TOMORROW starts here.

Deploying Cisco WebEx in Enterprise Networks (On-Premises or Cloud)

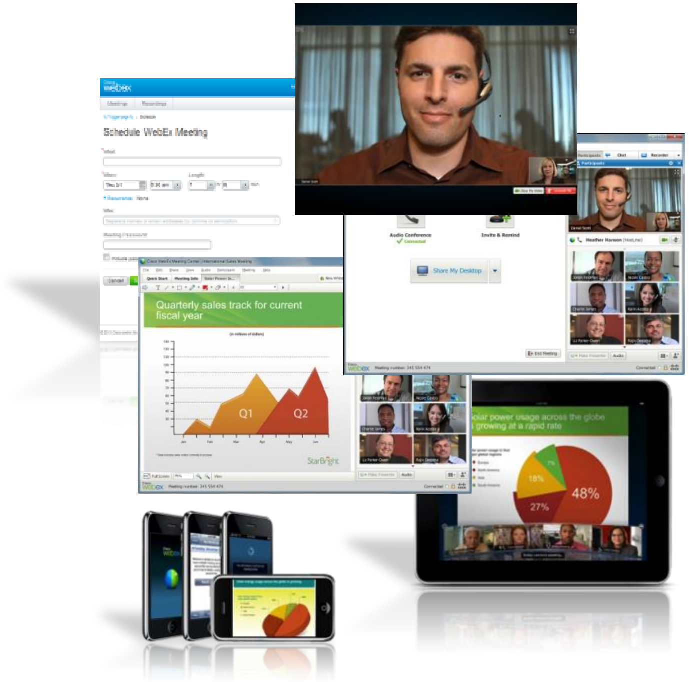
BRKCOL-2025

Cheyne Mailhot

Consulting Systems Engineer

Agenda

- Overview
- WebEx Cloud
  - Solution Overview
  - Configuration
  - Cloud Connect Audio
- Cisco WebEx Meetings Server
  - Solution Overview
  - Architecture
  - Deployment & Upgrades
- Resources
- Q&A



WebEx Conferencing

- Industry-leading web conferencing
  - Audio, web, and high-definition video
- Document, application, desktop sharing
- Consistent, cross-platform experience
  - Windows and Mac
  - Supported on mobile devices
- Delivered securely over the Cisco WebEx Cloud and on-premises

WebEx Cloud or WebEx Meeting Server

WebEx Cloud	WebEx On-Premise
Enterprise Edition - Meetings, Trainings, Events, Support	Meeting Centre
Broad range of 3rd party Plug-Ins	Outlook Calendaring Plug-In
Extensive Customisability	Limited Customisability
Unlimited Scalability	2,000 Peak Attendees (Ports)
Subscription Model	Perpetual User Licenses
Global Platform	Localised instances
HD Video / TelePresence Interoperability	Privacy or Regulatory requirements not met by SaaS

End of Sale - MeetingPlace

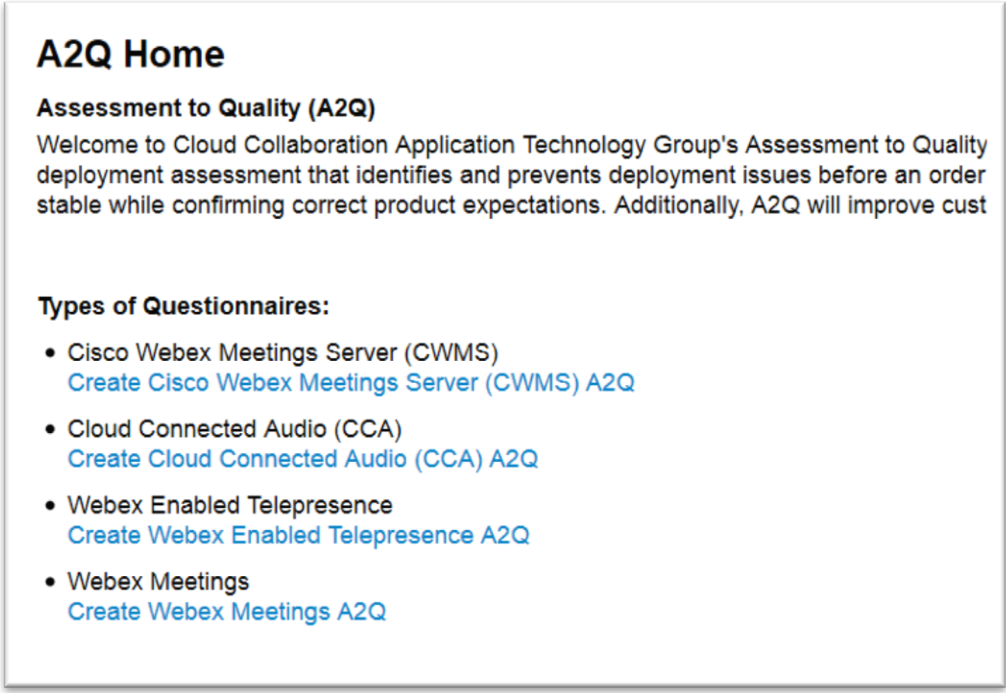
MeetingPlace Version #	License end-of-sale	Support end-of-life
MP Express	April 2010	April 2013
MP 6	July 2010	July 2013
MP 7	October 2012	October 2015
MP 8	August 2012	August 2015
MP 8.5	July 9, 2014	July 31, 2017

*** All MeetingPlace and MP Express UCSS SKUs being mapped to WebEx Meetings Server UCSS

A2Q Updates

- New Tool Available
- http://tools.cisco.com/atoq

- CWMS:
  - Form takes about 10 minutes and you can receive an instant approval if everything checks out.
  - If there are follow up items someone will verify and resubmit back to you.
  - There is no need to fill out the manual form anymore.



A2Q Home

Assessment to Quality (A2Q)

Welcome to Cloud Collaboration Application Technology Group's Assessment to Quality deployment assessment that identifies and prevents deployment issues before an order stable while confirming correct product expectations. Additionally, A2Q will improve cust

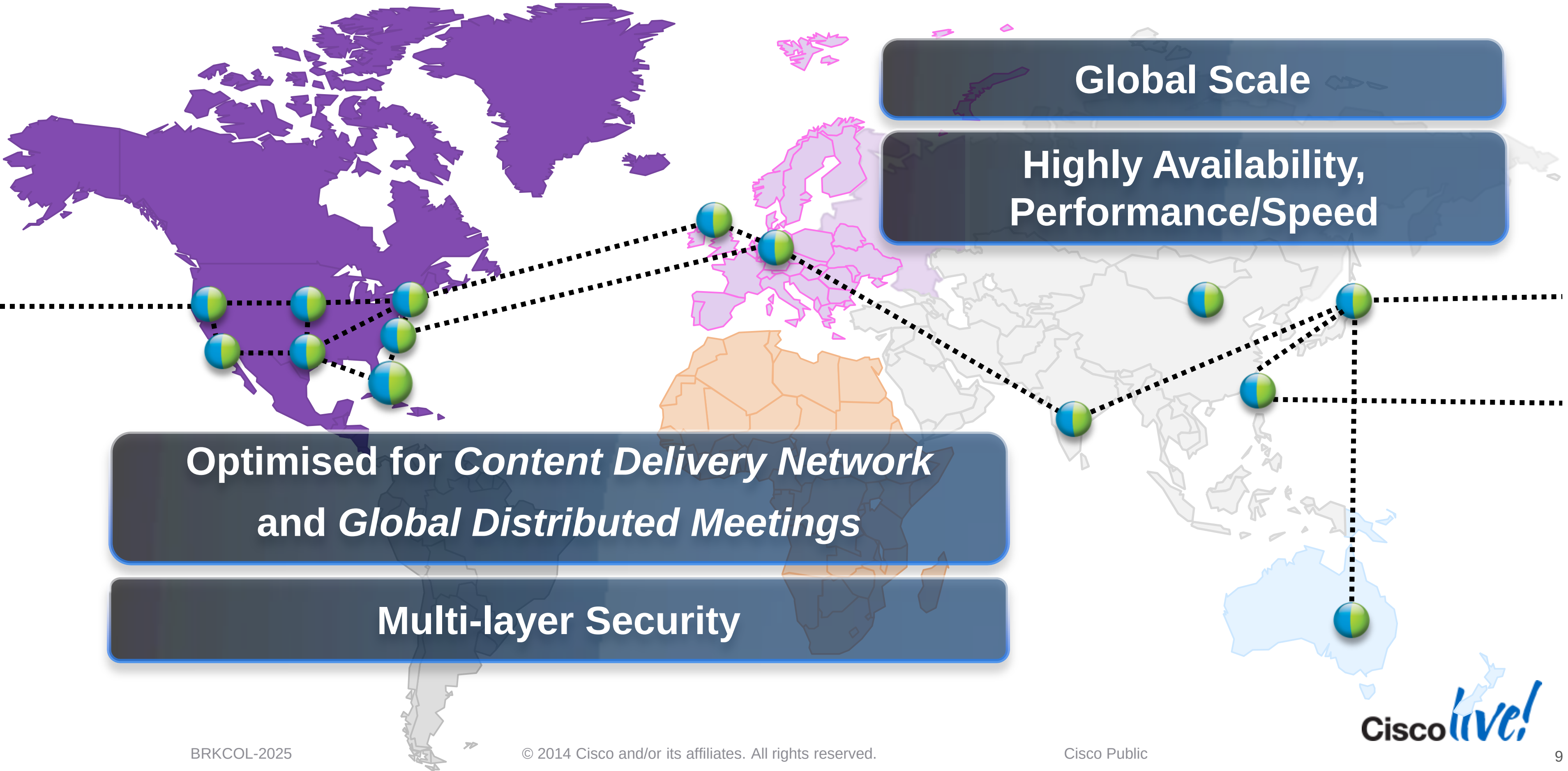
Types of Questionnaires:

- Cisco Webex Meetings Server (CWMS)
  Create Cisco Webex Meetings Server (CWMS) A2Q
- Cloud Connected Audio (CCA)
  Create Cloud Connected Audio (CCA) A2Q
- Webex Enabled Telepresence
  Create Webex Enabled Telepresence A2Q
- Webex Meetings
  Create Webex Meetings A2Q

WebEx Cloud

Solution Overview

WebEx Cloud



Global Scale

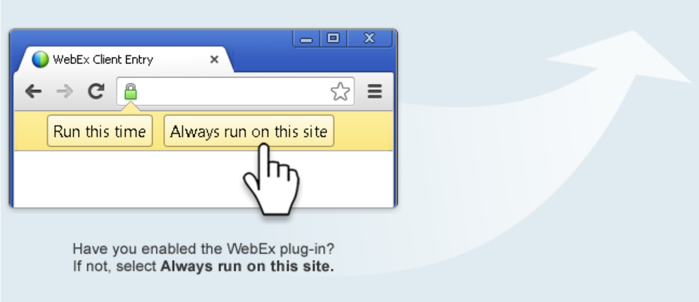
Highly Availability, Performance/Speed

Optimised for *Content Delivery Network* and *Global Distributed Meetings*

Multi-layer Security

Google & Mozilla Stop Using NPAPI Plug-ins

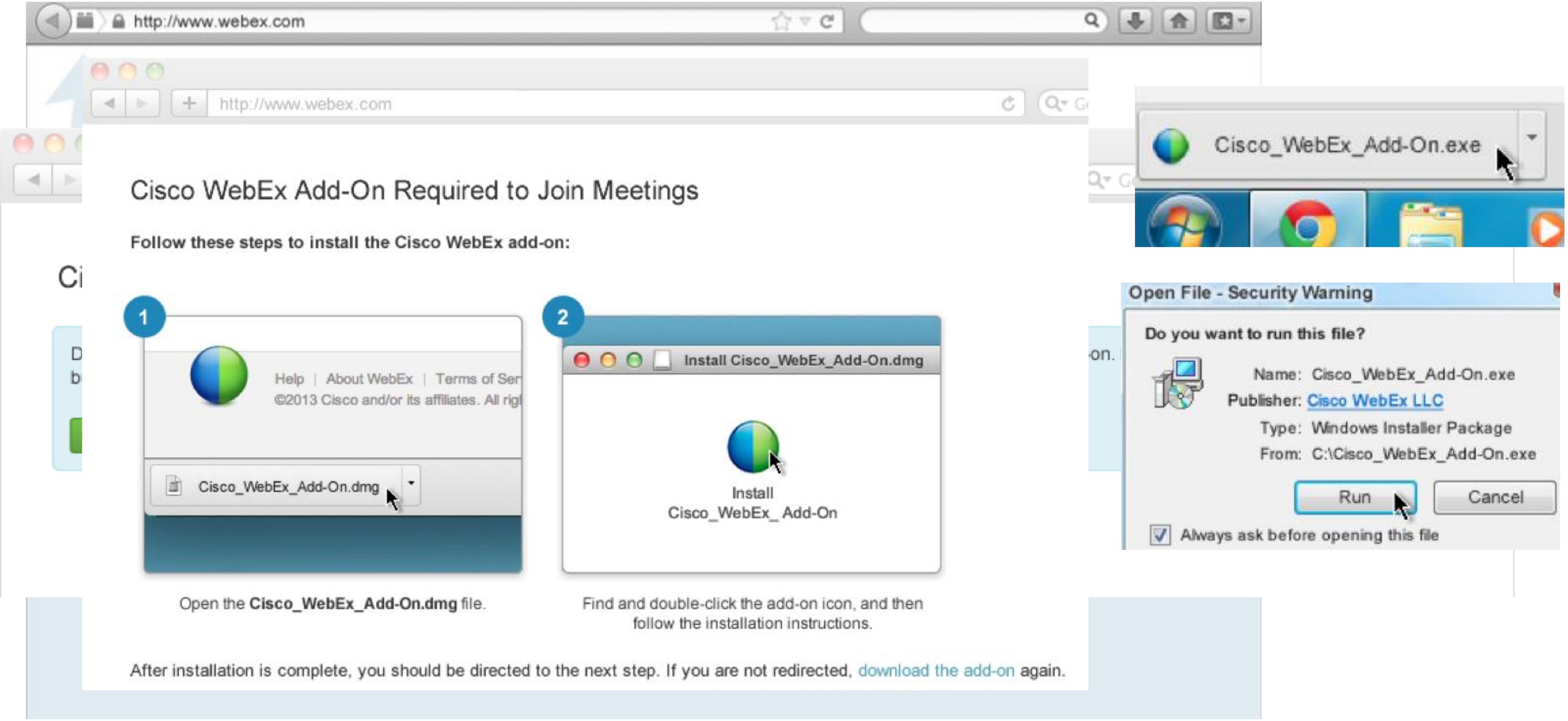
- NPAPI (Netscape Plug-in API) used by WebEx in Chrome, Firefox, & Safari to start meetings by launching the WebEx application from the browser
- Also impacts viewing a CWMS recording (streaming mode)
- From Chrome 32 (January) and Firefox 27 (February) ; estimated versions
- Add-on to be run once per URL and per browser
- No admin rights required



Have you enabled the WebEx plug-in?
If not, select **Always run on this site.**

More information: https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm

What Are We Doing About It?



http://www.webex.com

http://www.webex.com

Cisco WebEx Add-On Required to Join Meetings

Follow these steps to install the Cisco WebEx add-on:

1. Open the **Cisco_WebEx_Add-On.dmg** file.

2. Find and double-click the add-on icon, and then follow the installation instructions.

Help | About WebEx | Terms of Ser
©2013 Cisco and/or its affiliates. All rig
Cisco_WebEx_Add-On.dmg
Install Cisco_WebEx_Add-On.dmg
Install
Cisco_WebEx_ Add-On
Cisco_WebEx_Add-On.exe

After installation is complete, you should be directed to the next step. If you are not redirected, download the add-on again.

Open File - Security Warning

Do you want to run this file?

