Cisco Unified Communications Domain Manager Planning and Install Guide, Release 10.6(1)

First Published: June 30, 2015

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

CONTENTS

Preface

PART I

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

Preface

Purpose

This document provides instructions for installing and configuring Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) in Cisco Hosted Collaboration Solution (HCS). This guide includes information on installing and upgrading HCM-F and procedures to use to configure HCM-F using the administrative interface.

Audience

This document is intended for service providers who are responsible for installing, upgrading, and configuring HCM-F. This guide requires knowledge of Cisco Hosted Collaboration Solution (HCS).

Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.

Convention	Description
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` `font`	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Non-printing characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Obtain Documentation and Submit 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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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 using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

PART I

Planning

CHAPTER 1

Deployment Topologies

Deployment Topologies

Cisco Unified Communications Domain Manager 10.6(x) is deployed either as a single node, or as a cluster of multiple nodes with High Availability (HA) and Disaster Recovery (DR) qualities.

Each node can be assigned one or more of the following functional roles:

WebProxy

load balancing across multiple application roles

Standalone

combines the Application and Database roles for use in a nonclustered environment

Unified

similar to the Standalone role combining Application and Database roles, but clustered with other nodes to provide HA and DR capabilities

The nginx web server is installed on the WebProxy, Standalone, and Unified node, but is configured differently for each role.

In a clustered environment containing multiple Application or Unified nodes, a load balancing function is required to offer HA (High Availability providing failover between redundant roles). Either an external third-party load balancer (not recommended) or one or more WebProxy nodes can provide the load balancing function.

The following deployment topologies are defined:

Test or Small Production

a single Standalone node with Application and Database roles combined

Production with Unified nodes

a clustered six node system consisting of:

- 4 Unified nodes (each with combined Application and Database roles)
- 2 WebProxy nodes to provide load balancing. The two WebProxy nodes can be omitted if an external load balancer is available.

Cisco supports deployment of either the WebProxy node or a DNS load balancer. Here are some considerations in choosing a WebProxy node vs. DNS:

- The Proxy takes load off the Unified node to deliver static content (HTML/JAVA scripts). When using DNS or a third-party load balancer, the Unified node has to process this information.
- DNS does not know the state of the Unified node.
- The WebProxy detects if a Unified node is down or corrupt. In this case, the WebProxy will select the next Unified node in a round robin scheme.

Production with split Application and Database roles

Some customers requiring a multitiered architecture that supports geo-redundancy, high availability, and a separation of the presentation tier, application tier, and data tier. In this case Cisco recommends a clustered seven node system consisting of:

- 2 Application Nodes
- 3 Database nodes
- 2 WebProxy nodes (if an external load balancer is not available).

Cisco recommends that you run no more than two Unified nodes and one WebProxy node on a physical server (VMware server). Cisco also recommends that the disk subsystems be unique for each Unified node.

Multinode Cluster with Unified Nodes

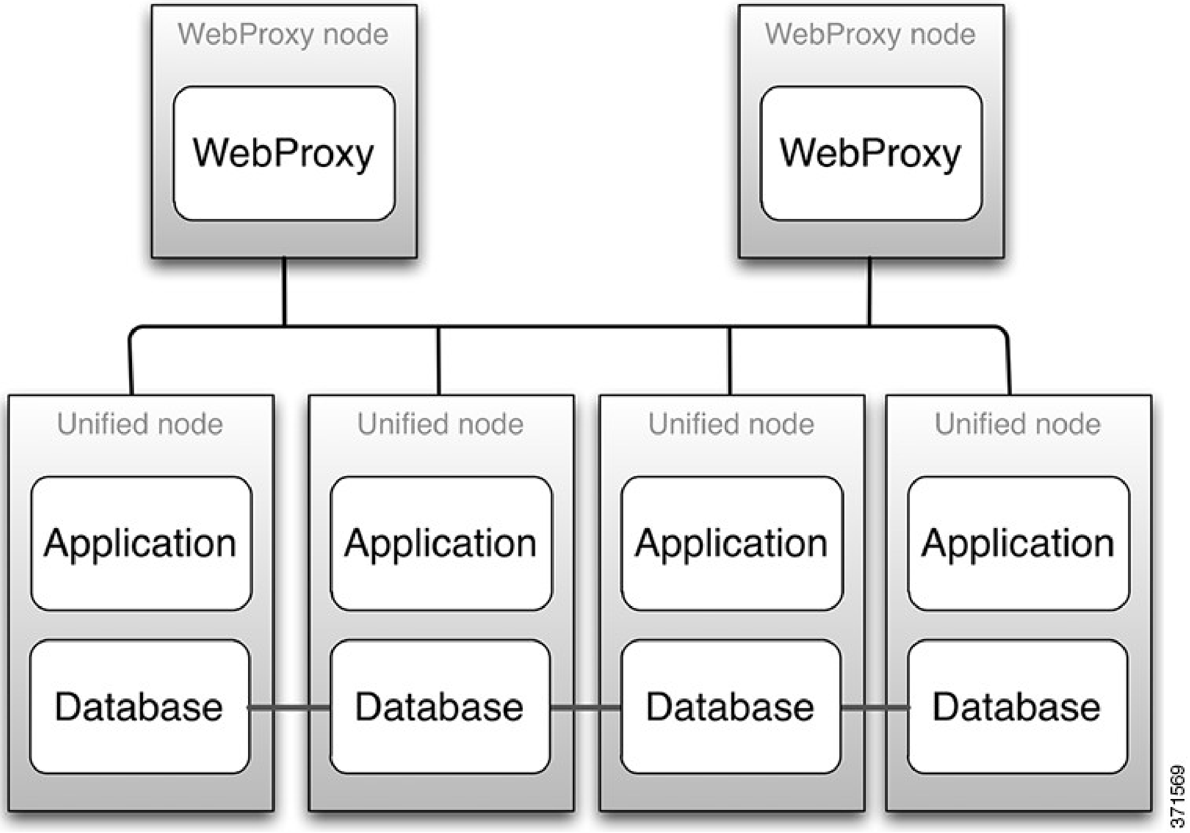
The recommended multinode deployment using Unified nodes has the following characteristics:

- Four Unified nodes - each node combining Application and Database roles - are clustered and split over two geographically disparate locations.
- Two Web Proxy nodes to provide High Availability that ensure an Application role failure is gracefully handled. It may be omitted if an external load balancer is available.
- Web Proxy and Unified nodes can be contained in separate firewalled networks.
- Database synchronization takes places between all Database roles, thus offering Disaster Recovery, and High Availability.
- All nodes in the cluster are active.

Primary and fall-back Secondary Database servers can be configured manually.

Note For a geo-redundant multinode deployment, please contact your Cisco support representative.

Figure 1: A Graphical Representation of a Recommended Multinode Cluster



Note WebProxies can be configured to load balance across two or four Unified nodes.

Clustering Considerations

The cluster contains multiple nodes that can be contained in separate firewalled networks.

Open network ports on firewalls to allow internode communication. Port requirements are described in the Platform Guide.

All communication between nodes is encrypted.

