log entries might include the following:

- Installation progress—Make a copy of the appliance installation checklist, and insert it into the site log. Make entries as you complete each task.

- Upgrade, removal, and maintenance procedures—Use the site log as a record of ongoing appliance maintenance and expansion history. Each time a task is performed on the appliance, update the site log to reflect the following information:
  - Installation of new adapter cards
  - Removal or replacement of adapter cards and other upgrades
  - Configuration changes
Ethernet Connector and Console Port Guidelines

This section provides the following guidelines for the Ethernet connector and asynchronous serial console port for the Cisco ISE 3300 Series appliances:

- Each Cisco ISE 3300 Series appliance provides an Ethernet connector on the rear panel, and the Gigabit Ethernet 0 port uses unshielded twisted-pair (UTP) cabling (we recommend using Category 6 UTP cable). The maximum segment distance is 328 feet (100 meters).
  
  UTP cables look like the cables that are used for ordinary telephones. However, UTP cables meet specific electrical standards that telephone cables do not meet (these UTP cables are not included in the installation package).

- Each Cisco 3300 Series appliance provides an asynchronous serial console port on the rear panel that enables you to access the appliance locally (using a console terminal). It is important that you verify and use the proper cabling type before attempting to connect a console terminal—either an ASCII terminal or a PC running terminal-emulation software—to the console port.

Caution

To help prevent a potential network security threat, Cisco strongly recommends physically disconnecting from the Cisco ISE console management port when you are not using it. For more details, see http://seclists.org/fulldisclosure/2011/Apr/55, which applies to the Cisco ISE, Cisco NAC Appliance, and Cisco Secure ACS hardware platforms.

Note

The console cable is not included with the Cisco ISE 3300 Series appliance.
Preparing to Install the Cisco SNS-3400 Series Hardware

This appendix briefly describes the safety guidelines, site requirements, and guidelines that you must observe before installing the Cisco SNS-3400 Series appliances. This appendix contains the following sections:

- Unpacking and Inspecting the Server, page 1-1
- Safety Guidelines, page 1-2
- Installing the Cisco SNS-3400 Series Appliance in a Rack, page 1-3

Unpacking and Inspecting the Server

This section provides information on how you can prepare your site for safely installing the Cisco SNS-3400 series appliance.

Caution

When handling internal server components, wear an ESD strap and handle modules by the carrier edges only.

Tip

Keep the shipping container in case the server requires shipping in the future.

Note

The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

To inspect the shipment, follow these steps:

Step 1

Remove the server from its cardboard container and save all packaging material.

Step 2

Compare the shipment to the equipment list provided by your customer service representative and Figure 1-1. Verify that you have all items.

Step 3

Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

Step 4

Invoice number of shipper (see the packing slip)
Step 5  Model and serial number of the damaged unit
Step 6  Description of damage
Step 7  Effect of damage on the installation

Figure 1-1  Shipping Box Contents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server</td>
</tr>
<tr>
<td>2</td>
<td>Power cord (optional, up to two)</td>
</tr>
<tr>
<td>3</td>
<td>Documentation</td>
</tr>
<tr>
<td>4</td>
<td>KVM cable</td>
</tr>
</tbody>
</table>

Safety Guidelines

Before you install, operate, or service a Cisco SNS-3400 series appliance, review the http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/regulatory/compliance/csacsresi.html for important safety information.

**Warning**  IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071
Installing the Cisco SNS-3400 Series Appliance in a Rack

When you are installing a server, use the following guidelines:

- Plan your site configuration and prepare the site before installing the server. See the Cisco UCS Site Preparation Guide for the recommended site planning tasks.
- Ensure that there is adequate space around the server to allow for servicing the server and for adequate airflow. The airflow in this server is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the Maintaining the Cisco ISE 3300 Series Applliance.
- Ensure that the cabinet or rack meets the requirements listed in the “Rack Requirements” section on page 1-4.
- Ensure that the site power meets the power requirements listed in the Maintaining the Cisco ISE 3300 Series Applliance. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Caution

Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

Installing the Cisco SNS-3400 Series Appliance in a Rack

This section describes how to mount the Cisco SNS-3400 series appliance on a rack and contains the following topics:

- Rack Requirements, page 1-4
- Equipment Requirements, page 1-4
- Slide Rail Adjustment Range, page 1-4
- Installing the Server In a Rack, page 1-4
Appendix 1 Preparing to Install the Cisco SNS-3400 Series Hardware

Rack Requirements

This section provides the requirements for the standard open racks.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square .38-inch (9.6 mm), round .28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

Equipment Requirements

The slide rails supplied by Cisco Systems for this server do not require tools for installation. The inner rails (mounting brackets) are pre-attached to the sides of the server.

Slide Rail Adjustment Range

The slide rails for this server have an adjustment range of 24 to 36 inches (610 to 914 mm).

Installing the Server In a Rack

This section describes how to install the server in a rack.

⚠️ Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

To install the slide rails and the server into a rack, follow these steps:

Step 1

Open the front securing latch (see Figure 1-2). The end of the slide-rail assembly marked “FRONT” has a spring-loaded securing latch that must be open before you can insert the mounting pegs into the rack-post holes.

a. On the rear side of the securing-latch assembly, hold open the clip marked “PULL.”

b. Slide the spring-loaded securing latch away from the mounting pegs.

c. Release the clip marked “PULL” to lock the securing latch in the open position.
Appendix 1 Preparing to Install the Cisco SNS-3400 Series Hardware

Installing the Cisco SNS-3400 Series Appliance in a Rack

Figure 1-2 Front Securing Latch

| 1 | Clip marked “PULL” on rear of assembly |
| 2 | Front mounting pegs                |
| 3 | Spring-loaded securing latch on front of assembly |

Step 2 Install the slide rails onto the rack:

a. Position a slide-rail assembly inside the two left-side rack posts (see Figure 1-3).

   Use the “FRONT” and “REAR” markings on the slide-rail assembly to orient the assembly correctly with the front and rear rack posts.

b. Position the front mounting pegs so that they enter the desired front rack-post holes from the front.

   The mounting pegs that protrude through the rack-post holes are designed to fit round or square holes, or smaller #10-32 round holes when the mounting peg is compressed. If your rack has #10-32 rack-post holes, align the mounting pegs with the holes and then compress the spring-loaded pegs to expose the #10-32 inner peg.

c. Expand the length-adjustment bracket until the rear mounting pegs protrude through the desired holes in the rear rack post.

   Use your finger to hold the rear securing latch open when you insert the rear mounting pegs to their holes. When you release the latch, it wraps around the rack post and secures the slide-rail assembly.
Step 3

Insert the server into the slide rails:

\[\text{Note}\] The inner rails are pre-attached to the sides of the server at the factory. You can order replacement inner rails if these are damaged or lost (Cisco PID UCSC-RAIL1-I).

a. Align the inner rails that are pre-attached to the server sides with the front ends of the empty slide rails.
b. Push the server into the slide rails until it stops at the internal stops.
c. Push in the plastic release clip on each inner rail (labelled PUSH), and then continue pushing the server into the rack until its front latches engage the rack posts.

Step 4

Attach the (optional) cable management arm (CMA) to the rear of the slide rails:

\[\text{Note}\] The CMA is designed for mounting on either the right or left slide rails. These instructions describe an installation to the rear of the right slide rails, as viewed from the rear of server.

a. Slide the plastic clip on the inner CMA arm over the flange on the mounting bracket that attached to the side of the server. See Figure 1-4.

\[\text{Note}\] Whether you are mounting the CMA to the left or right slide rails, be sure to orient the engraved marking, “UP” so that it is always on the upper side of the CMA. See Figure 1-4.
b. Slide the plastic clip on the outer CMA arm over the flange on the slide rail. See Figure 1-4.

c. Attach the CMA retaining bracket to the left slide rail. Slide the plastic clip on the bracket over the flange on the end of the left slide rail. See Figure 1-4.

**Figure 1-4 Attaching the Cable Management Arm (Rear of Server Shown)**

| Step 5 | Continue with the “Configuring Cisco ISE on the Cisco SNS-3400 Series Appliance Using CIMC” section on page 1-11. |
Installing the Cisco ISE 3300 Series Hardware

This appendix describes how to install your Cisco Identity Services Engine (ISE) 3300 Series appliances and connect any of the three supported appliances (Cisco ISE 3315, Cisco ISE 3355, and Cisco ISE 3395) to the network. This information is contained in the following sections:

- Rack-Mounting Configuration Guidelines, page 1-1
- Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack, page 1-2
- Connecting Cables, page 1-8
- Powering Up the Cisco ISE 3300 Series Appliance, page 1-14

**Warning**
Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Statement 1030

**Warning**
This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.
Statement 1017

Rack-Mounting Configuration Guidelines

Each Cisco ISE 3300 Series appliance has a set of rack handles (installed at the factory). You will use these handles when installing the appliance in a four-post rack. You can front (flush) mount or mid-mount the appliance in a 19-inch (48.3-cm) equipment rack that conforms to the four-post rack specification.

**Note**
The inside width of the rack must be 17.5 inches (44.45 cm).

The first task that you need to perform is to mount the appliance in the brackets. After the appliance is installed in the rack, it requires one EIA 1.75-inch (4.4-cm) vertical mounting space or 1 rack unit (RU) for mounting.

**Caution**
You must leave sufficient clearance in the front and rear of the Cisco ISE 3300 Series appliance to allow for cooling air to be drawn in through the front, circulated through the appliance, and exhausted out the rear of the appliance. For details, see Airflow Guidelines, page 1-8.
Appendix 1      Installing the Cisco ISE 3300 Series Hardware

Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack

The Rack Installation Safety Guidelines, page 1-7 and the following information will help you plan the equipment rack configuration:

- When mounting an appliance in an equipment rack, ensure that the rack is firmly bolted to the floor.
- Because you may install one or more appliances in the rack, ensure that the weight of all the installed appliances does not exceed the weight capacity of the rack or make the rack unstable.

Caution

Some equipment racks are also secured to ceiling brackets because of the weight of the equipment in the rack. For this type of installation, make sure that the rack that you are using to install the appliances is firmly secured to the building structure.

- As recommended in Airflow Guidelines, page 1-8, maintain a 6-inch (15.2-cm) clearance at the front and rear of the appliance to ensure that it maintains an adequate space for air intake and exhaust.
- Avoid installing appliances in an overly congested rack. Air flowing to or from other appliances in the rack might potentially interfere with the normal flow of cooling air through the appliances, and thereby increasing the risk for causing the appliance(s) to overheat.
- Allow at least 24 inches (61 cm) of clearance at the front and rear of the rack for performing any appliance maintenance operations.

Caution

To prevent appliance overheating, never install an appliance in an enclosed rack or in a room that is not properly ventilated or supported by adequate air conditioning.

- Follow your local best practices for cable management. Ensure that cables running to and from appliances do not impede access needed for performing equipment maintenance or upgrades.

Note

The rack-mount hardware kit does not include a two-post equipment rack.

Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack

Warning

When the appliance is installed in a rack and is fully extended on its slide rail, it is possible for the rack to become unstable and tip over, which could cause serious injury. To eliminate the risk of rack instability from extending the rail or in the event of an earthquake, you should affix the rack to the floor.

This section contains information about the following topics:

- Using a Four-Post Rack-Mount Hardware Kit, page 1-3
- Installing the Slide Rails in a Rack, page 1-4
- Installing the Appliance into the Slide Rails, page 1-6
Using a Four-Post Rack-Mount Hardware Kit

Figure 1-1 displays the items that you need to install the Cisco ISE 3300 Series appliance in a four-post rack.

