



Technical Design Document

For Cisco Collaboration System Upgrade and Migration

Written by ConvergeOne
For Barstow Community College

Mark Lyman | Solutions Architect, CCIE #45725 | mlyman@convergeone.com

Confidentiality Statement -- This document is strictly private and confidential. It is not to be copied or reproduced nor its contents disclosed to any other company without the prior written consent of ConvergeOne.

Copyright ConvergeOne. All Rights Reserved. This document is the property of and is proprietary to ConvergeOne. It shall not be disclosed in whole or in part without the express written consent of ConvergeOne. It shall not be duplicated or used, in whole or in part, for any purpose other than the implementation of the project described herein.

Disclaimer -- The right is reserved to amend the information provided in the event there are any additional requirements or information. ConvergeOne will not be responsible for any errors or omissions contained within the documentation supplied. Information in this document is subject to change without notice.

Trademarks -- ConvergeOne acknowledges all third party trademarks used in this document.

Table of Contents

Table of Contents	2
Versions	4
Introduction	5
Document Purpose	5
Project Overview	5
Project Rationale	5
Project Goals	5
High-level Project Description	6
Upgrade and Install Approach	6
Phase 1 - CUC Migration	6
Phase 2 - CUCM & UCCX Migration	6
Phase 3 - New Applications	7
Change Control	8
Intended Audience	8
Related Documents	8
Solution Overview	9
Cisco Approved Architecture	9
Deployment Model	9
Technology, Versions, and OVA Templates	10
Locations	11
Network Infrastructure	11
Domains	11
Network Services	11
(DHCP) Dynamic Host Configuration Protocol	11
(DNS) Domain Name System	12
(NTP) Network Time Protocol	12
(QoS) Quality of Service	13
Firewalls	14
(UCS) Cisco Unified Computing System	15
UCS Cabling	15
VM Application MAP	15
Gateways	16
Gateways	16
Solution Components	17
Endpoints	17
Jabber	17
Emergency Services	18
Media Resources	18

Conference Now	19
(MoH) Music on Hold	19
Voicemail	19
Attendant Console	20
Server Requirements	20
Desktop Requirements	21
(PCD) Prime Collaboration Deployment	22

Versions

Date	Version	Author	Notes
26 Feb 2018	1	Mark Lyman	Initial Release

1. Introduction

1.1. Document Purpose

ConvergeOne has been secured to assist in the upgrade and migration of the following Cisco Collaboration applications onto new Cisco UCS-C 220-M4 servers.

- Cisco Unified Communications Manager (CUCM)
- Cisco Unity Connection (CUC)
- Cisco Unified Contact Center Express (UCCX)

2 existing Voice Gateways will be upgraded to ISR 4321 Voice Gateways.

ConvergeOne has also been tasked with the implementation of the following new Cisco Collaboration applications.

- Cisco IM and Presence (IMP) Pub/Sub pair
- CUCM Subscriber pair
- CUC Subscriber
- Cisco Unified Attendant Console (CUAC) server
- Cisco Paging Server

Cisco Emergency Responder (CER) will added in a later phase of this project.

This document acts as the technical design guide for this implementation. The intent is to document technical objectives governing this project, and the design for implementing the objectives. It is expected that after review, customer representatives will sign off on this document for work to continue on the remainder of the deployment activities.

This documentation is not meant to replace, but rather augment the training, installation and configuration manuals from Cisco and other vendors providing hardware and software implemented as part of this solution. The information contained in this document assumes a level of competency in the components being deployed.

1.2. Project Overview

Projects of this nature are complex and the integration is unique in each environment. The following sections provide a high-level summary of the overall architecture of this project.

1.2.1. Project Rationale

Barstow CC would like to replace their existing UCS hardware and upgrade an existing Unified Communications version 8.X environment to version 11.X Existing features and functionality will remain in place, and new features and functionality will be added as outlined in the SoW.

1.2.2. Project Goals

The following goals have been identified as part of this project:

Upgrade and Migrate the following existing applications:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unity Connection (CUC)
- Cisco Unified Contact Center Express (UCCX)

Integrate 2 new 4321 Voice Gateways.

Install and integrate the following new Cisco Collaboration applications.