Node type	Ports
WebProxy	22 (SSH and SFTP), 80 (HTTP), 161 and 162 (SNMP), 443 and 8443 (HTTPS)
Unified	22 (SSH and SFTP), 80 (HTTP), 161 and 162 (SNMP), 443 and 8443 (HTTPS), 27019, 27020, and 27030 (database)

- 22/SSH is used for remote administration.
- 80 and 443 are used for the web server.
- 161 and 162 are used for sending and receiving SNMP.
- 8443 is used for intercluster communication.
- 27019, 27020, and 27030 are used for database queries and replication.

Cisco Unified Communications Domain Manager 10.6(x) Redundancy and Disaster Recovery

High Availability (HA) is an approach to IT system design and configuration that ensures Cisco Unified Communications Domain Manager 10.6(x) is operational and accessible during a specified timeframe. High Availability is achieved using redundant hardware and resources. Cisco recommends the use of two physical data centers, where the primary site contains three VMs and the secondary site contains three VMs. If there is a failure, an automatic failover to the secondary DR (Disaster Recovery) site takes place.

Web server proxy nodes perform load-balancing between application roles, so that load is distributed. During provisioning, the web server proxy is provided with all the IP addresses of the application nodes. The web server software then does load balancing among these nodes, according to its configuration. If a node fails to respond in a set time, the proxy sends the transaction to another node. If an Application role is lost, the WebProxy transparently bypasses the faulty Application role.

The proxy web server that is configured to be located in the primary site normally load balances to the two unified nodes in the primary site. The proxy web server falls back to the two nodes in the Disaster Recovery site if the nodes in the primary site are down. The web proxy nodes in the secondary site defaults load balancing to the two unified nodes configured for the secondary site.

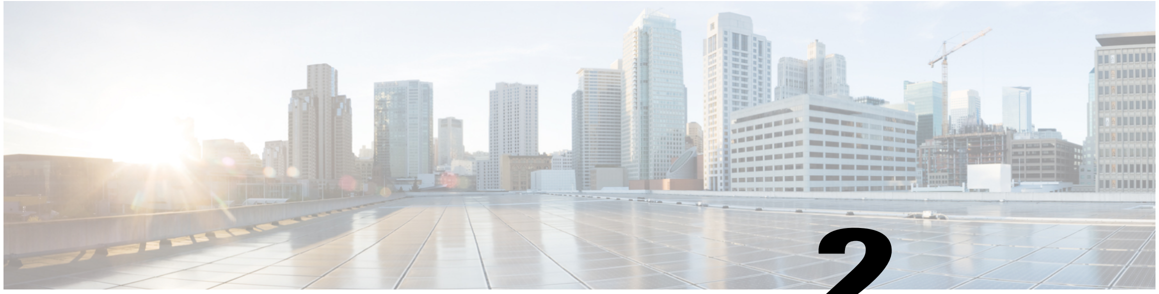
Data is replicated between unified node roles, and role failure is recoverable. Data replication is done using the database replication facility. Automatic failover between unified node roles occurs while there is greater than 50% unified node role availability. Once there is insufficient role availability, the system must be manually reprovisioned.

HA can be increased by adding nodes to the cluster. Application performance and availability can be increased by adding more application role servers.

Backups can be scheduled to run automatically across the cluster. Backups include application data, configuration, and software. Backups can take place to both local disk and remote network location. Every node upgrade includes a snapshot backup which allows any upgrade to be rolled back.

Capacity Considerations

For capacity considerations, see *Cisco Hosted Collaboration Solution, Release 10.6(1) Capacity Planning Guide*.



CHAPTER 2

Hierarchy

Understanding Hierarchy

It is important to understand hierarchy used in Cisco Unified Communications Domain Manager 10.6(x) to successfully provision collaboration services.

Hierarchy levels are used to organize configuration tasks and control scoping visibility.

There are four standard hierarchy levels:

- Provider
- Reseller (optional)
- Customer
- Site

The order of the hierarchy is maintained. Provider is the top level of the hierarchy. Reseller is beneath Provider, but is optional. Customer is beneath Provider or Reseller. Site is beneath Customer.

Intermediate nodes can be created between the standard hierarchy nodes to provide logical grouping of lower hierarchy nodes. For instance, the Provider could create intermediate nodes to group Customers by industry, or a Customer could create intermediate nodes to group Sites by region.

Each hierarchy node, standard and intermediate, can have an administrator to manage that node and the hierarchy beneath that node. The administrator's scope does not include other nodes at the same level. Thus, an administrator for Customer A can see Customer A and Customer A's sites, but cannot see Customer B or Customer B's Sites.

Administrators at the standard levels have dedicated menu layouts, according to the role assigned when the node is created. So the Provider administrator's menu layout is not the same as a Customer administrator's menu layout.

The four standard hierarchy nodes are automatically synchronized with the HCM-F hierarchy. Site nodes are mapped to Locations in HCM-F.

Navigating the Hierarchy

Navigate through the hierarchy by using the hierarchy bar at the top of the page. Each hierarchy node selection from the bar that is a parent node may further enable a drop-down list to select its child node.

Use the tree icon on the hierarchy bar at the top of the page to show a tree view of the entire hierarchy. Choose a hierarchy node on the tree to navigate to the node.

The hierarchy level to which an object belongs is indicated in a list view of the objects in the Hierarchy column. The hierarchy is indicated in a dot notation in the format`<System>.<Provider>.<Reseller>.<Customer>.<Site>`, for example `sys.hcs.VS-P1.VS-OB.GenCorp.GenCorp-EMEA.GenCorp-London`.

Manage the Hierarchy Structure

Hierarchy levels are created and deleted by adding and deleting Providers, Resellers, Customers, Sites, and Intermediate nodes. Permissions for these operations are available to administrators that are configured at higher levels in the hierarchy. For example, Provider administrators have permission to create and delete Resellers; both Provider and Reseller administrators have permission to create and delete Customers; etc. These operations a available from the **Provider Management**, **Reseller Management**, **Customer Management**, and **Site Management** menu items. Note that the Provider Management menu item is only available to the built-in hcsadmin account.

Each business entity that is created (Provider, Reseller, Customer, Site) will create a new node in the hierarchy that will appear in the hierarchy bar at the top of the Cisco Unified Communications Domain Manager user interface. New intermediate nodes can be created between the standard nodes using the **Hierarchy Management** menu item. Deleting both standard hierarchy nodes and intermediate nodes is done with a special cascade delete page available in each of the **Hierarchy Management** menu items. For example: **Site Management** > **Delete Site**, **Customer Management** > **Delete Customer**, and **Hierarchy Management** > **Delete Intermediate Node**.

CHAPTER 3

Multi-tenancy within Cisco Unified Communications Domain Manager

Data Partitioning

Data in the multitenant system is "partitioned" by a means of fully configurable hierarchy nodes.

The system can model the hierarchical nature of various businesses and manage the allocation of infrastructure. This infrastructure includes network devices, users, and other entities in the system. Hierarchy rules can be applied to various models in the system including creating hierarchy nodes, hierarchy node types (for example: provider, reseller, customer).