Name: Cisco_WebEx_Add-On.exe
Publisher: Cisco WebEx LLC
Type: Windows Installer Package
From: C:\Cisco_WebEx_Add-On.exe

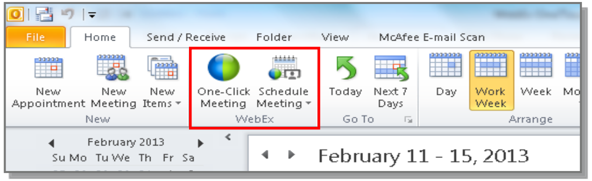
☑ Always ask before opening this file

More info here: https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm

WebEx Enabled TelePresence

1. Schedule

WebEx Productivity Tools



2. Launch

Click to join, One button to Push

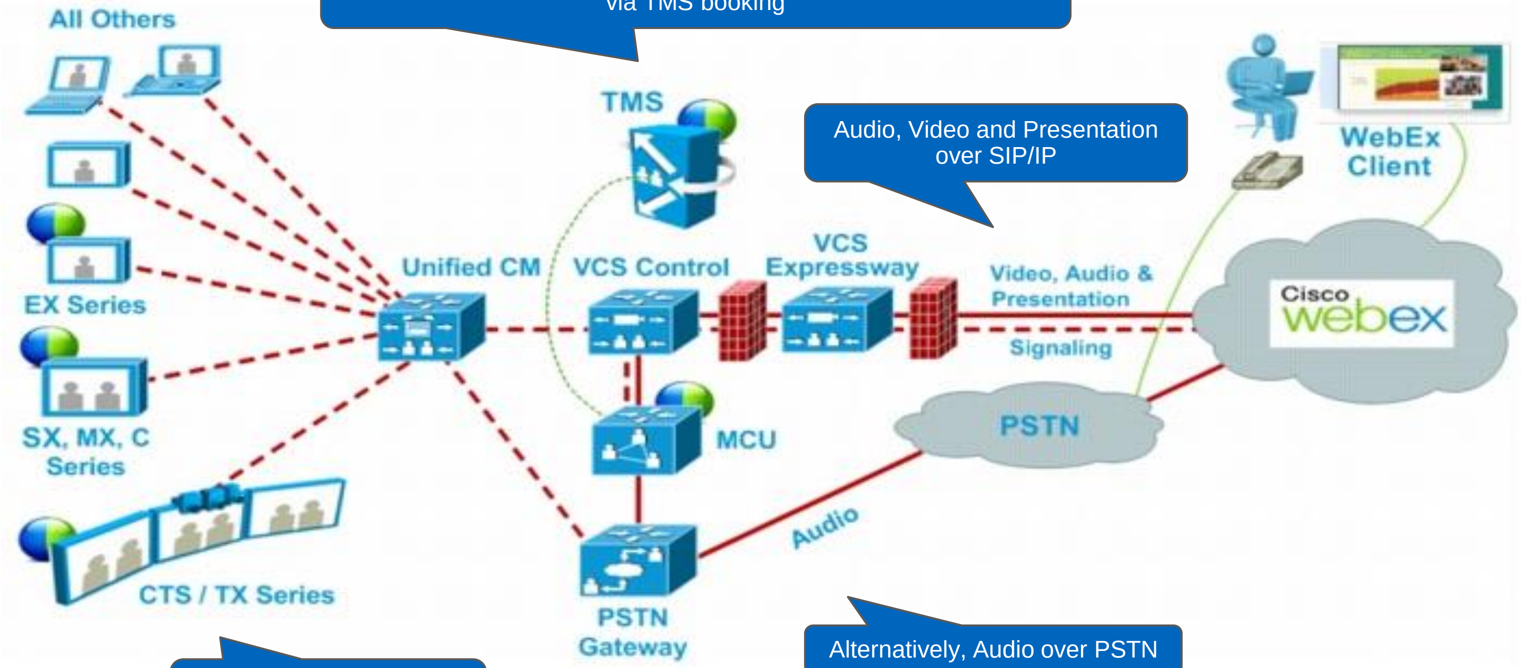
3. Meet

Voice, Video and Content

- Synchronised Audio Experience
- Easy Content Sharing
- Secure Collaboration Across All Video Endpoints

End - to - end security

WebEx for TelePresence Architecture



OneTouch scheduling in Outlook with WebEx Productivity Tool or via TMS booking

Audio, Video and Presentation over SIP/IP

Alternatively, Audio over PSTN

OBTP on all CTS, TX, EX, SX, MX and C Series

WebEx Cloud

Cloud Setup

WebEx Users - Directory DB

Adding New Users / Updating Users

- Site Administrators
  - Manually add users through Site Admin Tool
  - Add/Update users through CSV file import
  - Self sign-up page
- Cisco/WebEx Software Developer Kit (SDK)
  - Requires Developer Agreement for access and support
  - “Enterprise” (not WebEx on-line offers) XML APIs http://developer.webex.com
- WebEx doesn’t Delete user → Deactivate instead (auto-cleanup after 90+ days)
- Federated Single Sign-On (SSO)
  - Auto Account Create/Update (Optional) URL API
  - Requires “firstname”, “lastname”, “uid”, and “email”
  - Users are assigned the default session type / policy action

WebEx SSO

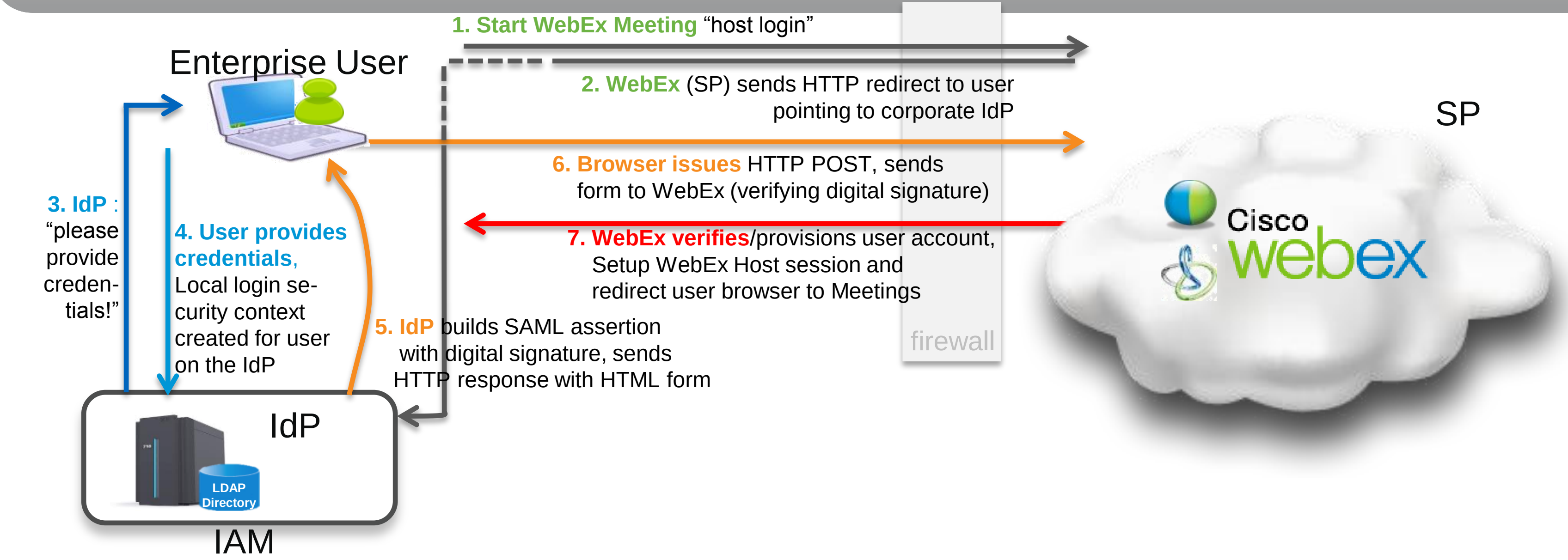
What Do We Need to Know About SSO Federation ?

- Users do not need to remember WebEx usernames or password
- **No WebEx passwords are stored or transmitted**
- Utilises WebEx Federated Authentication Service (FAS)
- Requires an Identity and Access Management (IAM) system that conforms to:
  - Security Assertion Markup Language (SAML) 1.1 or 2.0
  - WS-Federation 1.0
- IAM Certificate needs to be uploaded into WebEx
- The WebEx FAS has been tested with the following commercial IAM systems:

  CA SiteMinder, Ping Identity PingFederate, Sun Microsystems OpenSSO Enterprise Microsoft Windows Server ADFS and Geneva, Novell Identity Manager, IBM Tivoli Federated Identity Manager , Siemens IT Solutions DirX, TriCipher Armored Credential System

SSO Flow – SP Initiated

Users ***starts*** at the WebEx meeting site and are redirected to their corporate IAM (IdP) system for authentication. The IdP authenticates the user and sends a SAML assertion back to WebEx



1. **Start WebEx Meeting** "host login"

2. **WebEx** (SP) sends HTTP redirect to user pointing to corporate IdP

3. **IdP** : "please provide creden-tials!"