- Cisco IM and Presence (IMP) Pub/Sub pair
- CUCM Subscriber pair
- CUC Subscriber
- Cisco Unified Attendant Console (CUAC) server
- Cisco Paging Server

1.2.3. High-level Project Description

This project consists of a duplex Collaboration deployment spread across two servers.

1.2.4. Upgrade and Install Approach

Phase 1 - CUC Migration

Task #	Task	Notes
1	Install new version of CUC on new UCS servers	
2	Use COBRAS to migrate data from 8.5 CUC to 11.5 CUC	No outage, can be done during business hours
3	Integrate 11.5 CUC with 8.5 CUCM	Voicemail outage

Phase 2 - CUCM & UCCX Migration

Task #	Task	Notes
1	Use PCD to migrate data from 8.5 CUCM to 11.5 CUCM	No outage, can be done during business hours. Change freeze.
2	Install CUCM subscriber pair	
3	Install and integrate UCCX Pub/Sub pair	
4	Manually migrate data from 8.5 UCCX to 11.6 UCCX <ul style="list-style-type: none"> ● 3 applications ● 4 scripts ● 3 agents 	
5	Change 8.5 UCM to pre-8.0-rollback in prep for phone migration	Phone reboot. All unconnected phones will have to be factory reset.
6	Update DHCP option 150 to new servers. <ul style="list-style-type: none"> ● 10.1.21.11 Primary ● 10.1.21.10 Secondary 	
7	Reboot 1 phone and confirm migration	
8	Migrate PSTN connectivity to new gateways and confirm PSTN connectivity	PSTN outage
9	Reboot all phones and confirm connectivity	Full phone outage
10	Confirm agent login and UCCX useability	

Phase 3 - New Applications

Task #	Task	Notes
1	Install IM&P Subscriber pair	
2	Integrate Paging Server	
3	Install CUAC	

1.3. Change Control

The project environment should be treated, even during initial deployment, as a production environment. If changes need to be made to the system in any way, the customer's change-control procedures need to be closely followed.

1.4. Intended Audience

This document covers information required to successfully implement this project, but this is a small part of operations, network and services. Therefore, this document should be distributed and reviewed by all Project Team members and technology owners, as it provides valuable information about how this product will integrate with and impact business operations.

1.5. Related Documents

Additional documents are available which can be referenced for additional information regarding requirements and high-level solution design:

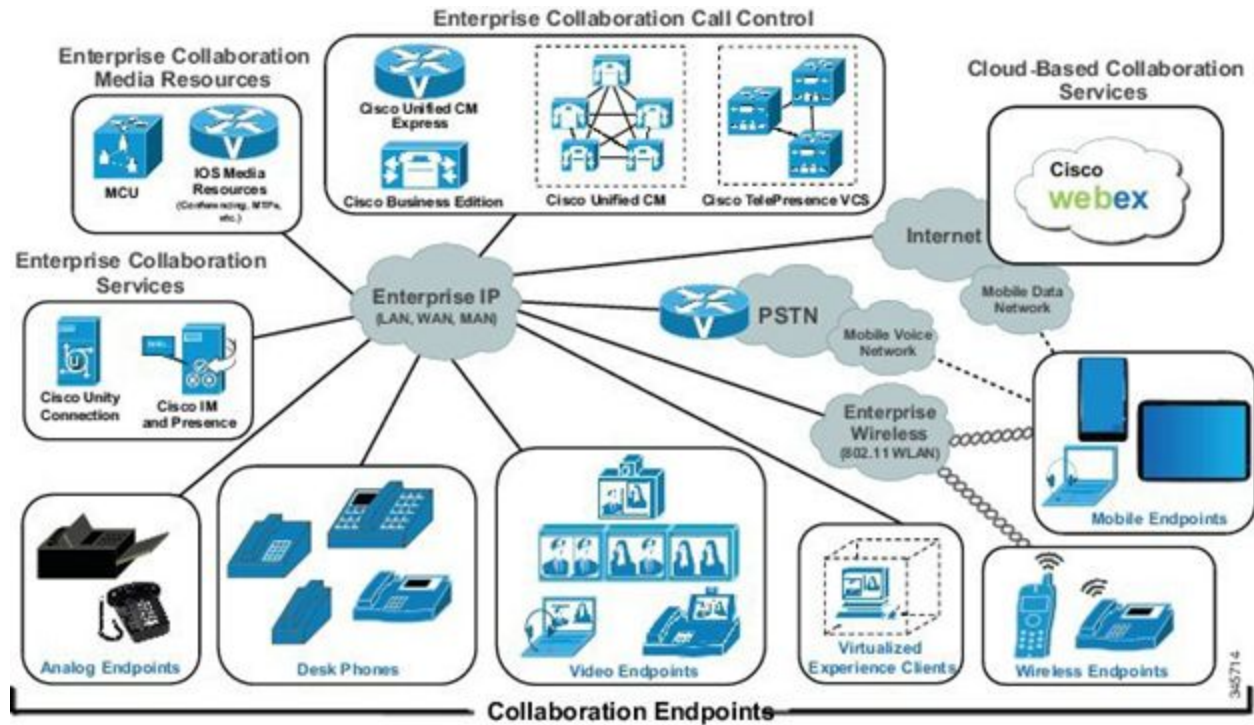
- Statement of Work
- Bill of Materials
- IP Spreadsheet