Devolved administration is enabled by creating administrators with different roles for different types of hierarchy nodes. For example:

- An administrator is responsible for the setup of the overall system.
- Provider administrators own and manage infrastructure and define services available to resellers or customers.
- Resellers offer the infrastructure and services to customers or enterprises.
- Customers and enterprises are grouped into various groupings.
- Groupings such as divisions or branches belong to customers.
- Physical locations hold users and phones.
- Users consume services and manage their own configurable settings.

The flexible mechanism is used to define as many levels as needed. Hierarchy node instances of different types can be created and the required business rules can be defined.

Parent-Child Relationships

All entities in the system reside at a specific hierarchy and the data displayed is within the scope of the specified hierarchy. Every entity in the system - including users, device models, and network components - has a parent hierarchy defined. A user is for example provisioned with a specific hierarchy node in a parent-child relationship. Usernames must be unique within a specific hierarchy.

The hierarchy at which an entity resides is always displayed in the list view of the item. For example, to see at which hierarchy users are defined in the system, sign in to the system as a provider, reseller, customer, or site administrator and navigate to **User Management** > **Users**. The resulting list view shows the hierarchy at which each user resides. Furthermore, the users displayed are scoped by the setting of the hierarchy bar at the top of the UI. Only users that reside at the current setting of the hierarchy bar and below are displayed in the list view.

Security

The system defaults to a self-signed web certificate.

- A unique web certificate can be copied onto the host using **scp** or **system download**.
- The web certificate is installed using **web cert add <certificate file>**.

SSH keys are used for sftp, passwordless ssh, and scp.

- Keys can be created using **keys createkey**.
- The public key copied to a remote host using **keys sendkey <user@host>**.
- A host can be authorized for incoming connections using **keys add <host>**.

The system uses an internal repository to check whether security package updates are available.

More repositories can be added with:

security repos add <repo-name> <url> <distro> <section> <categories>

For example, **security repos mymirror add http://archive.ubuntu.com/ubuntu/ precise-updates main universe multiverse**

In order to check whether there are security updates available, use:

security check

The system can be updated using:

security update

CHAPTER 4

Authentication Management

User Authentication

When signing in to the user interfaces, the credentials of the user can be authenticated based on user credentials in:

- The internal system database
- An LDAP-based external authentication server
- A SAML-based identity management server

Administrator users are users that are able to sign in to the administrator interface. Presence of an administrator interface means that a system user instance exists.

Subscribers are system users that have, and are linked to, user accounts in one or more UC applications. Subscriber management supports the management of UC application user accounts that in turn may also be configured for local, LDAP or SAML authentication.

API users are system users that connect directly to Cisco Unified Communications Domain Manager 10.6(x) using the API. The system controls access to its service through HTTP basic authentication. The technique is defined in section 11.1 of RFC1945.

Credential Policies

Cisco Unified Communications Domain Manager helps secure user accounts by authenticating user sign-in credentials before allowing system access. Administrators can specify settings for, among other things, failed sign-in attempts, lockout durations, password reset questions, and so on. The number of questions in the Password Reset Question Pool must be equal to (or more than) the number set in the **Number of Questions Asked During Password Reset** field. Collectively, these rules form a credential policy, which can be applied at any hierarchy level, and determine user sign-in behavior at that specific level.

A credential policy is not mandatory at specific levels in the hierarchy. However, a default credential policy is provided at the sys.hcs level. Administrators at lower levels can copy and edit this default policy if necessary. Administrators can also save it at their own hierarchy level so that it can be applied to the associated users at that level. If the administrators at the various levels do not create a credential policy at their level, it is inherited from the closest level above them. If a Provider Administrator has defined a credential policy, but a Customer Administrator has not, the customer automatically inherits the credential policy from the Provider. A different credential policy can also be defined for each user.

For each administrator user where IP address throttling (sign-in Limiting per Source) is required, manually create and assign a credential policy. The credential policy must have IP address, and username and email throttling enabled.

The default credential policy is defined at the sys.hcs level.

Note Credential Policies are not applicable for SSO authenticated users. For LDAP Synched users, only the session timeouts are applicable.

System User

The authentication method of a system user is specified when creating a user. the following authentications methods are available Cisco Unified Communications Domain Manager 10.6(x)in:

- Standard sign-in (Cisco Unified Communications Domain Manager 10.6(x)user authentication or proxy authentication)
- LDAP (LDAP authentication)
- SSO (using a SAML-based identity management server)

Standard Users and Sign-in

When creating a system user that uses the standard authorization method, the password is stored in the internal system database. Cisco Unified Communications Domain Manager 10.6(x) uses the PBKDF2 algorithm with an SHA256 hash, a key stretching mechanism recommended by the National Institute of Standards Technology (NIST), Computer Security Resource Center (CSRC).

When signing in as a standard user, go to the URL:

```
http://{hostname}/login
```

A sign-in page theme can be applied to the sign-in page during the log in process by adding the suffix '?theme={theme_name} where {theme_name} is an available theme. For example:
http://{hostname}/login/?theme=default

When signing in, the username can be entered in either of the following formats:

```
{username}@hierarchy or {email address}
```

The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

The hierarchy on the log in form is prefixed with `sys`.

For example: `johndoe@sys.VS-OPS.VS-Corp.Chicago`

LDAP Users and Sign-in

When creating a system user using the LDAP authorization method, specify the LDAP server and the LDAP username. The LDAP username corresponds to the sign-in Attribute Name specified in the LDAP network connection.

When signing in as an LDAP user, go to the URL:

```
http://{host name}/login
```

Regardless of the sign-in Attribute Name specified in the LDAP network connection, the user email address can be used to log in.

When signing in with LDAP credentials, the username is in the format:

```
{user ID}[@hierarchy]
```

Note:

- `@hierarchy` is not required when the user ID corresponds to the user's email address.
- `{user ID}` corresponds to the sign-in attribute name (for example email address, user principal name, sAMaccountName). The sign-in attribute name is configured in the Authentication attribute of the LDAP device connection associated with this hierarchy.
- The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

SSO Users and Login

When creating a system user using the SSO authorization method, the SSO Identity Provider must be specified and the SSO username.

When signing in as an SSO user, go to the URL:

```
http://{host name}/sso/{SSO login URI}/login
```

For example:

```
http://host.Agency1.CustomerA.com/sso/CustomerA/Agency1/login
```

Log in using the relevant SSO identity provider credentials.

CHAPTER 5

Entitlement Management

Entitlement

Cisco Unified Communications Domain Manager Entitlement represents the set of rules surrounding the suite of services and devices (and their number) available for particular subscribers. For instance, one customer may specify that end users may only have voice service with a maximum of two devices, one being a flavor of IP set, and the other being an analog set. Another customer may configure their end users to have both voice and voicemail services, with a maximum of ten devices limited to SIP sets. Both of these are valid rule sets intended to govern their respective users' service or device set.

There are four principal Cisco Unified Communications Domain Manager models from which the entitlement rule sets are built:

- Device Types
- Device Groups
- Entitlement Catalogs
- Entitlement Profiles

Device Types

Device types represent the suite of physical devices which may be grouped into device groups for subsequent entitlement purposes. These device types should mirror the supported product types available on the Cisco Unified Communications Manager.

The device type data model is prepopulated with a snapshot of current product types; however, the provider administrator can add, as well as update or remove, additional device types, if needed.