4. **User provides credentials,** Local login se-curity context created for user on the IdP

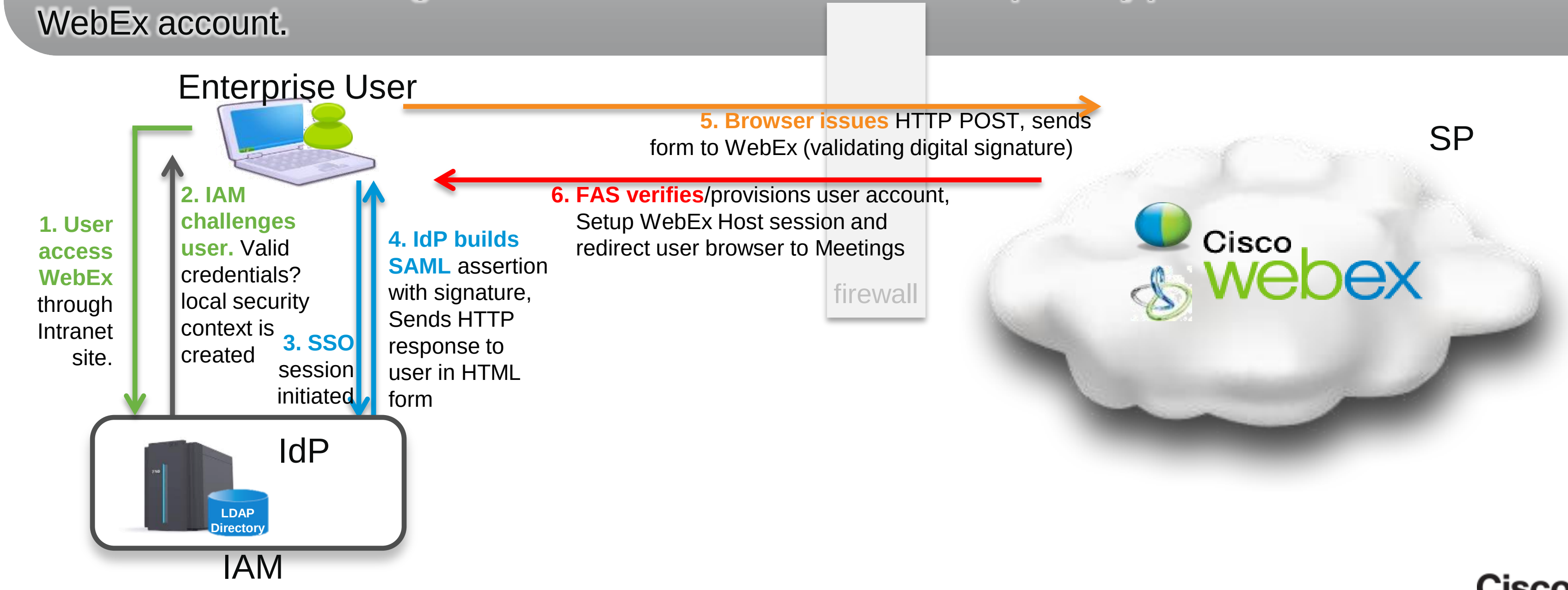
5. **IdP** builds SAML assertion with digital signature, sends HTTP response with HTML form

6. **Browser issues** HTTP POST, sends form to WebEx (verifying digital signature)

7. **WebEx verifies**/provisions user account, Setup WebEx Host session and redirect user browser to Meetings

SSO Flow – IdP Initiated

Users would access WebEx ***through*** their corporate IAM system. The IAM system acts as an IdP which would authenticate the user and verify they are authorised by the company to use WebEx. The IAM posts a signed SAML assertion to the WebEx FAS which verifies the signature and authenticates the user or optionally provisions a WebEx account.



Enterprise User

5. Browser issues HTTP POST, sends form to WebEx (validating digital signature)

6. FAS verifies/provisions user account, Setup WebEx Host session and redirect user browser to Meetings

1. User access WebEx through Intranet site.

2. IAM challenges user. Valid credentials? local security context is created

3. SSO session initiated

4. IdP builds SAML assertion with signature, Sends HTTP response to user in HTML form

Managing Video - Maximum Bandwidth

The bandwidth required to send the video is higher. The video technology used in the client software is using the multilayer frames to send video and allows the receiving client to automatically select the best possible resolution to receive video. Actual bandwidth used is less then the maximum and it is variable.

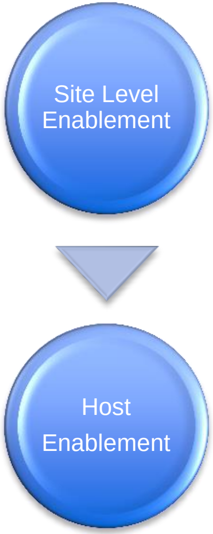
		Max bit rate (send)	Max bit rate (receive)
High Definition (HD)	720p (1280x720)	3.0 Mbps	2 Mbps
High Quality (HQ)	360p (640x360)	1.5 Mbps	1 Mbps
Standard Quality	180p (320x180)	0.5 Mbps	0.5 Mbps
6 thumbnails	90p	N/A	0.5 Mbps
1 thumbnails	90p	50 kbps	N/A

Conditions affecting performance of a WebEx session

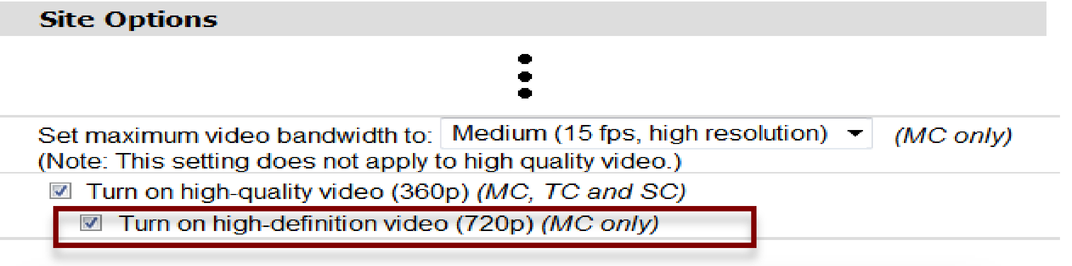
WebEx Network Bandwidth Whitepaper

http://www.webex.com/pdf/wp_bandwidth.pdf

Managing Video – Policy Settings


Site Level Enablement

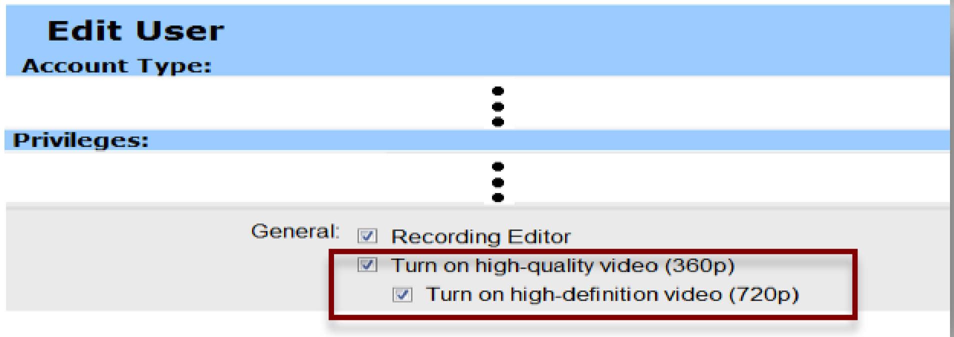
Host Enablement


Site Options

Set maximum video bandwidth to: Medium (15 fps, high resolution) *(MC only)*
(Note: This setting does not apply to high quality video.)