![Figure 1-1 Release Levers on the Slide Rail Hardware](image)

The following table describes the callouts in Figure 1-1.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cable straps</td>
</tr>
<tr>
<td>2</td>
<td>Slide rail</td>
</tr>
<tr>
<td>3</td>
<td>Front of rail</td>
</tr>
<tr>
<td>4</td>
<td>M6 screws</td>
</tr>
<tr>
<td>5</td>
<td>Shipping bracket</td>
</tr>
<tr>
<td>6</td>
<td>Rear of rail</td>
</tr>
</tbody>
</table>

Table 1-1 lists the contents of the rack-mount hardware kit.

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide rails</td>
<td>2</td>
</tr>
<tr>
<td>Cable straps</td>
<td>6</td>
</tr>
<tr>
<td>M6 screws</td>
<td>6</td>
</tr>
</tbody>
</table>
Installing the Slide Rails in a Rack

To install the Cisco ISE 3300 Series appliance in a rack, complete the following steps:

**Step 1** Press on the rail-adjustment bracket on the rear of the slide rail (see Figure 1-2) to prevent the bracket from moving.

**Step 2** Press the adjustment tabs 1 and 2 (see Figure 1-2) and slide the rail-locking carrier toward the front of the slide rail until it snaps into place.

**Step 3** Press the adjustment Tabs 1 and 2 and slide the rail-locking carrier toward the rear of the slide until it snaps into place.

**Figure 1-2 Installing the Slide Rail into the Rack**

The following table describes the callouts in Figure 1-2.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adjustment tab 1</td>
</tr>
<tr>
<td>2</td>
<td>Adjustment tab 2</td>
</tr>
<tr>
<td>3</td>
<td>Rail-adjustment bracket</td>
</tr>
</tbody>
</table>

If you need to adjust the slide-rail length, lift the release tab (see Figure 1-3) and fully extend the rail-adjustment bracket from the rear of the slide rail until it snaps into place.

**Step 4** Align the pins on the rear rail-locking carrier with the holes on the rear mounting flange.

**Step 5** Press the adjustment tab (see Figure 1-3) to secure the rear of the slide rail to the rear mounting flange.

**Note** Ensure that the pins are fully extended through the mounting flange and slide rail.
Appendix 1 Installing the Cisco ISE 3300 Series Hardware

Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack

Figure 1-3 Adjusting the Slide-rail Length

The following table describes the callouts in Figure 1-3.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adjustment tab</td>
</tr>
<tr>
<td>2</td>
<td>Release tab</td>
</tr>
<tr>
<td>3</td>
<td>Pins (not extended through the mounting flange and slide rail)</td>
</tr>
<tr>
<td>4</td>
<td>Pins (extending through the mounting flange and slide rail)</td>
</tr>
</tbody>
</table>

Step 6 Align the pins (see Figure 1-4) on the front rail-locking carrier to the front mounting flange.
If you have adjusted the rail length, push the rail-locking carrier back toward the rear of the slide rail to align the slide rail with the mounting flange.

Step 7 Press the adjustment tab to secure the front of the slide rail to the front mounting flange.

Note Ensure that the pins are fully extended through the mounting flange and the slide rail.

Step 8 Repeat these steps for the other slide rail.
Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack

Figure 1-4  Aligning the Slide Rail with the Mounting Flange

The following table describes the callouts in Figure 1-4.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adjustment tab</td>
</tr>
<tr>
<td>2</td>
<td>Mounting flange</td>
</tr>
<tr>
<td>3</td>
<td>Pins</td>
</tr>
<tr>
<td>4</td>
<td>Pins (extending through the mounting flange and slide rail)</td>
</tr>
<tr>
<td>5</td>
<td>Pins (not extending through the mounting flange and slide rail)</td>
</tr>
</tbody>
</table>

Installing the Appliance into the Slide Rails

To install the Cisco ISE 3300 Series appliance into the slide rails, complete the following steps:

Step 1  Align the server on the slide rails and push it fully into the rack cabinet.

Step 2  Secure the server to the front mounting flanges with the captive thumbscrews (see Figure 1-5).

Note  You must leave the shipping brackets attached to the slide rails unless the shipping brackets impede the server from sliding fully into the rack cabinet. If you need to remove the shipping brackets, see Step 3.
Mounting a Cisco ISE 3300 Series Appliance in a Four-Post Rack

Figure 1-5  Aligning the Server on the Slide Rails

The following table describes the callouts in Figure 1-5.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shipping brackets</td>
</tr>
<tr>
<td>2</td>
<td>Cisco ISE 3300 Series appliance</td>
</tr>
<tr>
<td>3</td>
<td>Thumbscrews</td>
</tr>
</tbody>
</table>

Step 3  Press the release tab (see Figure 1-6) as indicated on the shipping bracket, and remove the shipping bracket from the slide rail.

Step 4  Repeat step 3 for the other shipping bracket. Store the shipping brackets for future use.

Note  You must reinstall the shipping brackets on the slide rails before you transport the rack cabinet with the server installed. To reinstall the shipping brackets, reverse the steps.
Connecting Cables

This section describes how to connect your Cisco ISE 3300 Series appliance to the network and the appliance console. In the following example, Figure 1-7 shows the Cisco ISE 3315 appliance. For the specific locations of the rear-panel features for the other Cisco ISE 3300 Series appliances, see the following topics:

- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14

The following topics describe how to connect and manage cabling:

- Connecting the Network Interface, page 1-10
- Connecting the Console, page 1-11
- Connecting the Keyboard and Video Monitor, page 1-13
- Cable Management, page 1-14
Figure 1-7  Cisco ISE 3315 Appliance Rear-Panel View

The following table describes the callouts in Figure 1-7.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AC Power supply cable socket</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>NIC 3 (eth2) add-on card</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>NIC 4 (eth3) add-on card</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>Serial port</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Video port</td>
<td></td>
</tr>
</tbody>
</table>

Attach your cables (such as keyboard, monitor cables, if required) to the rear of the server. Route the cables to the left corner of the server (from a rear-panel perspective as shown in Figure 1-8), and use the cable straps to secure the cables to the slide rails.

Figure 1-8  Connecting the Cables
Connecting Cables

Connecting the Network Interface

Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.
Statement 1001

This section describes how to connect the Cisco ISE 3300 Series appliance Ethernet port. The RJ-45 port supports standard straight-through and crossover Category 5 UTP cables.

Note

We do not supply Category 5 UTP cables; these cables are available commercially.

To connect the cable to the Cisco ISE 3300 Series appliance Ethernet port, complete the following steps:

Step 1 Verify that the appliance is turned off.
Step 2 Connect one end of the cable to the Gigabit Ethernet 0 port on the appliance.
Step 3 Connect the other end to a switch in your network.

Ethernet Port Connector

Each supported Cisco ISE 3300 Series appliance comes with two integrated dual-port Ethernet controllers. These Ethernet controllers provide an interface for connecting to 10-, 100-, or 1000-Mb/s networks, and they provide full-duplex (FDX) capability that enables simultaneous transmission and reception of data on the Ethernet LAN. For the exact location of the Ethernet port connector on each appliance, see the following:

- Cisco ISE 3315 Rear-Panel Features, page 1-7
- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14

To access the Ethernet port, connect at a minimum Category 5 or 5E (we recommend that you use Category 6) UTP cable to the RJ-45 connector on the back of the appliance. Table 1-2 describes the UTP cable categories.

Table 1-2 Ethernet to UTP Cabling Category Guidelines

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10BASE-T</td>
<td>EIA Categories 5 or 5E or higher UTP (2 or 4 pair) up to 328 ft (100 m)</td>
</tr>
<tr>
<td>100BASE-TX</td>
<td>EIA Category 5 or 5E or higher UTP (2 pair) up to 328 ft (100 m)</td>
</tr>
<tr>
<td>1000BASE-T</td>
<td>EIA Category 6 UTP (recommended), Category 5 or 5E UTP (2 pair) up to 328 ft (100 m)</td>
</tr>
</tbody>
</table>

Figure 1-9 shows the Ethernet RJ-45 port and plug.
Appendix 1 Installing the Cisco ISE 3300 Series Hardware

Connecting Cables

Figure 1-9 RJ-45 Port and Plug

Table 1-3 lists and describes the RJ-45 pin signals used on the Ethernet connector.

<table>
<thead>
<tr>
<th>Ethernet Port Pin</th>
<th>Signal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TxD+</td>
<td>Send data +</td>
</tr>
<tr>
<td>2</td>
<td>TxD–</td>
<td>Send data –</td>
</tr>
<tr>
<td>3</td>
<td>RxD+</td>
<td>Receive data +</td>
</tr>
<tr>
<td>4</td>
<td>Termination network</td>
<td>No connection</td>
</tr>
<tr>
<td>5</td>
<td>Termination network</td>
<td>No connection</td>
</tr>
<tr>
<td>6</td>
<td>RxD–</td>
<td>Receive data –</td>
</tr>
<tr>
<td>7</td>
<td>Termination network</td>
<td>No connection</td>
</tr>
<tr>
<td>8</td>
<td>Termination network</td>
<td>No connection</td>
</tr>
</tbody>
</table>

Warning To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. Statement 1021

Connecting the Console

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

Caution To help prevent a potential network security threat, Cisco strongly recommends physically disconnecting from the Cisco ISE console management port when you are not using it. For more details, see http://seclists.org/fulldisclosure/2011/Apr/55, which applies to the Cisco ISE, Cisco NAC Appliance, and Cisco Secure ACS hardware platforms.

Each Cisco ISE 3300 Series appliance has a data circuit-terminating equipment mode console port that allows you to connect a console terminal directly to your appliance. The appliance uses a DB-9 serial connector for the console port.
Connecting Cables

The console port on each Cisco ISE 3300 Series appliance includes an EIA/TIA-232 asynchronous serial (DB-9) connector. This serial console connector (port) allows you to access the appliance locally by connecting a terminal—either a PC that runs terminal-emulation software or an ASCII terminal—to the console port, and this can be performed by using one of the following methods:

- Connecting a PC that is running terminal-emulation software to the console port by using a DB-9 female to DB-9 female straight-through cable.
- Connecting an ASCII terminal to the console port by using a DB-9 female to DB-25 male straight-through cable with a DB-25 female to DB-25 female gender changer.
- Connecting a terminal or a PC running terminal-emulation software to the console port on the Cisco ISE 3300 Series appliance.

To connect a console terminal to your appliance, complete the following steps:

**Step 1**
Connect the terminal by using a straight-through cable to the console port.

**Step 2**
Configure your terminal or terminal-emulation software to use the following settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No hardware flow control

Serial (Console) Port Connector

Cisco ISE 3300 Series appliances have one serial port connector that is located on the rear panel of each appliance. For the exact location of each serial port connector on each appliance, see the following:

- Cisco ISE 3315 Rear-Panel Features, page 1-7
- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14

Figure 1-10 shows the pin number assignments for the 9-pin, male, D-shell serial port connector that is located on the rear panel of each Cisco ISE 3300 Series appliance. The defined pin number assignments are those that conform to industry standards for the RS-232-C.

**Figure 1-10 Serial Port Connector**

![Serial Port Connector Diagram]

Table 1-4 lists and describes the serial (console) port pinout.
Connecting Cables

Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.
Statement 1001

This section describes how you can connect a keyboard and video monitor to a Cisco ISE 3300 Series appliance. As an alternative to connecting a keyboard or video monitor, you can make a serial console connection to a Cisco ISE 3300 Series appliance. Note the following guidelines:

- Cisco ISE 3300 Series appliances do not support the use of a mouse device.
- Cisco ISE 3300 Series appliances provide USB ports on both the front and rear panel on each appliance that can be used for making a keyboard (USB port) or video monitor (video port) connection.