2. Solution Overview

This section describes the components included in this solution.

2.1. Cisco Approved Architecture

The following diagram was presented to and approved by the Cisco Assurance 2 Quality (A2Q) team, which reviews all Collaboration solutions. This architecture is what will be followed for this project:



2.2. Deployment Model

This solution’s deployment model is “Single Site with Centralized Call Processing. This model is coupled with clustering between UCS servers, as described in the “Collaboration Deployment Models” section of the “Collaboration Systems Components and Architecture” UC SRND. SRND’s can be found at the following location, and further describe best practices and recommendations for the deployment models.

<http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-collaboration/index.html>

Having this deployment model means that the components are split between the two main servers.

2.3. Technology, Versions, and OVA Templates

This project will be deployed with the versions specified in the following table. These specific versions are chosen based upon Cisco's system test releases, in conjunction with each SRND and/or Bill of Materials for the respective products involved in this project.

http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/unified/communications/system/ucstart.htm

Components	Purpose	Version	OVA
CUCM	The core of Cisco Collaboration services, CUCM facilitates session and call control for video, voice, messaging, mobility, and presence.	11.5(1)SU4	7500 Users
IM&P	Provides native standards-based, dual-protocol, enterprise instant messaging (IM) and network-based presence.	11.5(1)SU4	5000 Users
CUC	A robust unified messaging and voicemail solution that provides users with flexible message access options and IT with management simplicity.	11.5(1)SU4	5000 Users
UCCX	Unified CCX offers sophisticated call routing and comprehensive contact management capabilities. It includes an embedded reporting solution that offers a comprehensive view of contact center statistics at a glance.	11.6.1	300 Agents
PCD	An application that is designed to assist in the management of Unified Communications (UC) applications.	12.0.1	N/A
ISR Gateways	Connects large, midsize, and small business unified communications networks to the IP public switched telephone network (PSTN).	15.X	N/A
CUAC	This call queuing engine for dedicated operator centers helps manage calls from many sources. The directory handles up to 100,000 contacts and synchronizes with Active Directory.	11.X	N/A

Please note that the latest compatible releases are desirable. As such, the versions listed here may be different than what is actually deployed if newer releases become available during deployment.

For Physical location layout and IP Addressing of the actual components, please refer to the IP Worksheet.

2.4. Locations

This solution will be built upon the existing infrastructure by adding additional servers to pertinent locations for Call Routing and for Voicemail. Modifying existing network infrastructure and QOS will be customer's responsibility.

This solution consists of components in the following locations.

Location	Type	Notes
Campus	Main	
Ft. Irwin	Office	

2.5. Network Infrastructure

2.5.1. Domains

Internal Domain	External Domain	Email Domain
barstow.edu	barstow.edu	barstow.edu

2.5.2. Network Services

2.5.2.1. (DHCP) Dynamic Host Configuration Protocol

DHCP allows network endpoints to automatically obtain an IP address and other relevant configuration information.