☑ Turn on high-quality video (360p) *(MC, TC and SC)*

☑ Turn on high-definition video (720p) *(MC only)*


Edit User

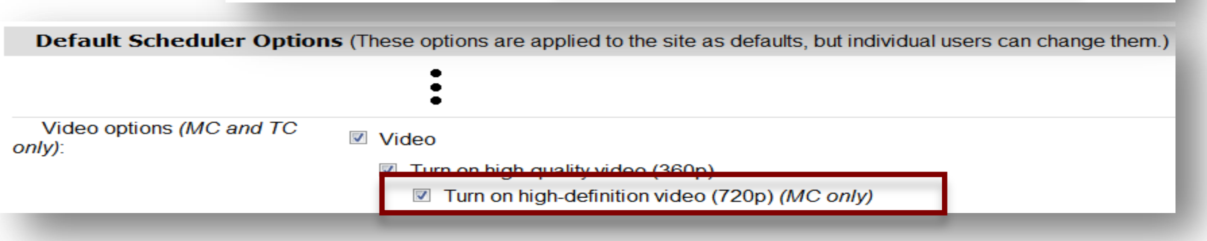
Account Type:

Privileges:

General: ☑ Recording Editor

☑ Turn on high-quality video (360p)

☑ Turn on high-definition video (720p)

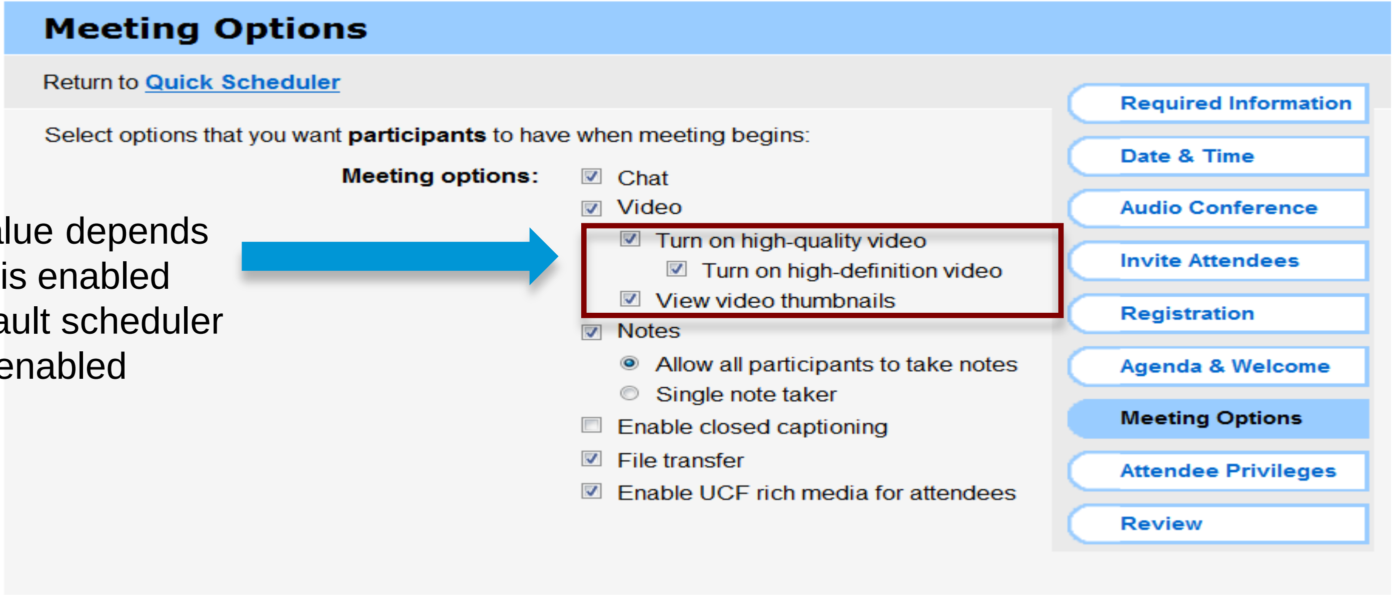

Default Scheduler Options (These options are applied to the site as defaults, but individual users can change them.)

Video options *(MC and TC only)*: ☑ Video

☑ Turn on high-quality video (360p)

☑ Turn on high-definition video (720p) *(MC only)*

Managing Video – User Level Control



Meeting Options

Return to Quick Scheduler

Select options that you want **participants** to have when meeting begins:

Meeting options:

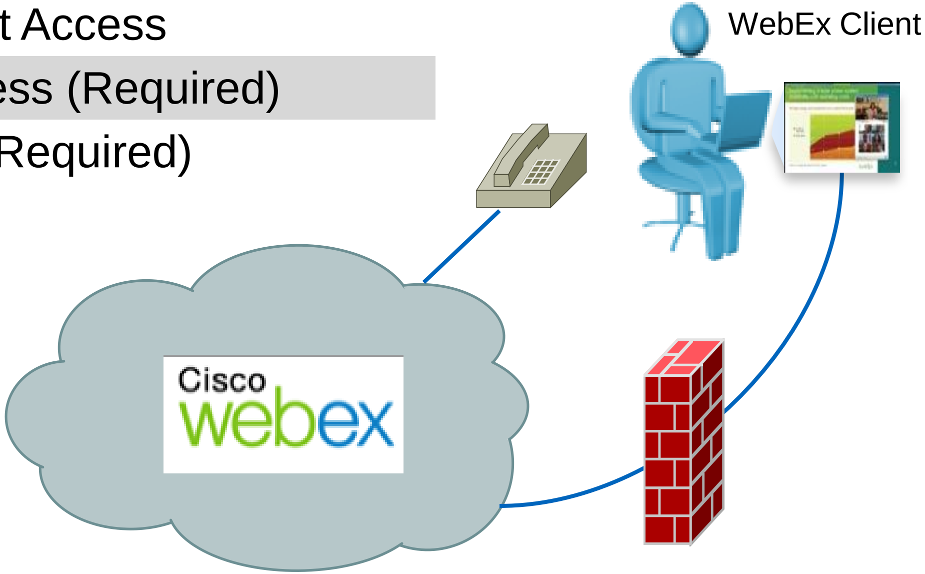
- ☑ Chat
- ☑ Video
  - ☑ Turn on high-quality video
    - ☑ Turn on high-definition video
  - ☑ View video thumbnails
- ☑ Notes
  - ● Allow all participants to take notes
  - ○ Single note taker
- □ Enable closed captioning
- ☑ File transfer
- ☑ Enable UCF rich media for attendees

Default value depends on if user is enabled and if default scheduler setting is enabled

* Enable these options during the scheduling process

Recommended Firewall Ports Settings

Protocol	Port	Access Type
TCP	80	Client Access
TCP	443	Client Access (Required)
TCP/UDP	53	DNS (Required)

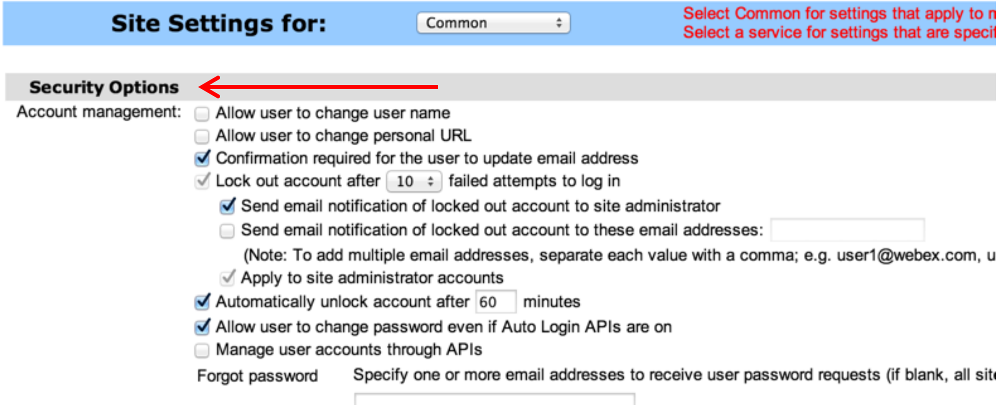


IP address ranges:

- 64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range)
- 66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range)
- 66.163.32.0/20 (CIDR) or 66.163.32.0 - 66.163.47.255 (net range)
- 209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range)
- 208.8.81.0/24 (CIDR) or 208.8.81.0 - 208.8.81.255 (net range)
- 210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range)
- 62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range)
- 173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range)
- 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)

KB WBX264 - How Do I Allow WebEx Traffic on My Network?