For the specific location of the USB and video ports on each appliance, see the following:

- Cisco ISE 3315 Rear-Panel Features, page 1-7
- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14

To connect a keyboard and video monitor to your appliance, complete the following steps:

**Step 1** Verify that the appliance is turned off.

**Step 2** Connect the end of the keyboard cable for the PS/2 (keyboard) to the supplied USB to the PS/2 dongle adapter that is located on the rear panel of the appliance.

**Step 3** Connect the end of the video monitor cable to the PS/2 VGA port that is located on the appliance. In the Cisco ISE 3315, there is one video port on the rear panel; on the Cisco ISE 3355 and Cisco ISE 3395, there is one video port on the front panel and one video port on the rear panel.

**Step 4** Turn on the appliance.

### Table 1-4 DB-9 Serial (Console) Port Pinout

<table>
<thead>
<tr>
<th>Serial Port Pin</th>
<th>Signal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD</td>
<td>Data carrier detect</td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>Receive data</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>Send/transmit data</td>
</tr>
<tr>
<td>4</td>
<td>DTR</td>
<td>Data terminal ready</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>Signal ground</td>
</tr>
<tr>
<td>6</td>
<td>DSR</td>
<td>Data set ready</td>
</tr>
<tr>
<td>7</td>
<td>RTS</td>
<td>Request to send</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>Clear to send</td>
</tr>
<tr>
<td>9</td>
<td>RI</td>
<td>Ring indicator</td>
</tr>
</tbody>
</table>

Connecting the Keyboard and Video Monitor
Cable Management

Cable management can be the most visual element that is part of setting up your appliance. However, the issue of cable management is often overlooked because the time spent is not considered a high-priority task. Because racks and enclosures typically house more equipment today than ever before, the increase in equipment installations per rack means you must better organize, route, and manage your cabling inside and outside the equipment rack.

Poor cable management can lead not only to damaged cables or added time spent rerouting or changing cabling, but it also can impair critical airflow that cools your appliance or blocks access to it. These types of problems can lead to inefficiencies in performance or potentially even some downtime. However, solutions that address cable management issues range from simple cable management rings, to vertical or horizontal organizers, to the use of cable troughs and ladders.

All Cisco ISE 3300 Series appliance cables should be properly dressed so as not to interfere with each other or with any other equipment in the rack. Use the best local or electrical practices to ensure that the cables that are attached to your appliance are properly dressed. You can now proceed to the next section, Powering Up the Cisco ISE 3300 Series Appliance, page 1-14, to continue the installation process.

Powering Up the Cisco ISE 3300 Series Appliance

Warning Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected. Statement 4

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use. Statement 39

This section contains the following topics:

- Power-Up Checklist, page 1-14
- Power-Up Procedure, page 1-15
- Checking the LEDs, page 1-16

Power-Up Checklist

You can proceed to power up the Cisco ISE 3300 Series appliance if you have met the following conditions:

- The appliance is securely mounted.
- The appliance is properly grounded.
- All power, network, and interface cables have been properly connected.
Power-Up Procedure

To power up a Cisco ISE 3300 Series appliance and verify its initialization and self-test, perform the following procedure. When the following procedure is completed, the appliance is ready to be configured. Figure 1-12 shows the Cisco ISE 3315 appliance. For specific front- and rear-panel views and control descriptions for the other Cisco ISE 3300 Series appliances, see:

- Cisco ISE 3355 Appliance:
  - Cisco ISE 3355 Front-Panel Features, page 1-8
  - Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Appliance:
  - Cisco ISE 3395 Front-Panel Features, page 1-12
  - Cisco ISE 3395 Rear-Panel Features, page 1-14

To power up a Cisco ISE 3300 Series appliance, complete the following steps:

**Step 1** Review the information in Safety Guidelines, page 1-1.

**Step 2** Plug the AC power cord into the AC power socket in the rear panel of the appliance. (Location 1 in Figure 1-11 shows the Cisco ISE 3315 appliance.)

**Figure 1-11 Cisco ISE 3315 Appliance Rear-Panel View**

For the location of the AC power socket in the other Cisco ISE 3300 Series appliances, see:

- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14

**Step 3** Connect the other end of the AC power cord to an approved AC power source at your installation site.

**Step 4** In the front panel of the appliance, press the AC power button On to begin the booting process. Location 2 in Figure 1-12 shows the Cisco ISE 3315 appliance. For the location of the AC power button in the other Cisco ISE 3300 Series appliances, see:

- Cisco ISE 3355 Front-Panel Features, page 1-8
- Cisco ISE 3395 Front-Panel Features, page 1-12

**Step 5** Observe the front-panel LEDs for the Cisco ISE 3300 Series appliances. For example, the Cisco ISE 3315 appliance is shown in Figure 1-12. Checking the LEDs, page 1-16 lists the status of the LEDs for all three Cisco ISE 3300 Series appliances.
### Powering Up the Cisco ISE 3300 Series Appliance

#### Figure 1-12  Cisco ISE 3315 Appliance Front-Panel View

The following table defines the front-panel features and LEDs shown in Figure 1-12.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>LED Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Appliance power LED</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>AC power control button</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Reset button</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>HDD activity LED</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Locator LED</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>System-error LED</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>USB 1 connector</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>USB 2 connector</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CD-eject button</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>CD drive activity LED</td>
<td></td>
</tr>
</tbody>
</table>

#### Checking the LEDs

When the Cisco ISE 3300 Series appliances have been started up and are running, observe the state of the front-panel LEDs. Table 1-5 describes the LED color, its power status, activity, and other important status indicators that are displayed for each of the Cisco ISE 3300 Series appliances.

**Table 1-5  Cisco ISE 3300 Series Appliance LEDs**

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
</table>
| Power status | Green | • Lit when appliance has AC power and is powered on.  
|            |       | • Unlit when appliance is turned off, AC power is disconnected, or an error condition has been detected in the operating voltages. |
## Powering Up the Cisco ISE 3300 Series Appliance

### LED Type and Description

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
</table>
| HDD activity               | Green     | • Flashing green when there is ongoing HDD activity.  
                                |           | • Unlit when there is no activity, the appliance has not yet booted, or an error condition has been detected in the boot process.          |
| Locator (LED button)       | Blue      | • Flashing blue when the locator button has been pressed.                                                                                  |
| System health              | Amber     | • Unlit when the system is operating normally.  
                                |           | • Lit indicates a prefailure system threshold condition, such as:  
                                |           |   - At least one fan failure (system or processor fan).  
                                |           |   - At least one of the temperature sensors reached critical level (system or processor thermal sensor).  
                                |           |   - At least one memory module failed.  
                                |           |   - A power supply unit error has occurred.                                                  |

### Cisco ISE 3355 Appliance Front-Panel LEDs

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
</table>
| HDD activity               | Green     | • Lit when there is continuous HDD activity.  
                                |           | • Flashing green when there is ongoing HDD activity.  
                                |           | • Unlit when there is no activity, the HDD is idle, or the HDD has been disabled.        |
| HDD status                 | Amber     | • Lit when HDD is in an error state.                                                                                                       |
|                           |           | • Unlit when HDD is functioning properly or when system is disconnected from AC power.                                                      |
| Ethernet (icon)            | Green     | • Lit when Ethernet interfaces are configured and up.  
                                |           | • Unlit when no Ethernet interfaces are currently configured or when Ethernet interfaces are all down.                                     |
| Ethernet interface activity (NIC 1 and NIC 2) | Green | • Lit when activity exists on NIC 1 or NIC 2.  
                                |           | • Flashing green when there is ongoing activity on NIC 1 or NIC 2.                       |
|                           |           | • Unlit when there is no activity on NIC 1 or NIC 2.                                                                                       |
## Powering Up the Cisco ISE 3300 Series Appliance

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>Amber</td>
<td>• Lit when a noncritical system even has occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unlit when system is functioning normally.</td>
</tr>
<tr>
<td>System health</td>
<td>Amber</td>
<td>• Unlit when the system is operating normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lit indicates a prefailure system threshold condition, such as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– At least one fan failure (system or processor fan).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– At least one of the temperature sensors reached critical level (system or processor thermal sensor).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– At least one memory module failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– A power supply unit error has occurred.</td>
</tr>
<tr>
<td>Locator (button)</td>
<td>Blue</td>
<td>• Flashing blue when locator button has been pressed.</td>
</tr>
<tr>
<td>Ethernet interface activity (NIC 3 and NIC 42)</td>
<td>Green</td>
<td>• Lit when activity exists on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flashing green when there is ongoing activity on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unlit when there is no activity on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td>Power (button)</td>
<td>Green</td>
<td>• Lit when the appliance has AC power and is turned on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rapidly flashing green indicates that the appliance is turned off and is not yet ready to be turned on. The appliance typically only remains in this state for 1 to 3 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Slowly flashing green indicates that the appliance is currently turned off and is ready to be turned on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Slowly fading on or off indicates that the appliance is in power-save mode (and is ready to be turned on).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unlit when the appliance is turned off (AC power is disconnected).</td>
</tr>
</tbody>
</table>
### Appendix 1: Installing the Cisco ISE 3300 Series Hardware

**Powering Up the Cisco ISE 3300 Series Appliance**

#### Cisco ISE 3395 Appliance Front-Panel LEDs

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
</table>
| HDD activity                     | Green     | • Lit when there is continuous HDD activity.  
• Flashing green when there is ongoing HDD activity.  
• Off when there is no activity, the HDD is idle, or the HDD has been disabled. |
| HDD status                       | Amber     | • Lit when HDD is in error state.  
• Unlit when HDD is functioning properly or when system is disconnected from AC power. |
| Ethernet (icon)                  | Green     | • Lit when Ethernet interfaces are configured and up.  
• Unlit when no Ethernet interfaces are currently configured or when Ethernet interfaces are all down. |
| Ethernet interface activity      | Green     | • Lit when activity exists on NIC 1 or NIC 2.  
• Flashing green when there is ongoing activity on NIC 1 or NIC 2.  
• Unlit when there is no activity on NIC 1 or NIC 2. |
| (NIC 1 and NIC 2)                |           |                                                                                                                                 |
| Informational                    | Amber     | • Lit when a noncritical system even has occurred.  
• Unlit when system is functioning normally. |
| System health                    | Amber     | • Unlit when the system is operating normally.  
• Lit indicates a prefailure system threshold condition, such as:  
  - At least one fan failure (system or processor fan).  
  - At least one of the temperature sensors reached critical level (system or processor thermal sensor).  
  - At least one memory module failed.  
  - A power supply unit error has occurred. |
| Locator (button)                 | Blue      | • Flashing blue when locator button has been pressed. |
### Powering Up the Cisco ISE 3300 Series Appliance

For more detailed information about the Cisco ISE 3300 Series LEDs, see Troubleshooting Overview, page 1-1. After the operating system boots, you are ready to initialize the basic software configuration. For configuration procedures, see Chapter 1, “Configuring the Cisco ISE Appliances.”