Device Groups

A device group is a subset of device types. Device groups are not necessarily discrete; that is, different device groups may share specific device types.

Provider administrators can add, delete, and update device groups. Reseller and customer administrators can only view device groups.

Entitlement Catalogs

An entitlement catalog specifies supported device groups and available services (broad categories of functionality) for a particular hierarchy. The services which are available to be selected in an entitlement catalog are as follows: Voice, Voicemail, Presence, and Extension Mobility. Entitlement catalogs also set the maximum allowed number of total devices and the maximum allowed number of devices in each device group within the catalog.

If entitlement is to be used, an entitlement catalog must exist at the Provider hierarchy node. No more than one entitlement catalog may exist at any given hierarchy node. The entitlement catalog at a particular hierarchy node restricts the device groups, device counts, and services which are available to entitlement profiles at or below that node in the hierarchy. No entitlement profile may exceed the restrictions imposed by its associated entitlement catalog. Similarly, an entitlement catalog at a particular hierarchy imposes limitations on any subsequent entitlement catalogs beneath it in the hierarchy structure. No entitlement catalog created deeper in the hierarchy structure may exceed the restrictions specified in a higher entitlement catalog.

Provider administrators can add, update, and delete entitlement catalogs at their hierarchy level and below. Reseller and customer administrators can only view entitlement catalogs.

Entitlement Profiles

Entitlement profiles establish the set of services, device groups, and device limits to which an end user may subscribe. No entitlement profile may exceed the specifications dictated by the hierarchy-associated entitlement catalog. An entitlement profile may not exist at a particular hierarchy node unless an entitlement catalog exists at or above the entitlement profile's hierarchy node.

Unlike entitlement catalogs, there may be multiple entitlement profiles at a given hierarchy node. Each of these entitlement profiles must have a unique name within the hierarchy. Additionally, no device type may appear in more than one device group within a given entitlement profile.

Entitlement profiles can be assigned to users when users are synched from Cisco Unified Communications Manager or from LDAP, or when users are added or modified in Cisco Unified Communications Domain Manager via Subscriber Management and User Management.

One entitlement profile at a given hierarchy node can be designated as the default entitlement profile. The default entitlement profile is applied to any users at or below the hierarchy node, if those users are not explicitly assigned another entitlement profile.

Provider administrators can add, update, and delete entitlement profiles at their hierarchy level and below. Reseller and customer administrators can only view entitlement profiles.

Entitlement Enforcement

Service Levels

The following table shows the impact to a user when a service is disabled in the entitlement profile applied to the user.

Note An entitlement profile can be explicitly assigned to a user, or implicitly applied if an entitlement profile is designated as the default entitlement profile in a hierarchy node at or above the user's hierarchy node.

Service disabled	Result
Voice	Adding a phone to a user in Subscriber Management will fail. For an existing user with a phone, updates to the user in Subscriber Management will fail after an entitlement profile with Voice disabled is applied to the user.
Voicemail	Adding Voicemail to a user in Subscriber Management will fail. For an existing user with Voicemail, updates in Subscriber Management will fail after an entitlement profile with Voicemail disabled is applied to the user.
Presence	Enabling Cisco Unified Communications Manager IM and Presence Service for a user in Subscriber Management will fail. For an existing user with Cisco Unified Communications Manager IM and Presence Service enabled, updates in Subscriber Management will fail after an entitlement profile with Presence disabled is applied to the user.
Extension Mobility	Adding Extension Mobility to a user in Subscriber Management will fail. For an existing user with Extension Mobility, updates in Subscriber Management will fail after an entitlement profile with Extension Mobility disabled is applied to the user.
Single Number Reach	For a new user, adding Single Number Reach in Subscriber Management will fail, and for an existing user with **Enable Mobility** checked, adding Single Number Reach will fail after an entitlement profile with Single Number Reach disabled is applied to the user.

Device Groups

A user to whom an entitlement profile is applied is limited to devices in the device groups assigned in the entitlement profile. Adding a Phone to a user in Subscriber Management will fail if the added Phone is not in a device group assigned to the entitlement profile applied to the user.

Device Limits

A user to whom an entitlement profile is applied is subject to the following device limits set in the entitlement profile:

- Total number of devices
- Total number of devices in a device group

Adding a Phone to a user in Subscriber Management will fail if the total number of devices limit or the total number of devices in a device group limit is exceeded.

Transaction Log

The transaction log messages contain detailed information that can be used to determine what entitlement profile limitation caused an action to fail.

CHAPTER 6

Upgrade Planning

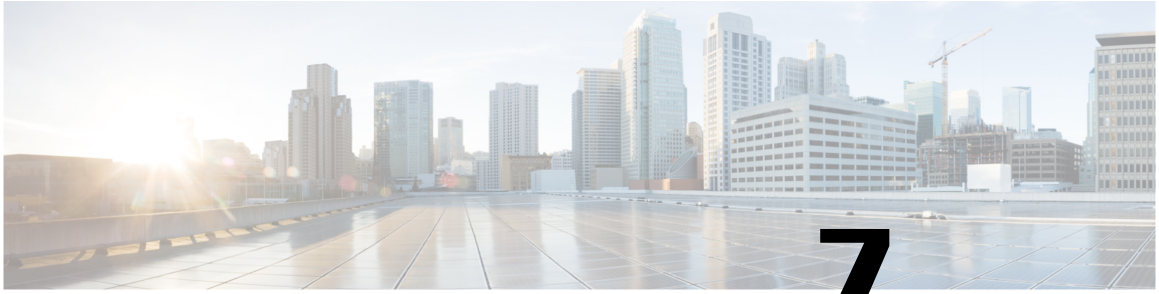
API Compatibility

In general, APIs are backwards compatible from Cisco Unified Communications Domain Manager 10.6(x) to Cisco Unified Communications Domain Manager 10.1(2). However, you should check the *Cisco Unified Communications Domain Manager, Release 10.6(2) API Reference Guide* for any non-compatible changes, and plan updates to clients impacted by non-compatible changes.

For a detailed list of differences between release 10.6(1) models and 10.1(2) models, see http://rtp1-netapp-ns-web/Local/hcsgc/Published/API/autogen/published/Release10.6.1-10.6.1.10000-2-Drop43.1-HCM_Standard/apidiff/CUCDM_API_Schema_Diffs_From10.1.2-10.1.2.11001-2-Drop30.10-HCM_Standard_To10.6.1-10.6.1.10000-2-Drop43.1-HCM_Standard.pdf.

PART II

Install



CHAPTER 7

Prepare to Install

Installation Prerequisites

Installation of Cisco HCM-Core has the following prerequisites:

- HCM-F is installed and all services are activated and running.
- Network connectivity is available between Cisco HCM-Core nodes and the HCM-F, UC App servers, and WebEx servers.

Multinode Cluster Hardware Specifications

Migration from the Stand-Alone Cisco Unified Communications Domain Manager 10.6(x) system to a 4 Unified Node/2 WebProxy Node cluster is supported. The resource requirements for each configuration are provided in Table 1.