Security



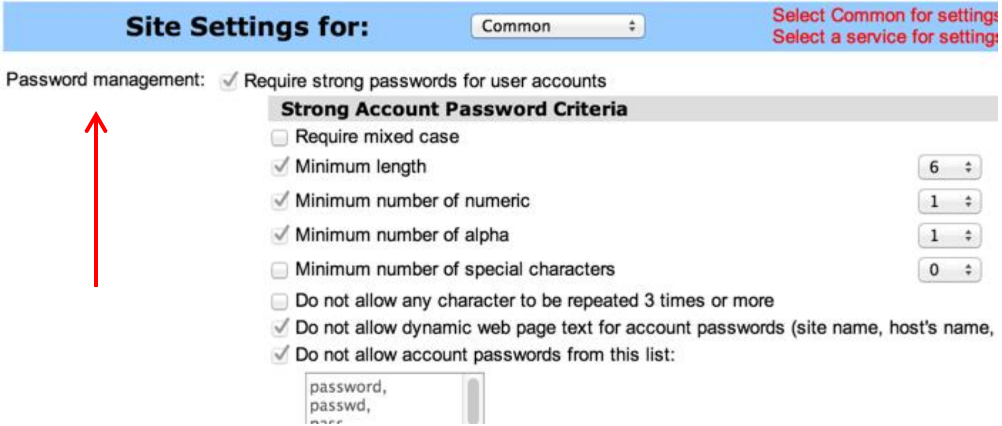
Site Settings for: Common

Select Common for settings that apply to n
Select a service for settings that are specit

Security Options

Account management:
- ☐ Allow user to change user name
- ☐ Allow user to change personal URL
- ☑ Confirmation required for the user to update email address
- ☑ Lock out account after 10 failed attempts to log in
  - ☑ Send email notification of locked out account to site administrator
  - ☐ Send email notification of locked out account to these email addresses:
  - (Note: To add multiple email addresses, separate each value with a comma; e.g. user1@webex.com, u
  - ☑ Apply to site administrator accounts
- ☑ Automatically unlock account after 60 minutes
- ☑ Allow user to change password even if Auto Login APIs are on
- ☐ Manage user accounts through APIs

Forgot password: Specify one or more email addresses to receive user password requests (if blank, all site



Site Settings for: Common

Select Common for setting
Select a service for setting

Password management: ☑ Require strong passwords for user accounts

Strong Account Password Criteria

- ☐ Require mixed case
- ☑ Minimum length 6
- ☑ Minimum number of numeric 1
- ☑ Minimum number of alpha 1
- ☐ Minimum number of special characters 0
- ☐ Do not allow any character to be repeated 3 times or more
- ☑ Do not allow dynamic web page text for account passwords (site name, host's name,
- ☑ Do not allow account passwords from this list:

```
password,
passwd,
pass
```

OPTIONAL:

- Attendee/Host privileges
- Password management
- Custom Session types
- File sharing permissions
- Require an account to join
- Recording (NBR) policies
- Storage allocation

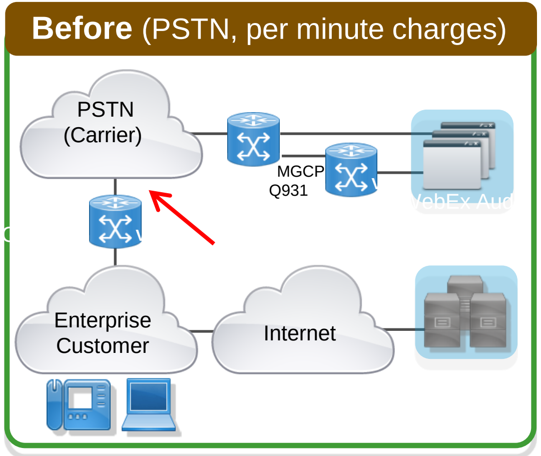
WebEx Cloud

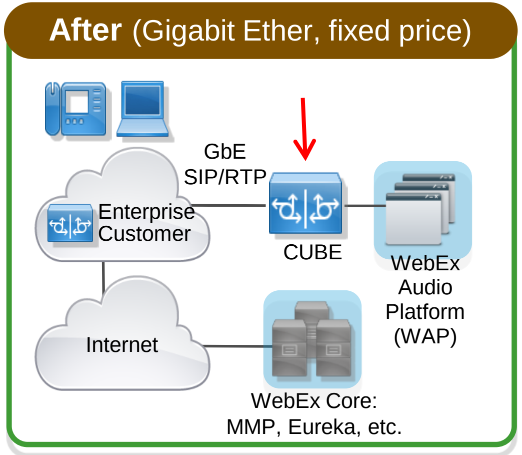
Cloud Connected Audio

CCA – Reducing the Cost of the WebEx Audio

Available Globally - Minimum 300 Audio Ports (1.5M minutes per month)

- A SIP trunking service, connecting customer’s telephones to WebEx’s conference servers
- Direct network peering with Enterprise customers
- Eliminates PSTN traversal, along with the associated costs, quality and reliability issues
- Replaces the per-minute price model with a flat rate for specific number of concurrent calls and possible future MP audio replacement as well
- SIP based
- Supports g.711 only
- Requires redundant MPLS
- sRTP not supported
- Supports both ISR/ASR
- Available on GPL
- Can mix with PSTN & VoIP
- TP integration coming soon

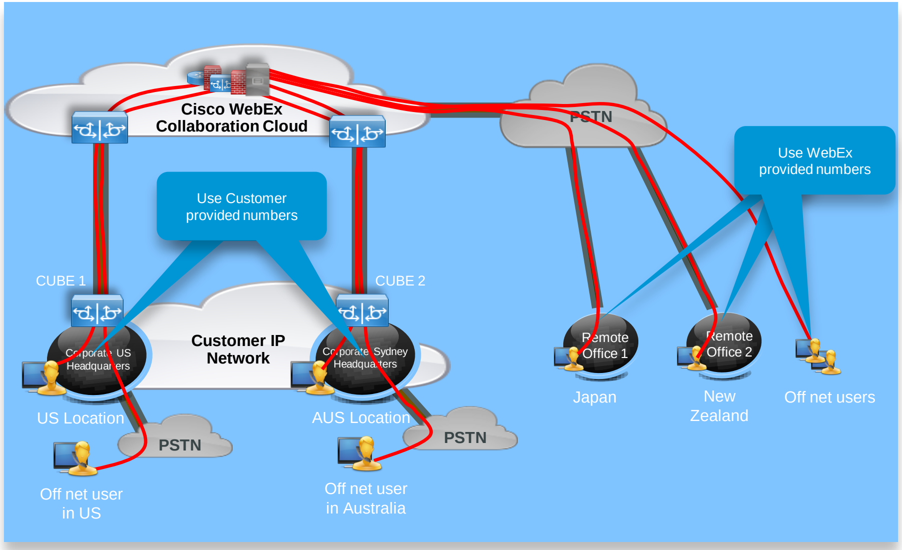




After (Gigabit Ether, fixed price)
GbE
SIP/RTP
Enterprise Customer
CUBE
WebEx Audio Platform (WAP)
Internet
WebEx Core: MMP, Eureka, etc.