<table>
<thead>
<tr>
<th>LED Type</th>
<th>LED Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet interface activity</td>
<td>Green</td>
<td>• Lit when activity exists on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td>(NIC 3 and NIC 42)</td>
<td></td>
<td>• Flashing green when there is ongoing activity on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unlit when there is no activity on NIC 3 or NIC 4.</td>
</tr>
<tr>
<td>Power (button)</td>
<td>Green</td>
<td>• Lit when the appliance has AC power and is turned on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rapidly flashing green indicates that the appliance is turned off and is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not yet ready to be turned on. The appliance typically only remains in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this state for 1 to 3 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Slowly flashing green indicates that the appliance is currently turned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>off and is ready to be turned on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Slowly fading on or off indicates that the appliance is in power-save</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mode (and is ready to be turned on).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unlit when the appliance is turned off (AC power is disconnected).</td>
</tr>
</tbody>
</table>

For more detailed information about the Cisco ISE 3300 Series LEDs, see Troubleshooting Overview, page 1-1. After the operating system boots, you are ready to initialize the basic software configuration. For configuration procedures, see Chapter 1, “Configuring the Cisco ISE Appliances.”
Installing the Cisco SNS-3400 Series Hardware

This appendix describes how to install your Cisco SNS-3400 Series appliances and connect any of the supported appliances to the network. This information is contained in the following sections:

- Connecting and Powering On the Server, page 1-1
- Checking the LEDs, page 1-2
- Configuring CIMC, page 1-4
- Creating a Bootable USB Drive, page 1-6
- Installing or Replacing Server Components, page 1-7

Connecting and Powering On the Server

This section describes how to power on the server and assign an IP address to connect to it. The server is shipped with a default NIC mode called *Shared LOM, default NIC redundancy is active-active, and DHCP is enabled*. Shared LOM mode enables the two 1-Gb Ethernet ports to access the Cisco Integrated Management Interface (CIMC). If you want to use the 1-Gb Ethernet dedicated management port, or a port on a Cisco UCS P81E Virtual Interface Card (VIC) to access the CIMC, you must first connect to the server and change the NIC mode as described in Step 3 of the following procedure. In that step, you can also change the NIC redundancy and set static IP settings.

Use the following procedure to perform initial setup of the server:

**Step 1**  
Attach a supplied power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet. See the Power Specifications, page 1-2 for power specifications.

Wait for approximately two minutes to let the server boot in standby power during the first bootup.

You can verify power status by looking at the Power Status LED:

- Off—There is no AC power present in the server.
- Amber—The server is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.
- Green—The server is in main power mode. Power is supplied to all server components.
Checking the LEDs

During bootup, the server beeps once for each USB device that is attached to the server. Even if there are no external USB devices attached, there is a short beep for each virtual USB device such as a virtual floppy drive, CD/DVD drive, keyboard, or mouse. A beep is also emitted if a USB device is hot-plugged or hot-unplugged during BIOS power-on self test (POST), or while you are accessing the BIOS Setup utility or the EFI shell.

Step 2
Connect a USB keyboard and VGA monitor by using the supplied KVM cable connected to the KVM connector on the front panel.

Note Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you are connected to one VGA connector and you then connect a video device to the other connector, the first VGA connector is disabled.

Checking the LEDs

When the Cisco SNS-3400 Series appliances have been started up and are running, observe the state of the front-panel and rear-panel LEDs. The following topics describe the LED color, its power status, activity, and other important status indicators that are displayed for the Cisco SNS-3400 Series appliance:

- Front Panel LEDs and Buttons, page B-2
- Rear Panel LEDs and Buttons, page B-4

Front Panel LEDs and Buttons

<table>
<thead>
<tr>
<th>LED Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power button/Power status LED</td>
<td>• Off—There is no AC power to the server.</td>
</tr>
<tr>
<td></td>
<td>• Amber—The server is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.</td>
</tr>
<tr>
<td></td>
<td>• Green—The server is in main power mode. Power is supplied to all server components.</td>
</tr>
<tr>
<td>Identification</td>
<td>• Off—The Identification LED is not in use.</td>
</tr>
<tr>
<td></td>
<td>• Blue—The Identification LED is activated.</td>
</tr>
</tbody>
</table>
### Table 1-1  Front Panel LEDs, Definitions of States (continued)

<table>
<thead>
<tr>
<th>LED Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>System status</td>
<td>• Green—The server is running in normal operating condition.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—The server is performing system initialization and memory check.</td>
</tr>
<tr>
<td></td>
<td>• Amber, steady—The server is in a degraded operational state. For example:</td>
</tr>
<tr>
<td></td>
<td>– Power supply redundancy is lost.</td>
</tr>
<tr>
<td></td>
<td>– CPUs are mismatched.</td>
</tr>
<tr>
<td></td>
<td>– At least one CPU is faulty.</td>
</tr>
<tr>
<td></td>
<td>– At least one DIMM is faulty.</td>
</tr>
<tr>
<td></td>
<td>– At least one drive in a RAID configuration failed.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—The server is in a critical fault state. For example:</td>
</tr>
<tr>
<td></td>
<td>– Boot failed.</td>
</tr>
<tr>
<td></td>
<td>– Fatal CPU and/or bus error is detected.</td>
</tr>
<tr>
<td></td>
<td>– Server is in over-temperature condition.</td>
</tr>
<tr>
<td>Fan status</td>
<td>• Green—All fan modules are operating properly.</td>
</tr>
<tr>
<td></td>
<td>• Amber, steady—One fan module has failed.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—Critical fault, two or more fan modules have failed.</td>
</tr>
<tr>
<td>Temperature status</td>
<td>• Green—The server is operating at normal temperature.</td>
</tr>
<tr>
<td></td>
<td>• Amber, steady—One or more temperature sensors have exceeded a warning threshold.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—One or more temperature sensors have exceeded a critical threshold.</td>
</tr>
<tr>
<td>Power supply status</td>
<td>• Green—All power supplies are operating normally.</td>
</tr>
<tr>
<td></td>
<td>• Amber, steady—One or more power supplies are in a degraded operational state.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—One or more power supplies are in a critical fault state.</td>
</tr>
<tr>
<td>Network link activity</td>
<td>• Off—The Ethernet link is idle.</td>
</tr>
<tr>
<td></td>
<td>• Green—One or more Ethernet LOM ports are link-active, but there is no activity.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—One or more Ethernet LOM ports are link-active, with activity.</td>
</tr>
<tr>
<td>Hard drive fault</td>
<td>• Off—The hard drive is operating properly.</td>
</tr>
<tr>
<td></td>
<td>• Amber—This hard drive has failed.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—The device is rebuilding.</td>
</tr>
<tr>
<td>Hard drive activity</td>
<td>• Off—There is no hard drive in the hard drive sled (no access, no fault).</td>
</tr>
<tr>
<td></td>
<td>• Green—The hard drive is ready.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—The hard drive is reading or writing data.</td>
</tr>
</tbody>
</table>
## Rear Panel LEDs and Buttons

### Table 1-2  Rear Panel LEDs, Definitions of States

<table>
<thead>
<tr>
<th>LED Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply fault</td>
<td>• Off—The power supply is operating normally.</td>
</tr>
<tr>
<td></td>
<td>• Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate.</td>
</tr>
<tr>
<td></td>
<td>• Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).</td>
</tr>
<tr>
<td>Power supply AC OK</td>
<td>• Off—There is no AC power to the power supply.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—AC power OK, DC output not enabled.</td>
</tr>
<tr>
<td></td>
<td>• Green, solid—AC power OK, DC outputs OK.</td>
</tr>
<tr>
<td>1-Gb Ethernet dedicated management link speed</td>
<td>• Off—link speed is 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>• Amber—link speed is 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>• Green—link speed is 1 Gbps.</td>
</tr>
<tr>
<td>1-Gb Ethernet dedicated management link status</td>
<td>• Off—No link is present.</td>
</tr>
<tr>
<td></td>
<td>• Green—Link is active.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—Traffic is present on the active link.</td>
</tr>
<tr>
<td>1-Gb Ethernet link speed</td>
<td>• Off—link speed is 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>• Amber—link speed is 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>• Green—link speed is 1 Gbps.</td>
</tr>
<tr>
<td>1-Gb Ethernet link status</td>
<td>• Off—No link is present.</td>
</tr>
<tr>
<td></td>
<td>• Green—Link is active.</td>
</tr>
<tr>
<td></td>
<td>• Green, blinking—Traffic is present on the active link.</td>
</tr>
<tr>
<td>Identification</td>
<td>• Off—The Identification LED is not in use.</td>
</tr>
<tr>
<td></td>
<td>• Blue—The Identification LED is activated.</td>
</tr>
</tbody>
</table>

## Configuring CIMC

You can perform all operations on the Cisco SNS-3400 series appliances through the CIMC. To do this, you must first configure an IP address and IP gateway to access the CIMC from a web-based browser.

**Step 1**  Plug in the power cord.

**Step 2**  Press the **Power** button to boot the server. Watch for the prompt to press F8 as shown in TBD.
Step 3  During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility. The following screen appears.

Step 4  Set the NIC mode to your choice for which ports to use to access the CIMC for server management (see Figure 1-3 on page 1-3 for identification of the ports):

- Dedicated—The 1-Gb Ethernet management port is used to access the CIMC. You must select NIC redundancy *None* and select IP settings.
- Shared LOM (default)—The two 1-Gb Ethernet ports are used to access the CIMC. This is the factory default setting, along with Active-active NIC redundancy and DHCP enabled.
- Cisco Card—The ports on an installed Cisco UCS P81E VIC are used to access the CIMC. You must select a NIC redundancy and IP setting.
Creating a Bootable USB Drive

The Cisco ISE 1.1.4 ISO image contains an “images” directory that has a Readme file and a script to create a bootable USB to install Cisco ISE 1.1.4.

Before You Begin
- Ensure that you have read the Readme in the “images” directory
- You need the following:
  - Linux machine with RHEL-5 or above, CentOS 5.x or above. If you are going to use your PC or MAC, ensure that you have installed a Linux VM on it.
  - An 8-GB USB drive
The iso-to-usb.sh script

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Plug in your USB drive into the USB port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Copy the iso-to-usb.sh script and the Cisco ISE 1.1.4 ISO image to a directory on your Linux machine.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the following command: iso-to-usb.sh source_iso usb_device For example, # ./iso-to-usb.sh ise-1.1.4.218.i386.iso /dev/sdb where iso-to-usb.sh is the name of the script, ise-1.1.4.218.i386.iso is the name of the ISO image, and /dev/sdb is your USB device.</td>
</tr>
<tr>
<td>Step 4</td>
<td>A screen appears prompting you to specify the Cisco SNS-3400 Series appliance (Cisco SNS-3415 or Cisco SNS-3495).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a value corresponding to your appliance type to create a bootable USB drive.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter Y to continue.</td>
</tr>
<tr>
<td>Step 7</td>
<td>A success message appears.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Unplug your USB drive.</td>
</tr>
</tbody>
</table>

What To Do Next
Configuring Cisco ISE on the Cisco SNS-3400 Series Appliance Using CIMC, page 1-11

Installing or Replacing Server Components

Refer to the Cisco UCS C220 Server Installation and Service Guide for information on how to install or replace the SNS 3415 or 3495 appliance components.
Maintaining the Cisco ISE 3300 Series Appliance

All Cisco Identity Services Engine (ISE) 3300 Series appliances are configured to order and are ready for installation when they leave the factory. After you install and configure an appliance in your own network environment, you may need to perform some specific maintenance procedures or operations to ensure that the appliance is operating properly and is integrated into your network. These types of preventive procedures maintain your appliance in good operating condition and minimize the need for costly, time-consuming service procedures.

To help prevent problems, before performing any procedures in this appendix, review all Related Documentation, page -5, and Safety Guidelines, page 1-1.

The following sections discuss various environmental factors that can adversely affect the performance and longevity of your appliance.