Table 1: Virtual Machine Requirements

Node Type	Quantity	VM Level	Memory[1]	CPU	Disk	Network
Unified	>= 4	VMware 5.1 or later	8 GB	4vCPU @ 2 GHz	370 GB partitioned as follows: • 20 GB for OS • 50 GB for application • 50 GB for compressed backups • 250 GB for database	1 Gbit/s minimum

Node Type	Quantity	VM Level	Memory[1]	CPU	Disk	Network
WebProxy	>=2	VMware 5.1 or later	4 GB	2vCPU @ 2 GHz	70 GB partitioned as follows: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

[1] For the 4 Unified Node/2 WebProxy node deployments where the total number of end users is expected to exceed 100,000, it is recommended that 16 GB of RAM be provisioned for each Unified node. The recommended memory allocation for the WebProxy nodes does not change.

The size of the database storage partition supports the maximum deployment size for the release. Further increase in the size of the partition is not required when new customers are on-boarded.

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

Standalone Hardware Specification

Virtual machine requirements are specified in the following table.

Purpose	Quantity	VM	Memory	CPU	Disk	Network
Standalone node	1	>= VMware 4.1	8 GB	4vCPU @ 2 GHz	180 GB partitioned as follows: • 20 GB for OS • 50 GB for application • 50 GB for compressed backups • 60 GB for database storage	1 Gbit/s minimum

The Database storage partition is sized at the initial installation to support the maximum deployment size for the release. Further increase in the size of the partition is not required as new customers are on-boarded.

For the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. Perform this task after the OVA import but prior to the boot of the system.

Browser Compatibility for CUCDM

The following table describes web browser compatibility for Cisco Unified Communications Domain Manager within Cisco Hosted Collaboration Solution.

Table 2: Legend

Symbol and Abbreviation	Definition
✖	Browser not supported
✓	Browser supported
IE	Microsoft Internet Explorer
MF	Mozilla Firefox
GC	Google Chrome
AS	Apple Safari
ESR	Extended Support Release

Cisco Unified Communications Domain Manager 8.1(x) Browser Compatibility Tables

Table 3: Cisco Unified Communications Domain Manager 8.1(x) Windows Browser Compatibility

HCS Release	Operating System	IE 8	IE 9	IE 10	IE 11	MF 3.x	MF 4.x	MF 8.x	MF 9.x	MF 10.x	MF 17.x ESR	MF 20.x	MF 23	MF 28.0	GC 8	GC 25	GC 29	GC 34
HCS 8.x	Windows 7																	
	Windows 8																	
HCS 9.x	Windows 7	✓	✓									✓				✓		
	Windows 8																	
HCS 10.x	Windows 7	✖	✖	✓	✓	✖	✖	✖	✖	✖	✖	✖		✓	✖	✖		✓
	Windows 8			✖			✖			✖					✖	✖	✓	
	Windows XP										✓		✓				✓	

Table 4: Cisco Unified Communications Domain Manager 8.1(x) MacOS X Browser Compatibility

HCS Release	Operating System	AS 4.x	AS 5.x	AS 6.x	MF 4.x	MF 10.x	MF 11.x	MF 17.x ESR	MF 23	MF 28	GC 22	GC 34
HCS 8.x	OS X 10.8 (Mountain Lion)											
	OS X 10.9 (Mavericks)											
HCS 9.x	OS X 10.8 (Mountain Lion)											
	OS X 10.9 (Mavericks)											
HCS 10.x	OS X 10.8 (Mountain Lion)			✓				✓ (nESR)	✓			
	OS X 10.8.5 (Mountain Lion)									✓		✓
	OS X 10.9 (Mavericks)											✓

Cisco Unified Communications Domain Manager 10.x Browser Compatibility Tables

Table 5: Cisco Unified Communications Domain Manager 10.x Windows Compatibility

HCS Release	Operating System	IE 8	IE 9	IE 10	IE 11	MF 3.x	MF 4.x	MF 9.x	MF 10.x	MF 20.x	GC 8	GC 25	GC 29	GC 34
HCS 10.x	Windows 7			✓	✓ see Note					✓ (MF 28)				✓
	Windows 8												✓	
	Windows XP								✓ (MF 17)	✓ (MF 23)			✓	

Note There have been issues identified with running HCS 10.x in IE 11 under Windows 7.

Table 6: Cisco Unified Communications Domain Manager 10.x MacOS X Browser Compatibility

HCS Release	Operating System	AS 4.x	AS 5.x	AS 6.x	MF 4.x	MF 10.x	MF 11.x	MF 20.x	GC 22	GC 34
HCS 10.x	OS X 10.8 (Mountain Lion)			✓		✓ (MF 17)		✓(MF 23)		✓(OS X 10.8.5)
	OS X 10.8.5 (Mountain Lion)							✓(MF 28)		✓
	OS X 10.9 (Mavericks)									✓

CHAPTER 8

Install Cisco Unified Communications Domain Manager

Install Workflow

Use the following table as a guide to install .

Step	Description	For more information
Step 1	For a production environment, install multinode or standalone .	Multinode Installation, on page 32 Standalone Installation, on page 34
Step 2	Create the Cisco Hosted Mediation Fulfillment device.	Create the HCM-F Device, on page 37
Step 3	Create provider.	Create a Provider, on page 39

Multinode Installation

We recommend that you install a multinode consisting of four Unified instances of Cisco Unified Communications Domain Manager (Unified CDM) 10.x and two WebProxy instances.

- A WebProxy node installs only the front-end web server, with the ability to distribute load among multiple middleware nodes.
- A Unified node consists of the Application and Database roles on one node. For geo-redundancy, there are two Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site.

Before You Begin

If you received (Unified CDM) 10.x on DVD, extract the platform-install OVA and the CUCDM template file from the CUCDM ISO file.

If you are downloading Cisco HCM-Core from Cisco.com, download the product ISO file. Mount the product ISO and extract the platform-install OVA and the CUCDM template file.

Optionally, download or extract language pack template files to support languages other than English.

Procedure

Step 1 Install the WebProxy instances.
For each WebProxy instance, create a new VM using the platform-install OVA. Use the instructions shown in Install Cisco Unified Communications Domain Manager 10.x Details, on page 35. For role, select **(3) WebProxy**. Specify the appropriate data center (Primary/DR site) for each WebProxy instance.

Step 2 Install the Unified instances.
For each Unified instance, create a new VM using the platform-install OVA. Use the instructions shown in Install Cisco Unified Communications Domain Manager 10.x Details, on page 35. For role, select **(2) Unified**. Specify the appropriate data center (Primary/DR Site) for each Unified instance.

The following Unified nodes are required in the cluster:

- One Unified node as the Primary node at the Primary site
- One Unified node as the Secondary node at the Primary site
- Two Unified nodes as the Secondary nodes at the DR site

Step 3 Check for needed security updates by running the **security check** command on each node.
If at least one update is required for any node, run the **security update** commands on the node.

Step 4 Install VMware tools on each node.

a) In vSphere, right-click the name of the appropriate VM.
b) Select **Guest** > **Install/Upgrade VMware Tools**.
If you are prompted to disconnect the mounted CD-ROM, click **Yes**.
c) Log in to each node and run the **app install VMware** command.

d) Verify by executing the **app list** command.