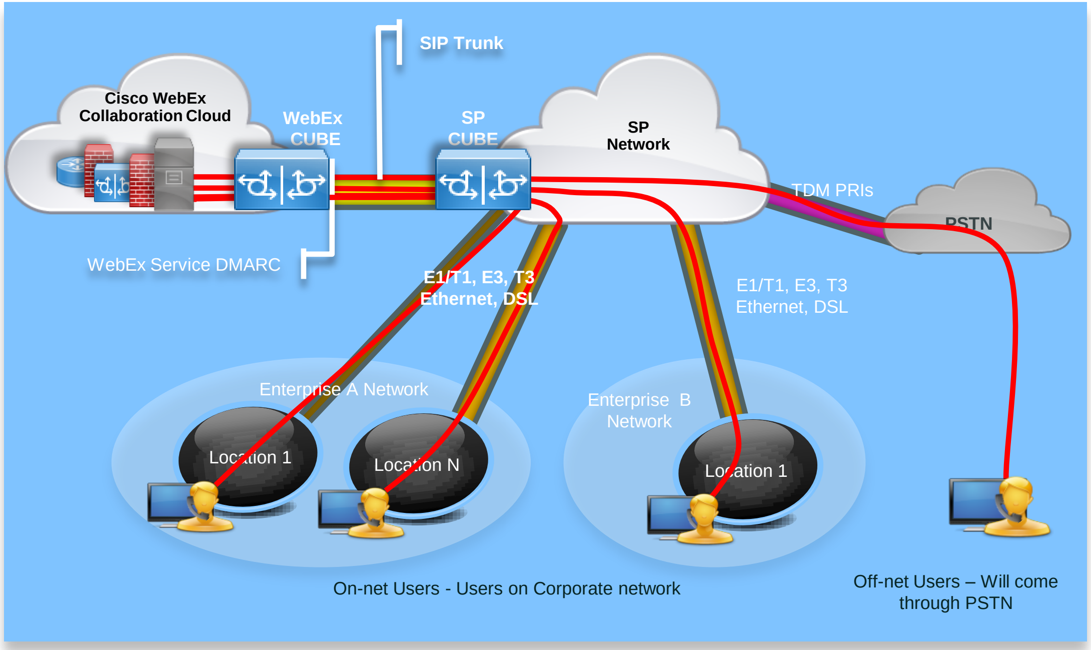
Hybrid Solution with CCA and PSTN Audio

- Customer can choose to have both CCA & WebEx PSTN audio on single WebEx site.
- Hybrid solution provides flexibility to customer to use WebEx PSTN numbers in countries where it does not have IP network.
- CCA billed based on ports and usage
- WebEx PSTN numbers billed by minutes
- In any given country, customer can either use CCA (its own numbers) or WebEx provided numbers but not both.


Cisco WebEx Collaboration Cloud
PSTN
Use WebEx provided numbers
Use Customer provided numbers
CUBE 1
CUBE 2
Customer IP Network
Corporate US Headquarters
Corporate Sydney Headquarters
Remote Office 1
Remote Office 2
Japan
New Zealand
Off net users
US Location
AUS Location
PSTN
PSTN
Off net user in US
Off net user in Australia

CCA SP Integrated Architecture (1HCY2014)

- Network to Network peer between Cisco/WebEx and SP
- Cisco/WebEx provides audio mixing from its cloud and SP provides the call routing for both on-net and off-net calls
- WebEx callback will be made to SP and SP to route the callback to the user
- SP owns the customer and provides tier 1 support


SIP Trunk
Cisco WebEx Collaboration Cloud
WebEx CUBE
SP CUBE
SP Network
TDM PRIs
PSTN
WebEx Service DMARC
E1/T1, E3, T3 Ethernet, DSL
E1/T1, E3, T3 Ethernet, DSL
Enterprise A Network
Enterprise B Network
Location 1
Location N
Location 1
On-net Users - Users on Corporate network
Off-net Users – Will come through PSTN

WebEx Meetings Server

Solution Overview

An Entirely New WebEx Deployment Model

- WebEx meetings in a private cloud
  - Installed in your Data Centre
- All-in-one conferencing solution
  - Incorporates audio, web and video in a single solution
- Same great WebEx user experience
  - WebEx clients for PC, Mac, Andriod, iPhone, and iPad; high quality video; sharing, annotation, and collaboration tools; recording and playback etc.
- Software based
  - Designed for Cisco UCS Servers + VMware
- Integrates with Cisco UC suite
  - Extends Cisco Unified Communications Manager to conferencing, and meeting escalation from Jabber.

Secure

Designed for Customers with High Security Requirements

- Behind the firewall installation
- 100% 128 and 256 Bit SSL encrypted online meetings
- Industry-standard 2048 Bit encryption keys
- Wild-card and SAN SSL certificate support
- Optional TLS/SRTP SIP teleconferencing encryption
- Hardened ‘Virtual Appliance’ with SE/Linux extensions
- NIST FIPS 140-2 approved cryptographic algorithms supported

What's New?

- CentOS upgrade to 6.4
- Updated Client Support, PT tools, mobile devices
- NAS Storage
- Per Meeting increase in participants 250
- Android Client Support
- Admin and User Improvements
- Configurable entry/exit settings

What's Coming?

- Dual-data centre HA
- Increased System Scalability (>= 4,000 concurrent users)
- JITC compliance
- IPv6
- SSO enhancements
- Expanded security and certificate management
- Access-controlled meetings
- Blast dial-out

UCS Bundles

- Primary and IRP bundles – available for both B and C series
- Bundles will receive special discounts. ~15%
- Only 800 Blade includes HDD, others require SAN

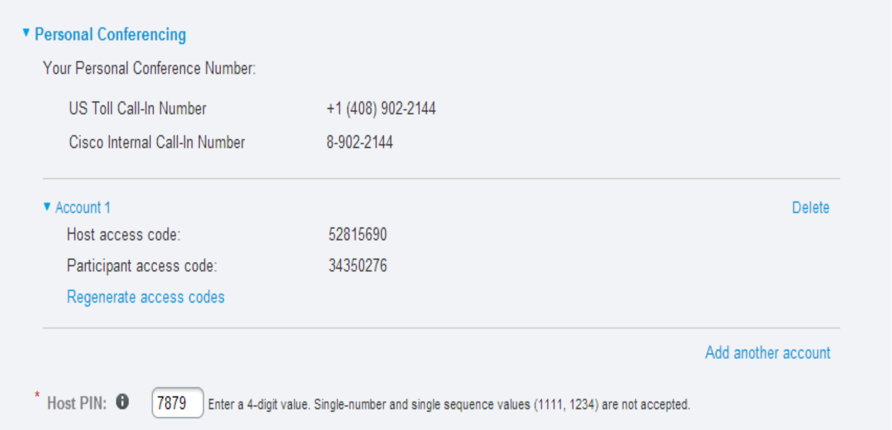
- **50 Port Server:**
  - 50 P is for admin or IRP
  - 50 I is for the all in one Primary/IRP/Centre

- **250 Port Server:**
  - 250 P is for admin or IRP
  - 250 I is for Admin/vCentre Co-Resident

- **800 & 2000 Port Server:**
  - 800 P is for 800 or 2000 Admin
  - 800 I is for 800 or 2000 IRP

Personal Conferencing Numbers (PCN)

- Hosts can create up to 3 PCN accounts
- Each account consists of a Host Access Code and Attendee Access Code
- Accounts are available 24x7; no prior scheduling required
- Hosts dial telephony access number, then entering Host Access Code and security PIN
- Attendees join by dialing telephony access number and entering Attendee Access Code
- Web portion available (if needed)



▾ Personal Conferencing

Your Personal Conference Number:

US Toll Call-In Number	+1 (408) 902-2144
Cisco Internal Call-In Number	8-902-2144

▾ Account 1 — Delete

Host access code:	52815690
Participant access code:	34350276

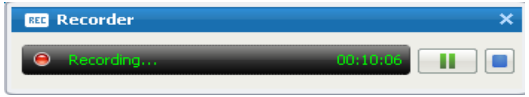
Regenerate access codes

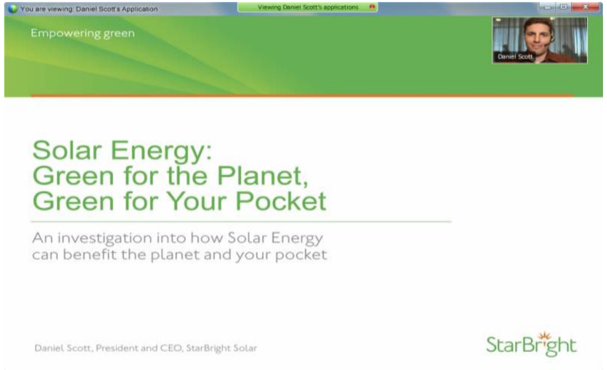
Add another account

* Host PIN: 7879 Enter a 4-digit value. Single-number and single sequence values (1111, 1234) are not accepted.