Maintaining Your Site Environment and Appliance

Good preventive maintenance includes regular visual inspections of the appliance, including exterior cleaning and inspection. This appendix provides the following topics that describe some best practices for maintaining your site and appliance:

- General Exterior Cleaning and Inspection, page 1-2
- Cooling, page 1-3
- Temperature, page 1-3
- Humidity, page 1-4
- Altitude, page 1-4
- ESD, page 1-4
- EMI and RFI, page 1-4
- Magnetism, page 1-5
- Power Source Interruptions, page 1-5
- Preparing to Transport the Rack Cabinet, page 1-6
- Removing or Replacing the Cisco ISE 3300 Series Appliance, page 1-7
General Exterior Cleaning and Inspection

This section describes cleaning requirements for the exterior surfaces of your appliance. In addition, it also provides guidelines for inspecting cables and adapter cards.

⚠️ Caution
Never spray cleaning solution on the surfaces of the appliance. Over-spray can penetrate the appliance, and this can increase the potential for electrical problems or corrosion of internal components.

Appliance

Use a lint-free, nonabrasive cloth to perform cleaning. Do not use a solvent, abrasive cleaning agents, or tissue paper. If the appliance is dirty (for example, with thick dust), use a soft, damp cloth and gently wipe the surface of the appliance. Make sure you immediately wipe any water or other liquid off the appliance.

Dust and Particles

A clean operating environment can greatly reduce the negative effects of dust and other particles, which act as insulators and can interfere with the operation of an appliance’s mechanical components. Besides performing regular and periodic cleaning, you should follow these guidelines to avoid contamination of the appliance:

- Do not permit smoking anywhere near the appliance.
- Do not permit food or drink near the appliance.

Cables and Connectors

Periodically inspect all your cables and connectors that run to and from your appliance. This practice ensures that the cable and connectors are properly connected, provides a visual check for wear and condition, and detects any loose connections before they become a problem.

Adapter Cards

Check the connections on the adapter cards. Ensure that they are firmly secured to the appliance and have not been jarred loose or mechanically damaged.

Corrosion

Skin oil from fingers and hands, or prolonged exposure to high temperature or humidity, can corrode the gold-plated edge connectors and pin connectors on adapter cards. Because corrosion on adapter card connectors is a gradual process, this can eventually lead to intermittent failure of electrical circuits.

To prevent corrosion, avoid touching contacts on adapter cards. Protecting the appliance from corrosive elements is especially important in damp, moist, and salty environments, all of which tend to promote corrosion. Also, as a further deterrent to corrosion, the appliance should not be used in extreme temperatures. For details, see Temperature, page 1-3.
Cooling

Exhaust fans in the power supply and in the appliance itself cool the power supply and the appliance by drawing air in through various intake openings in the front of the appliance and blowing it out the back through exhaust vents.

However, these fans also draw dust and other particles into the appliance, which causes contaminant buildup, that can directly cause an increase in the internal temperature of the appliance. Increased temperatures and contaminants interfere with the proper operation of various appliance components.

To avoid these conditions, we recommend keeping your work environment as clean as possible to reduce the amount of dust and dirt around the appliance. This best practice reduces the amount of contaminants that can be drawn into your appliance by the fans.

Temperature

Temperature extremes can cause a variety of problems, including premature aging and failure of integrated circuits or mechanical failure of devices.

Extreme temperature fluctuations can cause integrated circuits to become loose in their sockets and can cause expansion and contraction of disk drive platters, which can directly result in read or write data errors. The heat emission of a Cisco ISE appliance is in the range of 341 to 1024 BTUs (100 to 300 W).

To minimize the negative effects of temperature on appliance performance, observe the following guidelines:

- Ensure that the appliance has adequate ventilation. Do not place it within a closed-in wall unit or on top of cloth, which can act as insulation. Do not place the appliance where it receives direct sunlight, particularly in the afternoon. Do not place the appliance next to any heat source of any kind, including heating vents during winter.

Adequate ventilation is particularly important at higher altitudes. Your appliance performance may not be optimum when it is operating at high temperatures as well as high altitudes. Observe the following guidelines:

- Ensure that all slots and openings on the appliance remain unobstructed, especially the fan vents on the rear panel of the appliance.
- Clean the appliance at regular intervals to avoid any buildup of dust, dirt, or debris, which can all contribute to causing the appliance to overheat.
If the appliance has been exposed to abnormally cold temperatures, allow a two-hour warm-up period for it to come back up to a normal operating temperature range before powering it on. Failure to follow this practice can damage internal components, particularly the hard disk drive.

**Humidity**

High-humidity conditions can cause moisture migration and penetration into the appliance. This moisture can cause corrosion of internal components and degradation of properties such as electrical resistance, thermal conductivity, physical strength, and size. Extreme moisture buildup inside the appliance can result in electrical shorts, which can cause serious damage to the appliance.

Each appliance is rated to operate at 8 to 80 percent relative humidity, with a humidity gradation of 10 percent per hour. Buildings in which climate is controlled by air conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for appliances. However, if an appliance is located in an unusually humid location, a dehumidifier can be used to maintain the humidity within an acceptable range.

**Altitude**

Operating an appliance at higher altitudes (with lower atmospheric pressure) reduces the efficiency of forced and convection cooling which can result in electrical problems related to arcing and coronal effects. This condition can also cause sealed components with internal pressure, such as electrolytic capacitors, to fail or perform at reduced efficiency.

**ESD**

ESD results from the buildup of static electricity on the human body and certain other objects. This static electricity is often produced by simple movements, such as walking across a carpet.

ESD is a discharge of a static electrical charge that occurs when a person whose body contains such a charge touches a component in the appliance. This static discharge can cause components, especially integrated circuits (ICs), to fail. ESD is a problem particularly in dry environments where the relative humidity is below 50 percent. To reduce the effects of ESD, you should observe the following guidelines:

- Wear a grounding wrist strap. If a grounding wrist strap is unavailable, touch an unpainted metal surface on the appliance chassis periodically to neutralize any static charge.
- Keep components in their antistatic packaging until they are installed.
- Avoid wearing clothing made of wool or synthetic materials.

**EMI and RFI**

EMI and RFI from an appliance can adversely affect devices such as radio and television receivers operating near the appliance. Radio frequencies emanating from an appliance can also interfere with cordless and low-power telephones.
RFI is defined as any EMI with a frequency above 10 kHz. This type of interference can travel from the appliance to other devices through the power cable and power source, or through the air, like transmitted radio waves. The Federal Communications Commission (FCC) publishes specific regulations to limit the amount of EMI and RFI emitted by computing equipment. Each appliance meets these FCC regulations.

To reduce the possibility of EMI and RFI, observe the following guidelines:

- Operate the appliance only with the appliance cover installed.
- Ensure that the screws on all peripheral cable connectors are securely fastened to their corresponding connectors on the rear of the appliance.
- Always use shielded cables with metal connector shells for attaching peripherals to the appliance.

## Magnetism

Hard disk drives are susceptible to the effects of magnetism as they store data magnetically. Hard disk drives should never be stored near the following types of magnetic sources:

- Monitors
- Printers
- Telephones (with electrically driven bells)
- Fluorescent lights

## Power Source Interruptions

Appliances are especially sensitive to variations in the voltage supplied by AC power sources. Problems with overvoltage, undervoltage, or transient voltages (spikes) can erase data from the memory or even cause some components to fail. To protect against these types of problems, power cables should always be properly grounded and one, or both, of the following methods should be used:

- Place the appliance on a dedicated power circuit (rather than sharing a circuit with other electrical equipment).
- For best practices, do not allow the appliance to share a circuit with any of the following devices:
  - Photo-copier machines
  - Teletype machines
  - Laser printers
  - Fax machines
  - Any other motorized equipment

In addition to the equipment just noted, the greatest threat to an appliance’s power supply are the surges or blackouts caused by electrical storms.

If a blackout occurs—even a temporary one—while the appliance is turned on, turn off the appliance immediately and disconnect it from the electrical outlet. Leaving the appliance on may cause problems when the power is restored.
Maintaining Your Cisco ISE 3300 Series Appliance

This section provides information about the following appliance-related topics:

- Preparing to Transport the Rack Cabinet, page 1-6

Preparing to Transport the Rack Cabinet

Ensure that you complete all necessary pre-transport tasks before you attempt to transport the Cisco ISE 3300 Series appliance to another location after the appliance has been installed.

To prepare the Cisco ISE 3300 Series appliance for transport, complete the following steps:

Step 1 Remove the large screw (see Figure 1-1) and discard it.
Step 2 Remove and save the front screw.
Step 3 Loosen the other two rear screws.
Step 4 Fully extend the rail and insert the screw you saved into the position where the large screw had been located.
Step 5 Tighten all screws to secure the rail.
Step 6 Repeat the steps from 1 to 5 for the other rail.

![Preparing to Transport the Rack Cabinet](image)

The following table describes the callouts in Figure 1-1.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Large screw</td>
</tr>
<tr>
<td>2</td>
<td>Front screw</td>
</tr>
<tr>
<td>3</td>
<td>Rear screws (2)</td>
</tr>
</tbody>
</table>
Step 7  Secure the server to the rack:
   a. If necessary, disconnect the cables from the rear of the server.
   b. Slide the server out of the rack 150 mm (6 inches) and insert the M6 screws in each slide rail.
   c. Secure the server to the rack cabinet with the M6 screws (see Figure 1-2).

Step 8  Ensure that the rails are fully extended to the rear of the rack cabinet.

If you have removed the shipping brackets on the slide rails, you must reinstall them before you transport the rack cabinet with the server installed. Reverse the instructions on the shipping bracket to reinstall it, as shown in Figure 1-6 on page 1-8.

Figure 1-2  Preparing to Move the Rack Cabinet to Another Location

Removing or Replacing the Cisco ISE 3300 Series Appliance

Warning  Before working on a system that has an On/Off switch, turn the AC power off and unplug the power cord. Statement 1

Warning  Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

This section contains information about the following topics:

- Removing a Cisco ISE 3300 Series Appliance, page 1-8
- Replacing a Cisco ISE 3300 Series Appliance, page 1-8
Removing a Cisco ISE 3300 Series Appliance

To remove a Cisco ISE 3300 Series appliance from your network, complete the following steps:

Step 1  Turn off the appliance to be removed.
Step 2  Disconnect the power cords and network cables.
Step 3  Physically remove the appliance from the rack.

Because a Cisco ISE 3300 Series appliance is typically in constant communication on your network, when the network notices that the appliance is no longer responding to it, the network stops sending any requests to the appliance. This change will be visible to users.

Note  If other appliances are attached to the network, the network continues sending requests to the other appliances.

Replacing a Cisco ISE 3300 Series Appliance

To replace an appliance, complete the following steps:

Step 1  Ensure that the appliance being replaced has been removed from the network.
Step 2  Install a new appliance by using the same installation procedures that you used for the appliance that was removed.
Step 3  Configure the new appliance by using the same configuration parameters that you used for the appliance you removed.
Cisco SNS-3400 Series Server Specifications

This appendix lists the technical specifications for the server and includes the following sections:

- Physical Specifications, page A-1
- Environmental Specifications, page A-1
- Power Specifications, page A-2

Physical Specifications

Table A-1 lists the physical specifications for the server.

<table>
<thead>
<tr>
<th>Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>1.7 in. (4.3 cm)</td>
</tr>
<tr>
<td>Width</td>
<td>16.9 in. (42.9 cm)</td>
</tr>
<tr>
<td>Depth</td>
<td>28.5 in. (72.4 cm)</td>
</tr>
<tr>
<td>Weight (fully loaded chassis)</td>
<td>35.6 lb. (16.1 Kg)</td>
</tr>
</tbody>
</table>

Environmental Specifications

Table A-2 lists the environmental specifications for the server.