Step 5 Prepare each node to be added to the cluster. On each WebProxy and Unified node, except for the primary Unified node, run the **cluster prepnode** command.

Step 6 Add nodes to the cluster.

a) Log in to the primary Unified node.
b) Add the Unified and WebProxy nodes to the cluster with the **cluster add <ip_addr>** command.
c) Verify the list of nodes in the cluster with the **cluster list** command.

Step 7 Add the network domain.

a) Configure the domain with the **cluster run all network domain <domain_name>** command.
b) Verify the configured network domain with the **cluster run all network domain** command.
Each node shows the domain that you configured.
c) Verify the DNS configuration with the **cluster run all network DNS** command.
Each node responds with the DNS server address.
d) Attempt to contact each node in the cluster with the **cluster run all diag ping <hostname>** command.
e) (Optional) Shut down all the nodes with the **cluster run all system shutdown** command. Take a snapshot of each node. Restart each node.

Step 8 Reboot the cluster nodes with the **cluster run all system reboot** command.

Step 9 Provision the cluster.

a) Provide a weight for each database server with the **database weight add <database_ip> <priority>** command.
Weights of 40, 30, 20, and 10 are recommended for the four Unified nodes. The higher the value, the more priority.

In a geo-redundant system containing two data center infrastructures in two physical locations, the following weights are used:

- Specify a weight of 40 for the Primary node at the Primary site
- Specify a weight of 30 for the Secondary node at the Primary site
- Specify weights of 20 and 10 for the Secondary nodes at the DR site

b) Provision the primary node with the following command: **cluster provision primary <IP address of primary database node>**.
Allow approximately 2 hours to provision two WebProxy and four Unified nodes.

If no primary node exists, you are prompted to select a node to be the primary node.

c) When provisioning is complete, verify the status of the cluster with the **cluster status** command.
If a service is down, run the **cluster run <node_ip> app start** command to restart the service.

d) (Optional) Shut down all the nodes gracefully with the **cluster run all system shutdown** command. Take a snapshot of each node. Restart each node.

Step 10 Initialize the database and clear all data with the **cleardown** command on the primary database node.

Step 11 Import the template.

a) Copy the template file to the primary Unified node with the **scp <template_file> platform@<unified_node_ip_address>:./media** command.
b) Log in to the primary Unified node and import the template with the **app template media/<template_file>** command.

Note You see the message: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts any necessary applications.

c) When prompted to set the sysadmin password, provide and confirm a password.

d) When prompted to set the hcsadmin password, provide and confirm a password.

Step 12 Install the Macro_Update.template file on secondary nodes.

a) Upload the new Macro_Update.template file to the `media` directory on the Unified CDM server via SFTP.

1 From the VM console, enter **sftp platform@<cucdm10 hostname>**.

2 Enter **cd media**.

3 Enter **put Macro_Update.template**.

b) Enter the following command: **app template media/Macro_Update_xx.template**.
The template installs on each secondary node in less than a minute.

Step 13 Review the output from the **app template** command and confirm that the message `Script /opt/platform/admin/home/template_xxxxxx/install_script completed successfully` appears.

- If there are no errors indicated, we recommend that you make a backup or snapshot.
- If there was an error, the install script has stopped with a failure message listing the problem. Resolve the problem and retry the installation.

Step 14 (Optional) Install language templates for languages other than English.

a) Copy the language template file to any Unified node with the **scp <language_template_file> platform@<unified_node_ip_address>:./media** command.

b) Log in to the Unified node and install the template with the **app template media/<language_template_file>** command.

Example:
For example, to install French, **`app template media/CUCDMLanguagePack_fr-fr.template`**.

Standalone Installation

Before You Begin

If you have received Cisco Unified Communications Domain Manager 10.6(x) on DVD, extract the platform-install OVA and template files from the .

If you are downloading Cisco HCM-Core from Cisco.com, download the product ISO file. Mount the product ISO and extract the platform-install OVA and template files.

Procedure

Step 1 Create a new VM using the platform-install OVA.

Use the instructions shown in Install Cisco Unified Communications Domain Manager 10.x Details, on page 35. When prompted for role, select **Standalone**.

Step 2 After the system has rebooted, sign-in as the platform user.

Step 3 Issue the **system provision** command.

Step 4 Initialize the database and clear all data with the **cleardown** command.

Step 5 Issue the **network domain <your_domain>** command.

Step 6 Issue the **security update** command.

Step 7 Issue the **system reboot** command.

Step 8 Import the template.

a) Use sftp to transfer the template file to the platform user's media directory server.

b) Install the template with the **app template media/<template_file>** command.

Note You should see the message: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts any necessary applications.

c) When prompted to set the sysadmin password, provide and confirm a password.

d) When prompted to set the hcsadmin password, provide and confirm a password.

Step 9 Review the output from the **app template** command and confirm that the message `Script /opt/platform/admin/home/template_xxxxxx/install_script completed successfully` appears.

- If there are no errors indicated, make a backup or snapshot.
- If there was an error, the install script has stopped with a failure message listing the problem. Resolve the problem and retry the installation.

Step 10 Issue the **system reboot** command.

Step 11 Install VMware tools:

a) In vSphere, right-click the name of the appropriate VM.

b) Select **Guest** > **Install/Upgrade VMware Tools**.
If you are prompted to disconnect the mounted CD-ROM, click **Yes**.

c) Log in to the node and run the **app install VMware** command.

Install Cisco Unified Communications Domain Manager 10.x Details

The system is made available as an OVA file that can be imported into VMware vCenter Server. One OVA file is used to deploy all the functional roles. The specific role is chosen when the installation wizard is run. The administrator should set up the hardware settings on the VMware GUI.

Procedure

Step 1 Log in to vSphere to access the ESXi Host.

Step 2 Choose **File > Deploy OVF Template**.

Step 3 Choose **Source**, browse to the location of the .ova file, and click **Next**.

Step 4 On the Name and Location page, enter a Name for this server.

Step 5 On the Deployment Configuration page, select the appropriate node type.

Step 6 Choose the Resource Pool where the VM will be located.

Step 7 Choose which Datastore will be used to deploy the new VM.

Step 8 Choose the appropriate Disk format to use when deploying the new VM. In production environments, "thick provisioning" is mandatory. Eager-zeroed thick provisioning is recommended.

Step 9 On the Network Mapping, choose your network on which this VM will reside.

Step 10 Do not select **Power on after deployment**.

Step 11 On the **Ready to Complete** page, click **Finish** to start the deployment.

Step 12 After the VM has been created, verify the memory, CPU, and disk settings against the requirements shown in Multinode Cluster Hardware Specifications, on page 25.

Step 13 Power on the VM.

Step 14 Select the following options in the installation wizard:

Option	Option name	Description
1	IP	The IP address of the server.
2	netmask	The network mask for the server.
3	gateway	The IP address of the network gateway.
4	DNS	The DNS server is optional. The DNS server should be capable of looking up all hostnames referred to, including NTP server, remote backup locations, and so on.
5	NTP	The NTP server is mandatory to ensure that time keeping is accurate and synchronized among nodes in the same cluster.
6	hostname	The hostname, not the fully qualified domain name (FQDN).
7	role	• A WebProxy role installs only the front-end web server together with ability to distribute load among multiple middleware nodes. • An Application node is the main transaction processing engine and includes a web server which can operate by itself, or route transactions from a web node. • A Database node provides persistent storage of data. • A Standalone node consists of the Web, Application and Database roles on one node. • A Unified node consists of the Web, Application and Database roles on one node. On installation, the system needs to be clustered with other nodes and the cluster provisioned.