- A DHCP server will be made available at each site where collaboration endpoints exist.
- Option 150 (TFTP) will be set to the CUCM Publisher in LA as the primary and the CUCM Subscriber in Orem as the secondary

Primary TFTP	Secondary TFTP
10.1.21.11	10.1.21.10

2.5.2.2. (DNS) Domain Name System

The Cisco UC environment relies on DNS to function properly. All DNS A records must also have the accompanying DNS Reverse/PTR records recated. The following DNS entries must be made:

Internal A Records	
Hostname	IP Address
ucs1a-cimc.barstow.edu	10.1.21.2
ucs1a-esxi.barstow.edu	10.1.21.3
ucs1b-cimc.barstow.edu	10.1.21.4
ucs1b-esxi.barstow.edu	10.1.21.5
cucmpub.barstow.edu	10.1.21.10
cucmsub1a.barstow.edu	10.1.21.11
cucpub.barstow.edu	10.1.21.20
cucsub.barstow.edu	10.1.21.21
imppub.barstow.edu	10.1.21.30
impsub1a.barstow.edu	10.1.21.31
uccxpub.barstow.edu	10.1.21.40
uccxsub.barstow.edu	10.1.21.41
pagingpub.barstow.edu	10.1.21.50
acpub.barstow.edu	10.1.21.60
acsub.barstow.edu	10.1.21.61

Internal SRV Records						
Domain	Service	Protocol	Priority	Weight	Port	Target Host
barstow.edu	_cisco-uds	_tcp	10	10	8443	cucmsub1a.barstow.edu
barstow.edu	_cisco-uds	_tcp	10	20	8443	cucmpub.barstow.edu

2.5.2.3. (NTP) Network Time Protocol

NTP allows network devices to synchronize their clocks to a network time server or network-capable clock. NTP is critical for ensuring that all devices in a network have the same time. When troubleshooting or managing a telephony network, it is crucial to synchronize the timestamps within all error and security logs, traces, and system reports on devices throughout the network.

- NTP for all devices will point at the customer’s Stratum 2 NTP server, to be identified on the IP worksheet.
- For all VOS-based Cisco components, the Publisher of a cluster points at the NTP server. All Subscribers within the cluster are time-synced with the Publisher.
- NTP Servers must be Linux-based and not Windows-based.

Barstow NTP Server	10.1.10.11
---------------------------	------------

2.5.2.4. (QoS) Quality of Service

A communications network forms the backbone of any successful organization. These networks transport a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. The bandwidth-intensive applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources.

All QoS will be implemented and maintained by the customer.

Further information can be found in [the QoS section of the Cisco Collaboration SRND](#).

2.5.3. Firewalls

Cisco supports the use of firewalls with UC solutions, but there are several important things to be aware of that can drastically impact the performance of the environment. Phones use a client/server model for signaling for call setup, and if the signaling traffic does not go through the firewall, the attempt to set up an RTP stream between endpoints may be blocked. Firewalls must follow strict guidelines for capacity and performance. Generally, the CPU usage of the firewall must remain under 60% for normal usage. If CPU runs over 60% it impacts IP phone registration, call setup, and if stressed enough, will affect the voice quality of phone calls. Phone registration can be impacted such that rolling reboots of phones can occur, which increases the load of a firewall even more. CPU usage on firewalls should be carefully monitored if adding IP Telephony traffic to a network.

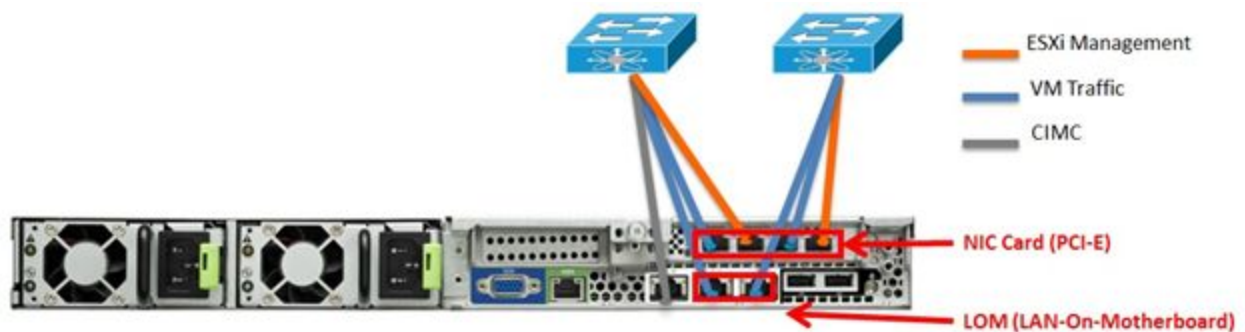
Further information can found in the [Security section of the Cisco Collaboration SRND](#).