<table>
<thead>
<tr>
<th>Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature, operating:</td>
<td>41 to 104°F (5 to 40°C)</td>
</tr>
<tr>
<td></td>
<td>Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.</td>
</tr>
<tr>
<td>Temperature, non-operating</td>
<td>−40 to 149°F (−40 to 65°C)</td>
</tr>
<tr>
<td>Humidity (RH), noncondensing</td>
<td>10 to 90%</td>
</tr>
<tr>
<td>Altitude, operating</td>
<td>0 to 10,000 feet</td>
</tr>
</tbody>
</table>
Power Specifications

The power specifications for the two power supply options are listed in the following sections:

- 450W Power Supply, page A-2

You can get more specific power information for your exact server configuration by using the Cisco UCS Power Calculator:

http://www.cisco.com/assets/cdc_content_elements/flash/dataCenter/cisco_ucs_power_calculator/

**Note**

Do not mix power supply types in the server. Both power supplies must be either 450W or 650W.

### 450W Power Supply

Table A-3 lists the specifications for each 450W power supply (Cisco part number UCSC-PSU-450W).

<table>
<thead>
<tr>
<th>Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC input voltage range</td>
<td>Low range: 100 VAC to 120 VAC</td>
</tr>
<tr>
<td></td>
<td>High range: 200 VAC to 240 VAC</td>
</tr>
<tr>
<td>AC input frequency</td>
<td>Range: 47 to 63 Hz (single phase, 50 to 60Hz nominal)</td>
</tr>
<tr>
<td>AC line input current (steady state)</td>
<td>6.0 A peak at 100 VAC</td>
</tr>
<tr>
<td></td>
<td>3.0 A peak at 208 VAC</td>
</tr>
<tr>
<td>Maximum output power for each power supply</td>
<td>450 W</td>
</tr>
<tr>
<td>Power supply output voltage</td>
<td>Main power: 12 VDC</td>
</tr>
<tr>
<td></td>
<td>Standby power: 12 VDC</td>
</tr>
</tbody>
</table>

### 650W Power Supply

Table A-4 lists the specifications for each 650W power supply (Cisco part number UCSC-PSU-650W).
### Table A-4    Power Supply Specifications

<table>
<thead>
<tr>
<th>Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC input voltage range</td>
<td>90 to 264 VAC (self-ranging, 180 to 264 VAC nominal)</td>
</tr>
<tr>
<td>AC input frequency</td>
<td>Range: 47 to 63 Hz (single phase, 50 to 60Hz nominal)</td>
</tr>
<tr>
<td>AC line input current (steady state)</td>
<td>7.6 A peak at 100 VAC</td>
</tr>
<tr>
<td></td>
<td>3.65 A peak at 208 VAC</td>
</tr>
<tr>
<td>Maximum output power for each power supply</td>
<td>650 W</td>
</tr>
<tr>
<td>Power supply output voltage</td>
<td>Main power: 12 VDC</td>
</tr>
<tr>
<td></td>
<td>Standby power: 12 VDC</td>
</tr>
</tbody>
</table>
APPENDIX A

Troubleshooting the Cisco ISE Appliance

The Cisco Identity Services Engine (ISE) 3300 Series appliance undergoes extensive testing before it leaves the factory. If you encounter problems, use the information in this appendix to help isolate problems or to determine whether the appliance is the source of the problem.

Although conditions due to excessive temperatures or excessive power consumption are unlikely at initial startup, see the general environmental conditions that are required to support the Cisco ISE 3300 Series appliances as described in Maintaining Your Site Environment and Appliance, page 1-1.

Note

The procedures in this appendix assume that you are troubleshooting the initial Cisco ISE 3300 Series appliance startup, and that the appliance is in the original factory configuration. If you have removed or replaced components, or changed any default settings, the recommendations in this appendix might not apply.

This appendix does not cover every possible issue that might occur on an appliance, but instead it focuses on those events that are frequently seen by the customer. This appendix provides information on the following topics:

- Troubleshooting Overview, page A-1
- Problem Solving, page A-2
- Reading the LEDs, page A-5
- Locating Appliance Serial Numbers, page A-5

Troubleshooting Overview

At the initial system boot, you should verify the following:

- The external power cable is connected, and the proper power source is being applied. For more information, see Power Considerations, page 1-9, Powering Up the Cisco ISE 3300 Series Appliance, page 1-14, and Troubleshooting the Power and Cooling Systems, page A-3.
- The appliance fan and blower are operating. See Airflow Guidelines, page 1-8 and Troubleshooting the Power and Cooling Systems, page A-3.
- The appliance software boots successfully.
- The adapter cards (if installed) are properly installed in their slots, and each card initializes (and is enabled by the appliance software) without problems.
When each of these conditions is met, the hardware installation is complete, and you should proceed to perform the basic configuration. To understand the features that this release of Cisco ISE offers, see the *Cisco Identity Services Engine User Guide, Release 1.1.x*. To properly configure the Cisco ISE features, see Chapter 1, “Configuring the Cisco ISE Appliances.”

If you cannot locate the source of a problem, contact a Cisco customer service representative for information on how to best proceed with resolving any issue. For more information on the Cisco Technical Assistance Center (TAC), see the *Cisco Information Packet* publication that is shipped with your appliance or visit the following website:


Before you contact Cisco TAC, make sure that you have the following information ready:

- The appliance chassis type and serial number.
- The maintenance agreement or warranty information (see the *Cisco Information Packet*).
- The name, type of software, and version or release number (if applicable).
- The date you received the new appliance.
- A brief description of the problem or condition you experienced, the steps you have taken to isolate or re-create the problem, and a description of any steps you took to resolve the problem.

**Note**

Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the Cisco ISE 3300 Series appliance after your initial installation. For site log information, see *Creating a Site Log*, page 1-14.

### Problem Solving

The key to problem solving is to isolate the problem to a specific location or task. Compare what the Cisco ISE 3300 Series appliance is doing with what it should normally be doing. So, when you are troubleshooting, you must define specific symptoms, and then identify potential problems that could be causing the symptoms. Next, you systematically run through each potential problem and try to eliminate it (from the most likely to the least likely) until the symptoms or conditions disappear.

**Observe these guidelines when performing troubleshooting, by completing the following steps:**

**Step 1**
Analyze the problem, and define a clear problem statement. Define symptoms and potential causes.

**Step 2**
Gather the necessary facts as needed to help isolate possible or potential causes.

**Step 3**
Consider possible or potential causes that are based on the facts that you have gathered.

**Step 4**
Create an action plan that is based on those causes. Begin with the most likely problem and devise a plan that tests only one variable.

**Step 5**
Implement the action plan. Perform each step carefully while testing to see if the symptom disappears.

**Step 6**
Analyze the results to determine if the problem has been resolved. If the problem is resolved, consider the process complete.

If the problem has not been resolved, create an action plan that is based on the next most probable cause on your list.

Return to Step 4 and repeat the process until the problem is solved. Be sure to undo any changes you made while implementing your action plan.
Tip
Remember to change only one variable at a time.

Note
The LEDs on the front and back panel of the appliance enable you to determine the performance and operation of the appliance. For a description of these LEDs, see Reading the LEDs, page A-5.

When troubleshooting, check the following appliance subsystems first:

• Power and cooling systems—Check external power sources, power cables, and appliance fans. In addition, check for inadequate ventilation, blocked air circulation, excessive dust or dirt, fan failures, or any environmental conditions that might affect the power or cooling systems.

• Adapter card—Check the LEDs on the adapter card that can aid you to identify a failure.

• Cables—Verify that the external cables connecting the appliance to the network are all secure and in good order.

Troubleshooting the Power and Cooling Systems

The power LED and the fans can help you troubleshoot a power problem. Check the following items to help isolate the problem:

• When the Cisco ISE 3300 Series appliance is connected to the power source, is the appliance power LED on the front panel on? If not, check the AC power cord connection; if the power LED is still off, the problem might be caused by a power supply failure.

• Does the appliance shut down after being on for only a short time?
  
  – Check if this is an environmentally induced shutdown. For more information, see Environmental Reporting Features, page A-4 section.
  
  – Check the cooling fans. If the cooling fans are not working, the appliance will overheat and shut itself down.

  If the cooling fans are not working, you need to check the power supply connection to the cooling fans.

  Checking the power supply connection requires you to shut down the appliance, remove any external cables, and open up the appliance.

  – Ensure that the appliance intake and exhaust vents are all clear.

  – Check that the environmental site requirements have been met (see the Temperature and Humidity Guidelines, page 1-9).

• Does the appliance partially boot, but the LEDs do not light? Check for a power supply failure by inspecting the power LED on the front panel of the appliance:

  – If the LED is on, the power supply is functional.

  – If the LED is off, see the Cisco Information Packet for warranty information, or contact your Cisco customer service representative.
Environmental Reporting Features

The Cisco ISE 3300 Series appliance has protection circuits that monitor and detect excessive current, voltage, and temperature conditions inside the appliance.

If the power supply shuts down or latches off, an AC power cycle switches off for 15 seconds and switches on for 1 second to reset the power supply. The following conditions can cause abnormally high appliance temperatures:

- Cooling fan failure
- An air conditioner failure in the room where the appliance is installed
- Airflow blocked to cooling vents (intake or exhaust)

Take steps to correct any problems that you discover. For information about environmental operating conditions, see Temperature and Humidity Guidelines, page 1-9.

Troubleshooting Adapter Cards, Cables, and Connections

Network problems can be caused by an adapter card, cables or cable connections, or external devices such as a hub, wall jack, WAN interface, or terminal. Check for the following symptoms to help isolate a problem:

- Adapter card is not recognized by the Cisco ISE 3300 Series appliance:
  - Ensure that the adapter card is firmly seated in its slot.
  - Check the LEDs on the adapter card. Each adapter card has its own set of LEDs.
  - Verify that your software release supports the adapter card. See the documentation that was included with your adapter card.

- Adapter card is recognized, but interface ports do not initialize:
  - Ensure that the adapter card is firmly seated in its slot.
  - Check external cable connections.
  - Verify that your software release supports the adapter card. See the documentation that was included with your adapter card.

- The Cisco ISE 3300 Series appliance does not boot properly, or it constantly or intermittently reboots:
  - Ensure that the adapter card is firmly seated in its slot.
  - Check the appliance chassis or the application software. For warranty information, see the Cisco Information Packet publication that is shipped with your appliance or contact your Cisco customer service representative.

- If you are using the console port with a terminal, and the Cisco ISE 3300 Series appliance boots, but the console screen is frozen:
  - Check the external console connection.
  - Verify that the parameters for your terminal are set as follows:
    (a) The terminal should have the same data rate that the appliance has (9600 bps is the default)
    (b) 8 data bits
    (c) No parity generated or checked
    (d) 1 stop bit
• The Cisco ISE 3300 Series appliance powers on and boots only when an adapter card is removed. Check the adapter card. For warranty information, see the *Cisco Information Packet* publication that is shipped with your appliance or contact your customer service representative.

• The Cisco ISE 3300 Series appliance powers on and boots only when a particular cable is disconnected. There might be a problem with the cable. For warranty information, see the *Cisco Information Packet* publication that is shipped with your appliance or contact your Cisco customer service representative.

---

### Reading the LEDs

The LEDs on the Cisco ISE 3300 Series appliance serve the following purposes:

- Indicate that basic power is available to the appliance.
- Indicate the status of the hard disk drive, CD/DVD drive, and network activity.