Option	Option name	Description
8	data centre	The system's geographic location (data center name, city, country that a customer might use to identify the system location).
9	platform password	Platform password must be at least eight characters long and must contain both uppercase and lowercase letters and at least one numeric or special character.
10	install	Completes the installation configuration and installs Cisco Unified Communications Domain Manager.

When the installation of the OVA is complete, a login prompt for the platform user is displayed.

What to Do Next

Return to Multinode Installation, on page 32 or Standalone Installation, on page 34 to complete the overall installation procedure.

Create the HCM-F Device

After creating the HCM-F device, a data sync begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Before You Begin

- Install and configure HCM-F. For more information, see *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(2)*.
- Verify that the NBI REST SDR Web Service is running:
  1. Log in to HCM-F CLI as user administrator.
  2. Run the **utils service list** command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
  3. If not running, start it with the **utils service start Cisco HCS NBI REST SDR Web Service** command.

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.6(2) as hcsadmin@sys.hcs.

Step 2 Create a new HCM-F instance:

a) Select **Device Management** > **HCM-F** and click **Add**.
b) Enter the HCM-F hostname.
c) Enter the HCM-F administrator Username.
d) Enter the HCM-F administrator Password.
e) Select the HCM-F Version from the drop-down list.

Note Once HCM-F Version is set to a new version, it cannot be changed to an older one.

f) Click **Save**.

Step 3 If the previous step fails:

- Verify that HCM-F Hostname is correct
- Verify that HCM-F administrator Username and administrator Password are correct
- Verify that HCM-F Version is correct
- Verify that the domain is set correctly using the Cisco Unified Communications Domain Manager 10.6(2) CLI:

  1 `ssh platform@<cucdm hostname>`

  2 **network domain**

Step 4 After a couple of minutes, verify that the initial sync between Cisco Unified Communications Domain Manager 10.6(2) and HCM-F is successful:

a) Select **Provider Management** > **Advanced** > **SDR Service Provider**.

b) The sync is successful if the default entry, "Service Provider Name", appears.

What to Do Next

If the initial sync is not working after following the previous steps, verify that the HCM-F REST API is working by browsing to the following: `http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider`. This command returns the JSON representation of the predefined ServiceProvider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as administrator on the HCM-F app node CLI and verify that the REST service is running:

To display the services, run the command: **utils service list**.

In the output, you see `Cisco HCS NBI REST SDR Web Service[STARTED]`.

If this service is not started, start it with the command: **utils service start Cisco HCS NBI REST SDR Web Service**

For data sync failures, try importing the new HCM-F:

1 Select **Device Management** > **HCM-F** and click the HCM-F device.

2 Update the Hostname and click **Save**.

3 Import the new HCM-F:

  a Select **Device Management** > **Advanced** > **Perform Actions**.

  b In the Action field, select Import.

  c In the Device field, select the HCM-F server.

  d Click **Save** and wait a few minutes.

4 Check the provider under **Provider Management** > **Advanced** > **SDR Service Provider**.

Create a Provider

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.6(2) as hcsadmin@sys.hcs.

Step 2 Select **Provider Management** > **Providers**.

Step 3 Click **Add**.

Step 4 On the **Service Provider Details** tab, complete the following fields:

Field	Description
Name	The name of the provider. This field is mandatory. **Note** Once you have saved the provider, you cannot change the provider name. **Note** Any spaces in the provider name are converted to underscores in the provider local administrator name and email, if **Create Local Admin** is checked.
Description	A description of the provider.
Domain Name	The domain of the provider. For example, provider.com. Used when creating the default local administrator so the administrator can sign in with an email ID such as ProviderAdmin@provider.com. This field is mandatory.
Create Local Admin	Controls whether a default local administrator is created.
Cloned Admin Role	The HCS default provider role used to create a new role prefixed with the provider name. The created provider role, shown in **Default Admin Role** field, is assigned to the default local administrator. This field appears only if **Create Local Admin** is checked.
Default Admin Role	The created provider role that is assigned to the default local administrator. This field is read only and appears only if **Create Local Admin** is checked.
Default Admin Password	The password to assign to the default local administrator. This mandatory field appears only if **Create Local Admin** is checked.
Repeat Default Admin Password	Confirm the default local administrator password. This mandatory field appears only if **Create Local Admin** is checked.

Step 5 On the **Contact Information** tab, enter address, e-mail, and phone information as appropriate.

Step 6 Click **Save**.

The provider hierarchy node in Cisco Unified Communications Domain Manager 10.6(x), the Service Provider name in SDR, and optionally a default provider administrator are created. All existing Cisco HCS System Administration-level dial plan schemas and schema groups are automatically cloned to the new provider. For more information on automatic cloning, see *Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(x)*.

Create Reseller

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.6(x) as provider admin.

Step 2 Select **Reseller Management** > **Resellers**.

Step 3 Click **Add**.

Step 4 Complete the following fields:

Field	Description
Name	The name of the reseller. This field is mandatory. **Note** Once you enter a reseller name, it cannot be changed.
Description	A description of the reseller.
Domain Name	The domain of the reseller. This field is mandatory.
Cloned Admin Role	The HCS default reseller role used to create a new role prefixed with the reseller name.

Step 5 Click **Save**.

The reseller hierarchy node in Cisco Unified Communications Domain Manager 10.6(x), the reseller in SDR, and a default reseller admin are created.

Create Customer

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.6(x) as provider admin or reseller admin.

Step 2 Select **Customer Management** > **Customers**.

Step 3 Click **Add**.

Step 4 Complete the following fields:

Field	Description
Name	The name of the customer. This field is mandatory. **Note** Once you enter a customer name, it cannot be changed.

Field	Description
Description	A description of the customer.
Domain Name	The domain of the customer. This field is mandatory.
Cloned Admin Role	The HCS default customer role used to create a new role prefixed with the customer name.

Step 5 Click **Save**.

The customer hierarchy node in Cisco Unified Communications Domain Manager 10.6(x), the customer in SDR, and a default customer admin are created.

Create Site

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.6(x) as customer admin.

Step 2 Select **Site Management** > **Sites**.

Step 3 Click **Add**.

Step 4 Complete the following fields:

Field	Description
Name	The name of the customer. This field is mandatory. **Note** Once you enter a customer name, it cannot be changed.
Country	A description of the location.

Step 5 Select a Network Device List.

Note The Network Device List dictates which Cisco Unified Communications Manager and Cisco Unity Connection xn is used by the site

Step 6 Click **Save**.

The site hierarchy node in Cisco Unified Communications Domain Manager 10.6(x), the location in Cisco Unified Communications Domain Manager 10.6(x), the customer location in SDR, and a default site admin are created.

