Preface

CHAPTER

This preface includes the following sections:

Overview

This guide explains how to implement Cisco Hosted Unified Communications Services (Hosted UCS) Release 7.1(a). It includes background information about the hardware and software components included in the Hosted UCS 7.1(a) platform and explains how these components fit together. It also provides a high-level overview of the procedures required to configure each component.

This document assumes that the high-level design, the low-level design, and the dial plan are complete.

Audience

This document is written for Cisco Advanced Services (AS), system integrators, Cisco partners, and Cisco customers who are interested in implementing Cisco Hosted UCS 7.1(a).

This document is to be used with the documentation for the individual components of the Hosted UCS 7.1(a) platform after completing the high-level design (HLD) and low-level design (LLD) for a specific customer implementation.

Organization

This document is organized as follows:

Chapter/Appendix	Description
Chapter 1, "Introducing Cisco Hosted Unified Communications Services"	Provides a high-level view of the architecture and overall operation of Cisco Hosted Unified Communications Services (Hosted UCS) 7.1(a).
Chapter 2, "Configuring Hosted Unified Communications Services Components Before Loading Bulk Data"	Describes the high-level tasks required to apply static configuration to Hosted UCS software components.
Chapter 3, "Managing the Hosted Unified Communications Services Platform with VisionOSS USM"	Summarizes the options provided by VisionOSS USM for managing the components of the Hosted UCS platform.
Chapter 4, "Using Bulk Loaders for the Initial Configuration of Hosted Unified Communication Services Components"	Explains how to perform the initial configuration of the Hosted UCS platform components by loading bulk data using VisionOSS USM.
Chapter 5, "Backing Up and Reinitializing Hosted Unified Communications Services Components"	Explains how to clear and reinitialize the components of a Hosted UCS platform and provides general recommendations for upgrading from previous versions.
Appendix A, "Sample Hosted Unified Communications Services Build of Materials"	Provides the standard bill of materials (BOM) for the Hosted UCS 7.1(a) platform.

Related Documentation

The following documentation provides additional information about the Hosted UCS 7.1(a) platform:

- *Release Notes for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a)*
- *Software Support Matrix for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a)*
- *Solutions Reference Network Design for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a)*
- *Provisioning Guide for Cisco Hosted Unified Communications Services, Release 7.1(a)*

Obtaining Documentation and Technical Assistance

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products

- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Document Conventions

This guide uses the following conventions to convey instructions and information:

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.