### Front-Panel LEDs

The front-panel LEDs for the supported Cisco ISE 3300 Series appliances are described in tables with supporting figures in the following locations:

- Cisco ISE 3315 Front-Panel Features, page 1-6
- Cisco ISE 3355 Front-Panel Features, page 1-8
- Cisco ISE 3395 Front-Panel Features, page 1-12

### Rear-Panel LEDs

The rear-panel LEDs for the supported Cisco ISE 3300 Series appliances are described in tables with supporting figures in the following locations:

- Cisco ISE 3315 Rear-Panel Features, page 1-7
- Cisco ISE 3355 Rear-Panel Features, page 1-10
- Cisco ISE 3395 Rear-Panel Features, page 1-14
- Cisco ISE SNS 3415/3495 Front and Rear Panels, page 1-16

### Locating Appliance Serial Numbers

In Cisco ISE 3300 Series appliances, the serial number label is located on the front panel of each appliance, and these are shown in the following locations:

- Cisco ISE 3315 Serial Number Location, page 1-5
- Cisco ISE 3355 Serial Number Location, page 1-8
- Cisco ISE 3395 Serial Number Location, page 1-12
- Cisco ISE SNS 3415/3495 Front and Rear Panels, page 1-16
Cisco ISE Appliance Ports Reference

This appendix lists the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports that Cisco ISE uses for intranetwork communications with external applications and devices.

Table A-1 lists the ports by TCP and UDP port number, identifies the associated feature, service, or protocol, and describes any specific port-related information that applies to the four Gigabit Ethernet ports: GbEth0, GbEth1, GbEth2, and GbEth3. The Cisco ISE ports listed in this table must be open on the corresponding firewall. The ports list provides information that can be useful when configuring a firewall, creating access control lists (ACL), and configuring services on a Cisco ISE network.
## Table A-1  
**Cisco ISE Services and Ports**

<table>
<thead>
<tr>
<th>Cisco ISE Node</th>
<th>ISE Service</th>
<th>Ports on Gigabit Ethernet 0</th>
<th>Ports on Gigabit Ethernet 1</th>
<th>Ports on Gigabit Ethernet 2</th>
<th>Ports on Gigabit Ethernet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration ISE node</td>
<td>Administration</td>
<td>• TCP: 22 (Secure Shell [SSH] server)</td>
<td>Cisco ISE management is restricted to Gigabit Ethernet 0.</td>
<td>Cisco ISE management is restricted to Gigabit Ethernet 0.</td>
<td>Cisco ISE management is restricted to Gigabit Ethernet 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 80₁ (HTTP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 443₁ (HTTPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Port 80 is redirected to port 443 (not configurable).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Ports 80 and 443 support Admin web applications and are enabled by default.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication and Synchronization</td>
<td></td>
<td>• TCP: 443 (HTTPS SOAP)</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 1521² (Database Listener and AQ)</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internet Control Message Protocol (ICMP) (Heartbeat)</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td>• UDP: 161 (Simple Network Management Protocol [SNMP] QUERY)</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This port is route table dependent.</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
Table A-1  Cisco ISE Services and Ports (continued)

<table>
<thead>
<tr>
<th>Cisco ISE Node</th>
<th>ISE Service</th>
<th>Ports on Gigabit Ethernet 0</th>
<th>Ports on Gigabit Ethernet 1</th>
<th>Ports on Gigabit Ethernet 2</th>
<th>Ports on Gigabit Ethernet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring ISE node</td>
<td>Administration</td>
<td>• TCP: 22 (SSH server)</td>
<td>• TCP: 22 (SSH server)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 801 (HTTP)</td>
<td>• TCP: 801 (HTTP)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 4433 (HTTPS)</td>
<td>• TCP: 4433 (HTTPS)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td>Replication and Synchronization</td>
<td>• TCP: 443 (HTTPS SOAP)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ICMP (Heartbeat)</td>
<td>• ICMP (Heartbeat)</td>
<td>• ICMP (Heartbeat)</td>
<td>• ICMP (Heartbeat)</td>
</tr>
<tr>
<td>Logging</td>
<td></td>
<td>• UDP: 20514 (Syslog)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note  Default ports are configurable for external logs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Alarms/activemq: TCP: 62627 (ISE 1.1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Service ISE node</td>
<td>Administration</td>
<td>• TCP: 22 (SSH server)</td>
<td>• TCP: 22 (SSH server)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 801 (HTTP)</td>
<td>• TCP: 801 (HTTP)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 4433 (HTTPS)</td>
<td>• TCP: 4433 (HTTPS)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td>Replication and Synchronization</td>
<td>• TCP: 443 (HTTPS SOAP)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
<td>• TCP: 15212 (Database Listener and AQ)</td>
</tr>
<tr>
<td>Session</td>
<td></td>
<td>• UDP: 1645,1812 (RADIUS Authentication)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 1646, 1813 (RADIUS Accounting)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 1700, 3799 (RADIUS change of authorization [CoA])</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note  UDP port 1700 is not configurable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 88, 389, 464 (Outbound AD and Lightweight Directory Access Protocol [LDAP])</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 30514 (Syslog))</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note  This is internal via session services.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ISE Node</td>
<td>ISE Service</td>
<td>Ports on Gigabit Ethernet 0</td>
<td>Ports on Gigabit Ethernet 1</td>
<td>Ports on Gigabit Ethernet 2</td>
<td>Ports on Gigabit Ethernet 3</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Policy Service ISE node (continued)</td>
<td>Guest and Sponsor Portal</td>
<td>• TCP: 8443 (HTTPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note TCP port 8443 is enabled by default and configurable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Provisioning</td>
<td></td>
<td>• TCP: 80, 8443 (web or Cisco NAC agent installation)</td>
<td>• TCP: 8905 (Cisco NAC agent update)</td>
<td>• TCP: 8905 (Cisco NAC agent update)</td>
<td>• TCP: 8905 (Cisco NAC agent update)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note TCP port 8443 is enabled by default, configurable, and corresponds to Guest configuration</td>
<td>• TCP: 8909 and UDP: 8909 (web, Cisco NAC Agent, supplicant provisioning wizard installation)</td>
<td>• TCP: 8909 and UDP: 8909 (web, Cisco NAC Agent, supplicant provisioning wizard installation)</td>
<td>• TCP: 8909 and UDP: 8909 (web, Cisco NAC Agent, supplicant provisioning wizard installation)</td>
</tr>
<tr>
<td>Posture and Heartbeat</td>
<td></td>
<td>• TCP: 8905 Discovery (HTTPS)</td>
<td>• UDP: 8905 (Layer 2) Discovery (SWISS)</td>
<td>• UDP: 8905 PRA/Keep-alive (SWISS)</td>
<td></td>
</tr>
</tbody>
</table>

Table A-1 Cisco ISE Services and Ports (continued)
**Table A-1 Cisco ISE Services and Ports (continued)**

<table>
<thead>
<tr>
<th>Cisco ISE Node</th>
<th>ISE Service</th>
<th>Ports on Gigabit Ethernet 0</th>
<th>Ports on Gigabit Ethernet 1</th>
<th>Ports on Gigabit Ethernet 2</th>
<th>Ports on Gigabit Ethernet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Service ISE node</td>
<td>Profiler</td>
<td>• UDP: 9996 (NetFlow)</td>
<td>• UDP: 9996 (NetFlow)</td>
<td>• UDP: 9996 (NetFlow)</td>
<td>• UDP: 9996 (NetFlow)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 67 (DHCP)</td>
<td>• TCP: 80, 8080 (DHCPSPAN probe and HTTP)</td>
<td>• UDP: 30514 (RADIUS logging)</td>
<td>Note This is internal via session services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note This port is configurable.</td>
<td>• NMAP uses ports 0-65535⁴ (outbound).</td>
<td>• UDP: 53 (DNS lookup)</td>
<td>• UDP: 161 (SNMP QUERY)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note This port is route table dependent.</td>
<td>Note This port is route table dependent.</td>
<td>Note This port is route table dependent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 162 (SNMP trap)</td>
<td>• UDP: 162 (SNMP trap)</td>
<td>• UDP: 162 (SNMP trap)</td>
<td>• UDP: 162 (SNMP trap)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
<td>Note This port is configurable.</td>
</tr>
<tr>
<td>Clustering</td>
<td></td>
<td>• UDP: 45588, 45590</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inline Posture ISE node</td>
<td>Administration</td>
<td>• TCP: 22 (SSH server)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP: 8443 (HTTPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note It is used by the Administra-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion ISE node.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inline Posture</td>
<td></td>
<td>• UDP: 1645, 1812 (RADIUS proxy for authentication)</td>
<td>• UDP: 1645, 1812 (RADIUS proxy for authentication)</td>
<td>• UDP: 1645, 1812 (RADIUS proxy for authentication)</td>
<td>• UDP: 1645, 1812 (RADIUS proxy for authentication)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 1646, 1813 (RADIUS proxy for accounting)</td>
<td>• UDP: 1646, 1813 (RADIUS proxy for accounting)</td>
<td>• UDP: 1646, 1813 (RADIUS proxy for accounting)</td>
<td>• UDP: 1646, 1813 (RADIUS proxy for accounting)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP: 1700, 3799 (RADIUS CoA)</td>
<td>• RADIUS CoA: Not applicable</td>
<td>• RADIUS CoA: Not applicable</td>
<td>• RADIUS CoA: Not applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TCP 9090: (Redirect)</td>
<td>• TCP 9090: (Redirect)</td>
<td>• TCP 9090: (Redirect)</td>
<td>• TCP 9090: (Redirect)</td>
</tr>
</tbody>
</table>

**Note** High Availability and Management services are Inline Posture-specific and do not apply to any other Cisco ISE node types.
### Table A-1  
*Cisco ISE Services and Ports (continued)*

<table>
<thead>
<tr>
<th>Cisco ISE Node</th>
<th>ISE Service</th>
<th>Ports on Gigabit Ethernet 0</th>
<th>Ports on Gigabit Ethernet 1</th>
<th>Ports on Gigabit Ethernet 2</th>
<th>Ports on Gigabit Ethernet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability</td>
<td>TCP: 9090 (Redirect)</td>
<td>TCP: 9090 (Redirect)</td>
<td>UDP: 694 (Heartbeat)</td>
<td>UDP: 694 (Heartbeat)</td>
<td></td>
</tr>
</tbody>
</table>

1. Because Inline Posture nodes do not support the Administration persona, they will not have access to this port.
2. Because Inline Posture nodes do not support the database listener function, they will not have access to this port.
3. NMAP OS Scan uses ports 0.65535 to detect endpoint operating system.
Installing Cisco ISE on Cisco NAC and Cisco Secure ACS Appliances

This appendix describes the process for performing an initial (or fresh) installation of the Cisco ISE 3300 Series software from the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD on the following supported Cisco Secure ACS and Cisco NAC Appliance platforms:

- Cisco Secure ACS-1121
- Cisco NAC-3315
- Cisco NAC-3355
- Cisco NAC-3395

Installing the Cisco ISE 3300 Series software on a Cisco Secure ACS or Cisco NAC appliance is a simplified process because the underlying hardware on which the Cisco ISE software will be installed is the same physical device type:

- Cisco Secure ACS-1121 and Cisco NAC-3315 appliances are based on the same physical hardware that are used for small Cisco ISE network deployments (Cisco ISE 3315 appliance).
- Cisco NAC-3355 and Cisco NAC-3395 appliances are based on the same physical hardware that are used for medium and large Cisco ISE network deployments (Cisco ISE 3355 and Cisco ISE 3395 appliances, respectively).

For specific details about the Cisco ISE 3300 Series hardware platforms, see Table 1-1 on page 1-2.

This appendix describes the following procedures:

- **Installing Cisco ISE Software on a Reimaged Cisco Secure ACS Appliance, page A-2**—Provides instructions for installing the Cisco ISE software with the use of the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, configuring the appliance by using the Setup program, and verifying the configuration process.

- **Installing Cisco ISE Software on a Reimaged Cisco NAC Appliance, page A-2**—Provides instructions for installing the Cisco ISE software with the use of the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, including how to reset the RAID configuration on the Cisco NAC appliance before you can complete the reimage process.