2.6. (UCS) Cisco Unified Computing System

2.6.1. UCS Cabling

VMware Standard Switches will be configured for the Cisco UC solution. Configuration must comply with the requirements documented by Cisco for the VMWare vSwitch configuration. Full requirements can be found here: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-qos-designs-considerations.html

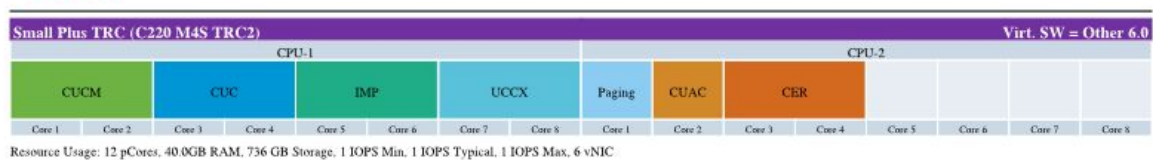
The fault tolerant design recommends the use of 7 physical connections and 3 VLANs - one for the CIMC, a second for Call Control and RTP traffic to the VMs, and a third for the VMWare management functions. In the case of the BE6K deployment, some customers have chosen to collapse it all into a single Voice VLAN. Although this is not Cisco Best Practices, it is Cisco supported. Upstream data center switches must be configured for either dot1Q trunking or access VLANs depending on chosen design. The intention of the uplinks is to ensure that no single failure (physical NIC card, cable, physical switch) causes the loss of management, voice & video traffic, or the loss of both the primary vmnic and secondary vmnic for the same vSwitch at the same time.



2.6.2. VM Application MAP



Barstow CC v01



File Name: Barstow CC v01

2.7. Gateways

2.7.1. Gateways

A voice gateway converts traditional voice signals to and from IP packets. The voice gateway selected for a site depends on a number of factors. The following voice gateways are being deployed in this solution.

Location	Device(s)
Campus	ISR 4321
Ft. Irwin	ISR 4421

3. Solution Components

Cisco Unified Communications Manager (CUCM) core of the Cisco Collaboration portfolio infrastructure, CUCM is a unified communications call control platform that can deliver the right experience to the right endpoint.

Cisco Unified Communications Manager provides services such as session management, voice, video, messaging, mobility, and web conferencing.

This powerful solution can help:

- Extend video capabilities to your employees through a single, unified communications infrastructure from the desktop to telepresence rooms
- Simplify voice systems with unified communications to cut costs and dramatically simplify provisioning and maintenance
- Build productivity with comprehensive unified communications to help workers communicate and work more effectively
- Enable mobility with embedded unified mobility software capabilities to keep workers productive wherever they are, with any content type, on any device
- Improve collaboration -simply click to begin an IM session, initiate a phone call, or easily start a video-conferencing call
- Cisco Unified Communications Manager is available in a choice of deployment models: public cloud, private cloud, on-premises, remote, or hybrid.

3.1. Endpoints

3.1.1. Jabber

Cisco Jabber helps you communicate and work with colleagues, partners, and customers more quickly and securely through best-in-class Cisco Unified Communications. Built on open standards for interoperability and integrated with commonly used desktop business applications, Cisco Jabber can help you:

- Reduce communication delays by providing presence information so you can see when your colleagues are available
- Accelerate team performance by instantly expanding one-on-one conversations to group chats or multiparty audio, video, and web conferences
- Collaborate directly from Microsoft Outlook by viewing a contact's availability and simply clicking to IM or call
- Limit the costs of business travel and phone calls by communicating with IM; audio, video, and web conferencing; or IP telephony
- Choose the best provisioning model for your business; Cisco Jabber can be deployed on-premises or on demand as a cloud-based service

3.2. Emergency Services

Emergency services are vital to the successful deployment of any phone system. This section outlines some information regarding 911 emergency networks deployed in the United States and Canada. It is the responsibility of <<CUSTOMER NAME>> to ensure they are in compliance with all emergency services for each of their sites.

For information regarding legislation covering 911 functionality required for multi-line telephony system (MLTS) users in the United States, consult the National Emergency Number Association (NENA) Technical Information Document on Model Legislation Enhanced 911 for Multi-Line Telephone Systems, available online at

http://www.nena9-1-1.org/9-1-1TechStandards/TechInfoDocs/MLTS_ModLeg_Nov2000.PDF.