CHAPTER 9

Upgrade

Upgrade a Multinode Environment

Before You Begin

Create a new backup using the platform command-line interface. You can back up the cluster, or back up each node individually.

Note You can reduce the time to upgrade Cisco Unified Communications Domain Manager (Unified CDM) by performing backup activities before the upgrade maintenance window. You can also reduce the time for upgrade and backup by running node upgrades in parallel (a process that includes a backup). Use the following CLI command:

cluster upgrade media/platform-install-1.x.x-x.iso fast

Another alternative is to use VMware snapshots for your backup if reducing the length of time for the upgrade is a primary consideration. Consider the following when using VMware snapshots to back up Unified CDM:

- Cisco cannot guarantee that a VMware snapshot can be used to successfully restore Unified CDM or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application.
- When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space.

For more information about the risks of using VMware snapshots, refer to the “Backup and Restore” chapter in the *Cisco Unified Communications Domain Manager, Release 10.6(2) Maintain and Operate Guide*.

Turn off any scheduled imports. See Turn off Scheduled Imports, on page 47.

Check for running imports. Either wait for them to complete or cancel them. See Cancel Running Imports, on page 47.

Procedure

Step 1 Use SFTP to transfer the upgrade .iso file to the platform user's media folder on the primary Unified node.

a) sftp platform@<unified_node_hostname>
b) cd media
c) put <upgrade_iso_file>

Step 2 On the primary Unified node, verify the .iso image with the **ls -l media** command.

Step 3 On the primary Unified node, run the **cluster upgrade media/<platform-xxx.iso>** command to upgrade the cluster.

Step 4 After the upgrade is complete, verify the cluster status with the **cluster status** and **cluster run all diag health** commands.

Step 5 On the primary Unified node, run the **VOSS upgrade_db** command.

Step 6 On the primary Unified node, run the **security update** command.

Step 7 On the primary Unified node, run the **cluster run all diag health** command to verify that all services are up.

Step 8 Use SFTP to transfer the upgrade template file to the platform user's media folder on the primary Unified node:

a) sftp platform@<unified_node_hostname>
b) cd media
c) put <upgrade_template_file>

Step 9 On the primary Unified node, run the **ls -l media** command to verify the template file.

Step 10 On the primary Unified node, run the **app template media/<CUCDM-xxx.template>** command.

Note You should see the message: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts any necessary applications.

Step 11 Review the output from the **app template** command and confirm that the message `Script /opt/platform/admin/home/template_xxxxxx/install_script completed successfully` appears.

- If no errors are indicated, make a backup or snapshot.
- For an unsupported upgrade path the install script stops with the message: `Upgrade failed due to unsupported upgrade path. Please log in as sysadmin and see Transaction logs for more detail.` You can restore to the backup or revert to the VM snapshot made before the upgrade.
- If there are errors for another reason, the install script stops with a failure message listing the problem. Resolve the problem and retry the installation.

Step 12 **Note** **These steps are to be run only on secondary nodes.**

Use SFTP to transfer the new Macro_Update.template file to the media directory on the Cisco Unified Communications Domain Manager 10.6(x) server (e.g. Macro_Update.template, see version compatibility chart)

a) sftp platform@<cucdm10 hostname>
b) cd media
c) put Macro_Update.template

Step 13 Issue the **app template media/Macro_Update_xx.template** command from the CUCDM platform CLI. It takes less than one minute to install the template on each secondary node.

What to Do Next

- Log in to the user interface as hcsadmin and verify the upgrade by selecting **About** > **Extended Version**. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.
- Reactivate the scheduled imports that you turned off before upgrading.

Upgrade a Standalone Environment

Before You Begin

Create a new backup using the platform CLI.

Note You can reduce the time to upgrade Cisco Unified Communications Domain Manager (Unified CDM) by performing backup activities before the upgrade maintenance window. You can also reduce the time for upgrade and backup by running node upgrades in parallel (a process that includes a backup). Use the following CLI command:

cluster upgrade media/platform-install-1.x.x-x.iso fast

Another alternative is to use VMware snapshots for your backup if reducing the length of time for the upgrade is a primary consideration. Consider the following when using VMware snapshots to back up Cisco Unified Communications Domain Manager:

- Cisco cannot guarantee that a VMware snapshot can be used to successfully restore Unified CDM or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application.
- When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space.

For more information about the risks of using VMware snapshots, refer to the “Backup and Restore” chapter in the *Cisco Unified Communications Domain Manager, Release 10.6(2) Maintain and Operate Guide*.

Before upgrading, turn off any scheduled imports. See Turn off Scheduled Imports, on page 47.

Before upgrading, check for running imports. Either wait for them to complete or cancel them. See Cancel Running Imports, on page 47.

Procedure

Step 1 Use SFTP to transfer the upgrade .iso file to the platform user's media folder on the server.

a) sftp platform@<cucdm_server_hostname>
b) cd media
c) put <upgrade_platform_iso>

Step 2 Log in to the server CLI as platform user.

Step 3 Run the **app upgrade media/<upgrade_iso_file>** command.

Step 4 Run the **system provision** command.

Step 5 Run the **upgrade_db** command.

Step 6 Run the **security update** command.

Step 7 Run the **system reboot** command.

Step 8 Use SFTP to transfer the Cisco Unified Communications Domain Manager 10.6(x) Cisco HCM-Core file to the platform user's media folder on the server:

a) sftp platform@<cucdm_server_hostname>
b) cd media
c) put <upgrade_template_file>

Step 9 Upgrade the template with the **app template media/<template_file>** command.

Note You should see the message: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts any necessary applications.

Step 10 Review the output from the **app template** command and confirm that the message `Script /opt/platform/admin/home/template_xxxxxx/install_script completed successfully` appears.

- If there are no errors indicated, make a backup or snapshot.
- If there are errors because of an unsupported upgrade path, the install script stops with a failure message: `Upgrade failed due to unsupported upgrade path. Please log in as sysadmin and see Transaction logs for more detail.` You can restore to the backup or revert to the VM snapshot made before the upgrade.
- If there are errors for another reason, the install script stops with a failure message listing the problem. Resolve the problem and retry the installation.

Step 11 Run the **system reboot** command.

What to Do Next

- Log in to the user interface as hcsadmin and verify the upgrade by selecting **About** > **Extended Version**. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.
- Reactivate any scheduled imports that you turned off before upgrading.

Cancel Running Imports

Cancel running imports to reduce load on the system and improve upgrade performance.

Procedure

Step 1 Log in as hcsadmin@sys.hcs.

Step 2 Select **Administration Tools** > **Transaction** to view Transactions.

Step 3 Hover over the Action heading, then click the search icon.

Step 4 In the Search String field, type Import and hit enter.
Import jobs are displayed.

Step 5 Look for jobs that have Status of "Processing" and either wait for them to complete or cancel them.

Step 6 To cancel a job, click the job, then click the **Cancel** button.

Turn off Scheduled Imports

Turn off scheduled imports to reduce load on the system and improve upgrade performance.

Procedure

Step 1 Log in as hcsadmin@sys.hcs.

Step 2 Select **Administration Tools** > **Scheduling** to view scheduled jobs.

Step 3 Click each scheduled job. On the **Base** tab, uncheck the **Activate** check box.