To reimage a Cisco Secure ACS or Cisco NAC appliance as a Cisco ISE 3300 Series appliance, install the Cisco ISE software, and use the Setup program to configure the appliance.
Installing Cisco ISE Software on a Reimaged Cisco Secure ACS Appliance

This section provides the procedure for reimaging an existing Cisco Secure ACS appliance as a Cisco ISE 3300 Series, Release 1.0, appliance.

To reimage a Cisco Secure ACS appliance as a Cisco ISE 3300 Series appliance, complete the following steps:

1. If the Cisco Secure ACS appliance is on, turn off the appliance.
2. Turn on the Cisco Secure ACS appliance.
3. Press F1 to enter the BIOS setup mode.
4. Use the arrow key to navigate to Date and Time and press Enter.
5. Set the time for your appliance to the UTC/GMT time zone.

Note: We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

6. Press Esc to exit to main BIOS menu.
7. Press Esc to exit from the BIOS setup mode.
8. Perform the instructions described in Before Configuring a Cisco ISE Series Appliance, page 1-1.
9. Perform the instructions described in Understanding the Setup Program Parameters, page 1-3.

Installing Cisco ISE Software on a Reimaged Cisco NAC Appliance

This section provides the procedure for reimaging an existing Cisco NAC appliance as a Cisco ISE 3300 Series, Release 1.0, appliance.

To reimage a Cisco NAC appliance as a Cisco ISE appliance, complete the following steps:

1. If the Cisco NAC appliance is on, turn off the appliance.
2. Turn on the Cisco NAC appliance.
3. Press F1 to enter the BIOS setup mode.
4. Using the arrow key, navigate to Date and Time and press Enter.
5. Set the time for your appliance to the UTC/GMT time zone.
### Note
We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

**Step 6**  
Press Esc to exit to main BIOS menu.

**Step 7**  
Press Esc to exit from the BIOS setup mode.

### Note
If the Cisco ISE DVD installation process returns a message indicating that “The installer requires at least 600GB disk space for this appliance type,” you may need to reset the RAID settings on the appliance to facilitate installation as described in Resetting the Existing RAID Configuration on a Cisco NAC Appliance.

**Step 8**  
Perform the instructions that are described in Before Configuring a Cisco ISE Series Appliance, page 1-1.

**Step 9**  
Perform the instructions that are described in Understanding the Setup Program Parameters, page 1-3.

**Step 10**  
Perform the instructions that are described in Verifying the Configuration Process, page 1-17.

---

### Resetting the Existing RAID Configuration on a Cisco NAC Appliance

**To reset the RAID settings on a Cisco NAC appliance:**

**Step 1**  
Reboot the Cisco NAC appliance with the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD installed.

**Step 2**  
When you see the RAID controller version information appear in the CLI, press Ctrl+C. The RAID controller version information appears, displaying a label like LSI Corporation MPT SAS BIOS, and the LSI Corp Config Utility becomes active.

**Step 3**  
Press Enter to specify the default controller. (The highlighted controller name should read something similar to SR-BR10i.) A screen containing the Cisco NAC appliance adapter information appears.

**Step 4**  
Arrow down to “RAID properties” and press Enter.

**Step 5**  
Press Enter again on “Manage Array.”

**Step 6**  
Arrow down to the “Delete Array” option and press Enter.

**Step 7**  
Enter “Y” to confirm that you want to delete the existing RAID Array.

**Step 8**  
Press Esc twice to exit the RAID configuration utility. You are prompted with an Exit the Configuration Utility and Reboot? prompt.

**Step 9**  
Press Enter. The Cisco NAC appliance reboots. As long as the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD is still installed, the appliance automatically boots to the install menu.

**Step 10**  
Press 1 to begin Cisco ISE installation.
INDEX

A

adapter cards
  troubleshooting G-4
airflow
  guidelines A-8
altitude
  guidelines E-4

B

back panel C-9
beeps for USB devices D-2

cable
  connecting C-8
  management C-14
  troubleshooting G-4

Cable management arm installation B-6
checking
  LEDs C-16
checklist, installation A-14
checklist, power up C-14
Cisco ISE deployment 1-1
configuration
  site A-8
connecting
  cables C-8
  network interface C-10
connections
  troubleshooting G-4

considerations
  power A-9
console port, pinouts
  serial C-12
cooling system
  troubleshooting G-3
corrosion
  preventing damage E-2

corrosion
  preventing damage E-2

dust
  preventing damage E-4

electricity
  safety with A-3

electromagnetic interference
  See EMI
electrostatic discharge A-5
  See ESD
EMI
  preventing effects of E-4
environment
  maintaining E-1
  site A-8
environmental
  features G-4
  specifications (table) A-9
environmental specifications F-1
equipment

Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x

OL-26137-01
IN-1
racks
  rack-mounting  A-9
  safety with  A-3

ESD
  preventing damage  E-4
  preventing effects of  A-5, E-4

F
features
  environmental reporting  G-4
four-post hardware kit
  rack-mount  C-3
four-post rack, mounting appliance on  C-2
front-panel
  LEDs
    troubleshooting  G-5

G
grounding (warning)  C-14
guidelines
  airflow  A-8
  lifting  A-5
  rack installation  A-7
  rack-mounting configuration  C-1
  safety  A-1
  temperature maintenance  E-3

H
hardware
  troubleshooting procedures  G-1
humidity
  maintenance guidelines  E-4

I
information packet and warranty  A-11
installation
  cable management arm  B-6
  checklist  A-14
  initial power-on and setup  D-1
  IP settings  D-6
  NIC modes  D-5
  NIC redundancy  D-6
  power cables  D-1
  rack installation  B-4
  rack requirements  B-4
  required equipment  B-4
  slide rails  B-4
  unpacking and inspection  B-2
  verification  3-17
  installing Cisco ISE
    setup program  3-3
    post-installation tasks  5-1
  IP settings, DHCP or static  D-6

K
kit
  mounting  C-2
  rack-mount hardware (table)  C-3

L
LEDs
  checking  C-16
lifting guidelines  A-5
location
  serial number  2-1, 2-5, 2-8, 2-12, 2-15, G-5
log, site  A-14
<table>
<thead>
<tr>
<th>M</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>magnetism</td>
<td></td>
</tr>
<tr>
<td>preventing effects of</td>
<td>E-5</td>
</tr>
<tr>
<td>maintenance</td>
<td>E-1</td>
</tr>
<tr>
<td>temperature</td>
<td>E-3</td>
</tr>
<tr>
<td>management</td>
<td></td>
</tr>
<tr>
<td>cable</td>
<td>C-14</td>
</tr>
<tr>
<td>MOP</td>
<td></td>
</tr>
<tr>
<td>method of procedure</td>
<td>A-10</td>
</tr>
<tr>
<td>motherboard beeps</td>
<td>D-2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>network interface</td>
<td></td>
</tr>
<tr>
<td>connecting</td>
<td>C-10</td>
</tr>
<tr>
<td>NIC</td>
<td></td>
</tr>
<tr>
<td>LEDs</td>
<td></td>
</tr>
<tr>
<td>troubleshooting</td>
<td>G-5</td>
</tr>
<tr>
<td>NIC 1 and NIC 2</td>
<td></td>
</tr>
<tr>
<td>RJ-45 pinout</td>
<td>C-11</td>
</tr>
<tr>
<td>NIC modes, setting</td>
<td>D-5</td>
</tr>
<tr>
<td>NIC redundancy</td>
<td>D-6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>packing list</td>
<td>B-2</td>
</tr>
<tr>
<td>physical specifications</td>
<td>F-1</td>
</tr>
<tr>
<td>planning</td>
<td></td>
</tr>
<tr>
<td>site</td>
<td>A-6</td>
</tr>
<tr>
<td>post-installation tasks</td>
<td>5-1</td>
</tr>
<tr>
<td>power</td>
<td></td>
</tr>
<tr>
<td>connecting power cords</td>
<td>D-1</td>
</tr>
<tr>
<td>considerations</td>
<td>A-9</td>
</tr>
<tr>
<td>specifications</td>
<td>F-2</td>
</tr>
<tr>
<td>power lines (warning)</td>
<td>A-3</td>
</tr>
<tr>
<td>power source interruptions</td>
<td></td>
</tr>
<tr>
<td>preventing damage from</td>
<td>E-5</td>
</tr>
<tr>
<td>power supplies (warning)</td>
<td>A-3</td>
</tr>
</tbody>
</table>

| power supply (warning)       | A-3, C-14|
| power system                 |   |
| troubleshooting              | G-3|
| power up                     |   |
| procedure                    | C-15|
| precautions                  |   |
| general precautions          | A-1|
| problem solving              |   |
| See troubleshooting procedure|   |
| method of                    | A-10|
| power up                     | C-15|

<table>
<thead>
<tr>
<th>R</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>rack</td>
<td></td>
</tr>
<tr>
<td>enclosed (do not use)</td>
<td>A-7</td>
</tr>
<tr>
<td>four-post (open)</td>
<td>A-7</td>
</tr>
<tr>
<td>rack, mounting on four-post</td>
<td>C-2</td>
</tr>
<tr>
<td>rack installation</td>
<td>B-4</td>
</tr>
<tr>
<td>guidelines</td>
<td>A-7</td>
</tr>
<tr>
<td>rack-mount</td>
<td></td>
</tr>
<tr>
<td>four-post hardware kit</td>
<td>C-3</td>
</tr>
<tr>
<td>rack-mounting configuration</td>
<td></td>
</tr>
<tr>
<td>guidelines</td>
<td>C-1</td>
</tr>
<tr>
<td>rack requirements</td>
<td>B-4</td>
</tr>
<tr>
<td>radio frequency interference.</td>
<td>See RFI</td>
</tr>
<tr>
<td>removing</td>
<td></td>
</tr>
<tr>
<td>Cisco ISE 3300 Series appliance</td>
<td>E-7</td>
</tr>
<tr>
<td>required equipment</td>
<td></td>
</tr>
<tr>
<td>installation</td>
<td>B-4</td>
</tr>
<tr>
<td>restricted access (warning)</td>
<td>A-3, A-6, C-1</td>
</tr>
<tr>
<td>RFI</td>
<td></td>
</tr>
<tr>
<td>preventing effects of</td>
<td>E-4</td>
</tr>
<tr>
<td>RJ-45 pinout</td>
<td></td>
</tr>
<tr>
<td>NIC 1 and NIC 2</td>
<td>C-11</td>
</tr>
</tbody>
</table>
Index

S

safety guidelines A-1

SELV circuits (warning) A-3

serial

console port, pinouts C-12

serial number

location 2-1, 2-5, 2-8, 2-12, 2-15, G-5

setting NIC modes D-5

setting NIC redundancy D-6

setting UDI

for Cisco ISE on Cisco NAC or Cisco Secure ACS appliances I-2

site

configuration A-8

environment A-8

maintenance factors E-1

log A-14

planning A-6

requirement, MOPs A-10

slide rail installation B-4

specifications

environmental F-1

physical F-1

power F-2

static IP, setting D-6

connections G-4

cooling system G-3

Ethernet LEDs G-5

front-panel LEDs G-5

power system G-3

U

unpacking

checking shipment A-11

unpacking the server B-2

upgrading

post-installation tasks 5-1

V

VMware

configuring 4-7

hardware requirements 4-1

installing 4-1

installing the Cisco ISE appliance 4-16

W

warranty A-11

T

temperature

maintenance guidelines E-3

temperature and humidity guidelines A-9

tools and equipment

required A-13

trained and qualified (warning) C-1

troubleshooting

adapter cards G-4

cables G-4