The Federal Communications Commission (FCC) also drafted a proposed new section to title 47, part 68, section 319, available at <http://www.apointl.org/pbx/worddocs/mltspart68.doc>.

Emergency calls are answered by organizations referred to as Public Safety Answering Points (PSAP). These organizations maintain databases of incoming numbers and associated physical locations as well as contact numbers. The PSAP is responsible for dispatching the appropriate emergency service such as fire, police or ambulance.

Emergency calls are typically routed to a PSAP via dedicated, regionally significant networks. Each PSAP is connected to one or more regional networks. Many times the incumbent Regional Bell Operating Company (RBOC) is the 911 network service provider.

Calls are routed to the appropriate PSAP (a single emergency network service provider may connect to multiple PSAP facilities) based on the automatic number identification (ANI) of the phone making the call. Hence, the ANI presented to the network service provider must be a routable number in their system.

Once a call is presented to a PSAP, the location of the phone making the call must be identified. The ANI associated with the call is used to look up location information, or automatic location identifier (ALI). The ALI provides physical address information as well as contact numbers.

Emergency 911 calling will work as it does today. No changes will be made.

3.3. Media Resources

A media resource is a software-based or hardware-based entity that performs media processing functions on the data streams to which it is connected. Media processing functions include mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (media termination point), converting the data stream from one compression type to another (transcoding), streaming music to callers on hold (music on hold), echo cancellation, signaling, voice termination from a TDM circuit (coding/decoding), packetization of a stream, streaming audio (annunciation), and so forth. The software-based resources are provided by the Cisco Unified Communications Manager (Unified CM) IP Voice Media Streaming Service (IP VMS). Digital signal processor (DSP) cards provide both software and hardware based resources.

3.3.1. Conference Now

Cisco Conferencing solutions give users more secure collaboration from mobile devices, desktops, or meeting rooms. Bring employees, customers, and partners together to collaborate from anywhere with highly scalable voice, video, and content sharing.

The Conference Now feature allows both external and internal callers to join a conference by dialing a Conference Now IVR Directory Number, which is a centralized conference assistant number. An IVR application guides the caller to join the conference by playing announcements.

Conference Now will not be configured as part of this upgrade.

[Conference Now Configuration - Cisco Documentation](#)

3.3.2. (MoH) Music on Hold

MOH is an audio stream that is played to PSTN and VoIP callers who are placed on hold by phones in a Cisco Collaboration system. This audio stream is intended to reassure callers that they are still connected to their calls.

No changes will be made to Music on Hold.

3.4. Voicemail

This deployment will utilize Cisco Unity Connection for voicemail functionality.

Cisco Unity Connection lets users access and manage messages from an email inbox, web browser, Cisco Jabber, Cisco Unified IP Phone, smartphone, or tablet. Unity Connection also provides flexible message access and delivery format options, including support for voice commands, speech-to-text transcription, and even video greetings.

Cisco Unity Connection is highly secure. It is designed for complex distributed global deployments with support for high availability, redundancy, and branch office survivability. It is fully virtualized, and can be run on specification-based hardware.

Unity Connection is easily deployed, provisioned, monitored and managed using Cisco Prime Collaboration, our single application for unified management of the entire voice and video deployment.

[Cisco Unity Connection Design Guide](#)

**All Unity Connection configuration will be migrated from the old server.
No configuration changes will be made.**

3.5. Attendant Console

This deployment will utilize Cisco Unified Attendant Console Advanced.

Cisco Unified Attendant Consoles help you ensure all calls are handled efficiently and professionally. Call control allows users to answer, transfer, park, hold, place calls, and more—directly from the Cisco Unified Attendant Console, which controls a Cisco Unified IP Phone.

The built-in corporate directory synchronizes with Cisco Unified Communications Manager end-user directory, or with Active Directory.

Speed dials create frequently-dialed contacts that may or may not already reside in the corporate directory.

With busy lamp field and presence users can easily see a contact's availability from the activity of their phone and their presence state.

[Attendant Console Design Guide](#)

- **Attendant Console configuration will be migrated from the existing server.**

3.6.1. Server Requirements

One of the following activated operating systems, with Windows regional settings set to English:

- Windows Server 2008 R1 (32-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- **2 Windows server licenses will be required. One per CUAC server.**

Operating System Configuration Notes:

- Cisco Unified Attendant Console Advanced server must be installed and operated exclusively on a supported platform.
- Cisco Unified Attendant Console Advanced server does not run under any version of Windows Server 2003.
- To ensure system security, your operating system must be configured according to your company's operating system hardening guidelines. Take care to ensure that all CUACA-specific configuration requirements are still met after hardening.
- Internet Information Service (IIS) 6.0 or later, with the Static Content role service added.
- ASP.NET 2.0.50727 or later
- .Net Framework 3.5 SP1

Database Requirements:

- Microsoft SQL Server 2008 Express, Standard or Enterprise (32-bit or 64-bit)
- Microsoft SQL Server 2008 R2 Express, Standard or Enterprise (32-bit or 64-bit)
- Microsoft SQL Server 2008 SP3 Express, Standard or Enterprise (32-bit or 64-bit)
- Microsoft SQL Server 2012 Express, Standard or Enterprise (32-bit or 64-bit)
- Microsoft SQL Server 2014 Express, Standard or Enterprise (32-bit or 64-bit)
- **1 SQL server licenses will be required for the publisher server.**

Database Configuration Requirements:

- Cisco Unified Attendant Console Advanced server does not support multiple SQL database instances or named instances, and requires exclusive use of and access to a local installation of SQL server.
- No 64-bit version of Microsoft SQL Server is supported under Windows Server 2008 R1 (32-bit).
- If the Cisco Unified Attendant Console Advanced server installer does not detect a supported version of Microsoft SQL Server, it will automatically install Microsoft SQL Server 2008 Express.
- If you are installing Microsoft SQL yourself, you must install it locally on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced does not support the use of external SQL Servers.
- To ensure system security, your SQL installation must be configured according to your company's SQL system hardening guidelines. Take care to ensure that all CUACA-specific configuration requirements are still met after hardening.

Backup Requirements:

Allen Matkins must provide backup facilities to ensure application and data integrity in the event of unforeseen circumstances. If possible, choose a solution that offers one-step disaster recovery, such as the ability to restore the complete contents of a hard drive from a bootable floppy disk and the backup media.

Antivirus Software Requirements:

The Cisco Unified Attendant Console Advanced software constantly accesses files in certain folders; consequently, your anti-virus software will constantly try to scan them for viruses, which will slow down the server. Therefore, your chosen antivirus product must support exclusions, which you use to specify the following files and folders that are not to be scanned by the antivirus software:

Default Folder	Contains
\\DBData	System configuration databases
\\Program Files\Cisco\	Software and application trace files
\\Apache	Active MQ folder
\\Temp\Cisco\Trace Cisco	TSP trace files
\\%ALLUSERSPROFILE%\Cisco\CUACA	Cisco Profile

3.6.2. Desktop Requirements

PC Hardware Requirements:

- 2.0 GHz Pentium 4 processor
- 4 GB RAM
- 1 GB of available hard disk space
- Network card, connected to the network using TCP/IP
- SVGA (1024x768) display card
- 17-inch or larger monitor highly recommended
- SoundBlaster-compatible sound card and speakers highly recommended
- Keyboard with 10-key number pad

PC Software Requirements:

- Microsoft Windows Vista Professional 32-bit
- Microsoft Windows Vista Professional 64-bit (using WoW64 emulation)
- Microsoft Windows 7 32-bit
- Microsoft Windows 7 64-bit (using WoW64 emulation)
- Microsoft Windows 8
- Microsoft Windows 8 Pro
- Microsoft Windows 8 Enterprise
- Microsoft Windows 8.1
- Microsoft Windows 10

3.6. (PCD) Prime Collaboration Deployment

Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications (UC) applications. It allows you to perform tasks such as migration of older software versions of clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

Cisco Prime Collaboration Deployment has four primary high-level functions:

- Migrate an existing cluster of UC servers to a new cluster (such as MCS to virtual or virtual to virtual)
- Perform operations on existing clusters (8.6(1) or later). Examples of these operations include:
 - Upgrade and apply patches
 - Switch version
 - Restart

[PCD Design Guide](#)

ConvergeOne will utilize PCD to aid in the migration and upgrade of the Cisco applications.