Recording Features

- WebEx “.arf” formats (proprietary)
- Requires storage server
- Unique URL for both internal and external users
- Enable or Disable Recordings (system wide)
- Cannot be automated for all sessions
- **Downloadable and convertible**
- Player for Windows and Mac OS
- Set recording when scheduling




You are viewing: Daniel Scott's Application

Viewing Daniel Scott's applications

Empowering green

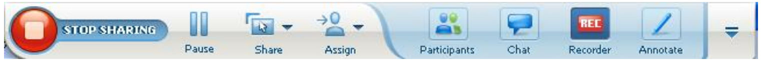
Daniel Scott

Solar Energy:
Green for the Planet,
Green for Your Pocket

An investigation into how Solar Energy can benefit the planet and your pocket

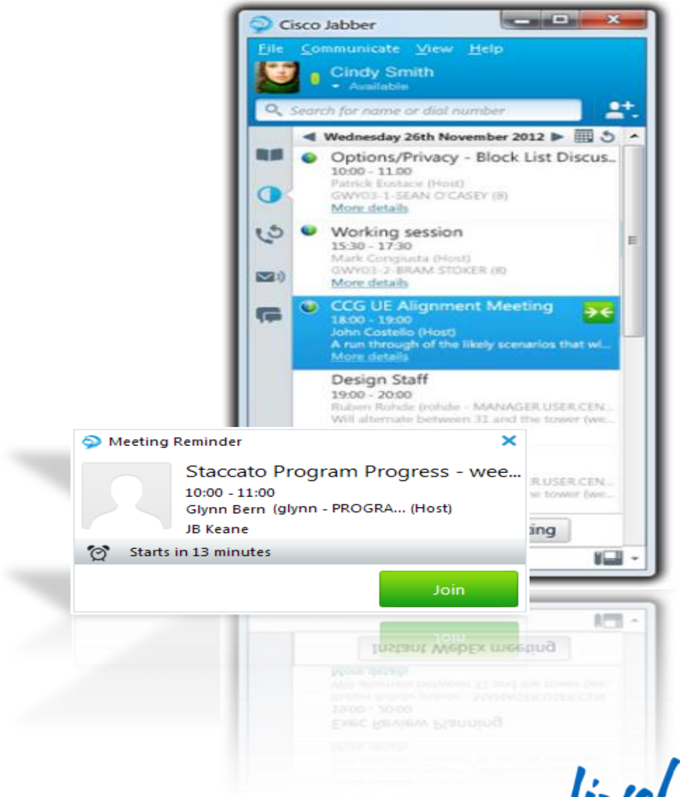
Daniel Scott, President and CEO, StarBright Solar

StarBright



Cisco Jabber Integration

- Jabber for Windows only (from 9.1.2)
- On-premise presence server only
- Display and launch scheduled CWMS meetings
- Start /Join CWMS meeting -Start instant meeting
- Escalate IM Session to a full CWMS meeting
- Authentication method:
  - Manually entered by users
  - SSO on CWMS



Options/Privacy - Block List Discus...
10:00 - 11.00
Patrick Eustace (Host)
GWY03-1-SEAN O'CASEY (8)
More details

Working session
15:30 - 17:30
Mark Congiusta (Host)
GWY03-2-BRAM STOKER (8)
More details

CCG UE Alignment Meeting
18:00 - 19:00
John Costello (Host)
A run through of the likely scenarios that wi...
More details

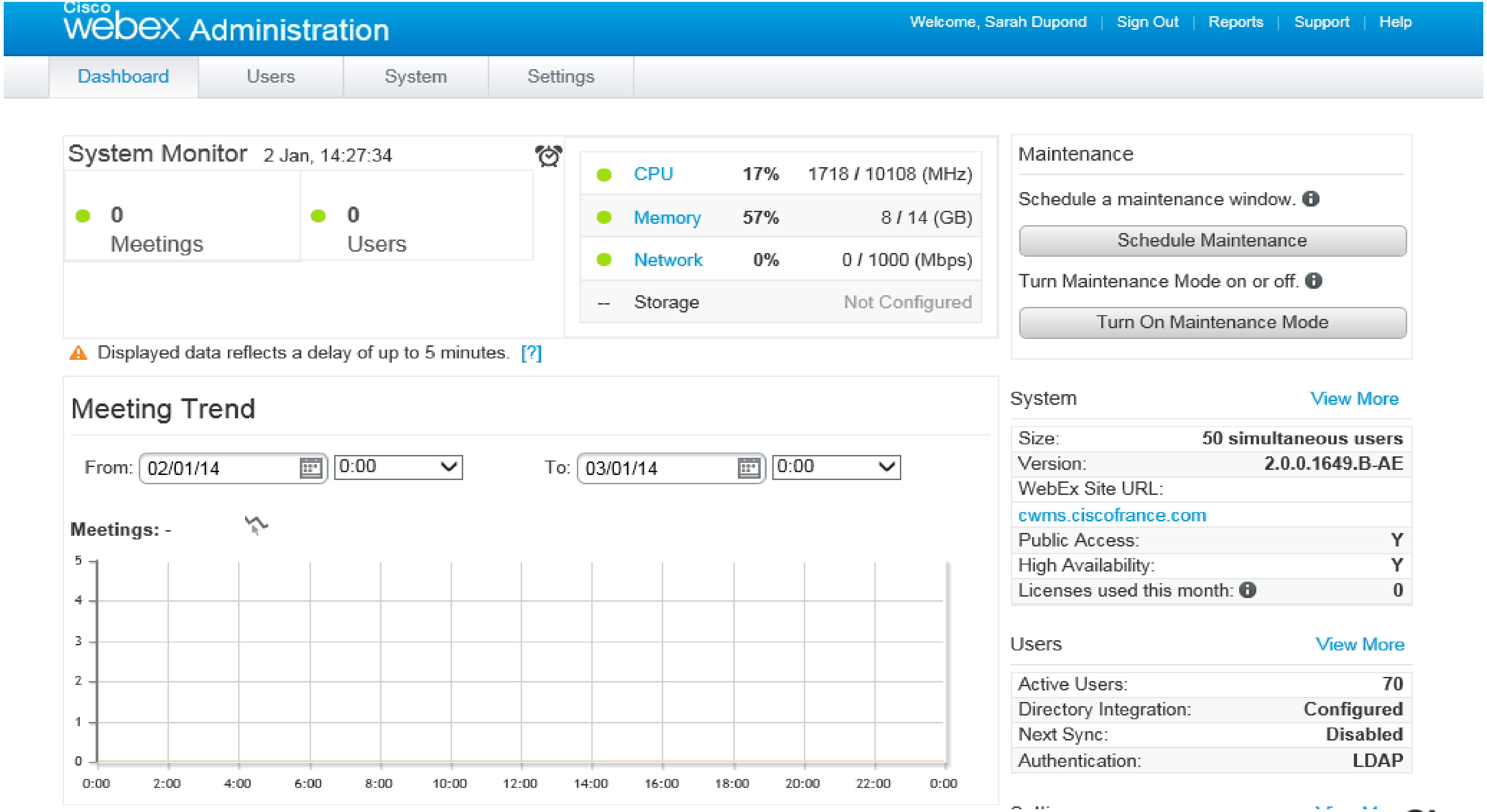
Design Staff
19:00 - 20:00
Ruben Rohde (rohde - MANAGER.USER.CEN...
Will alternate between 31 and the tower (we...

Meeting Reminder

Staccato Program Progress - wee...
10:00 - 11:00
Glynn Bern (glynn - PROGRA... (Host)
JB Keane

Starts in 13 minutes

Administration dashboard overview (2.0)



Cisco webex Administration
Welcome, Sarah Dupond | Sign Out | Reports | Support | Help
Dashboard
Users
System
Settings

System Monitor 2 Jan, 14:27:34

● 0 Meetings

● 0 Users

●	CPU	17%	1718 / 10108 (MHz)
●	Memory	57%	8 / 14 (GB)
●	Network	0%	0 / 1000 (Mbps)
--	Storage		Not Configured

⚠ Displayed data reflects a delay of up to 5 minutes. [?]

Maintenance

Schedule a maintenance window.

Turn Maintenance Mode on or off.

Meeting Trend

From: 02/01/14 0:00 To: 03/01/14 0:00

Meetings: -

System View More

Size:	50 simultaneous users
Version:	2.0.0.1649.B-AE
WebEx Site URL:	
cwms.ciscofrance.com	
Public Access:	Y
High Availability:	Y
Licenses used this month:	0

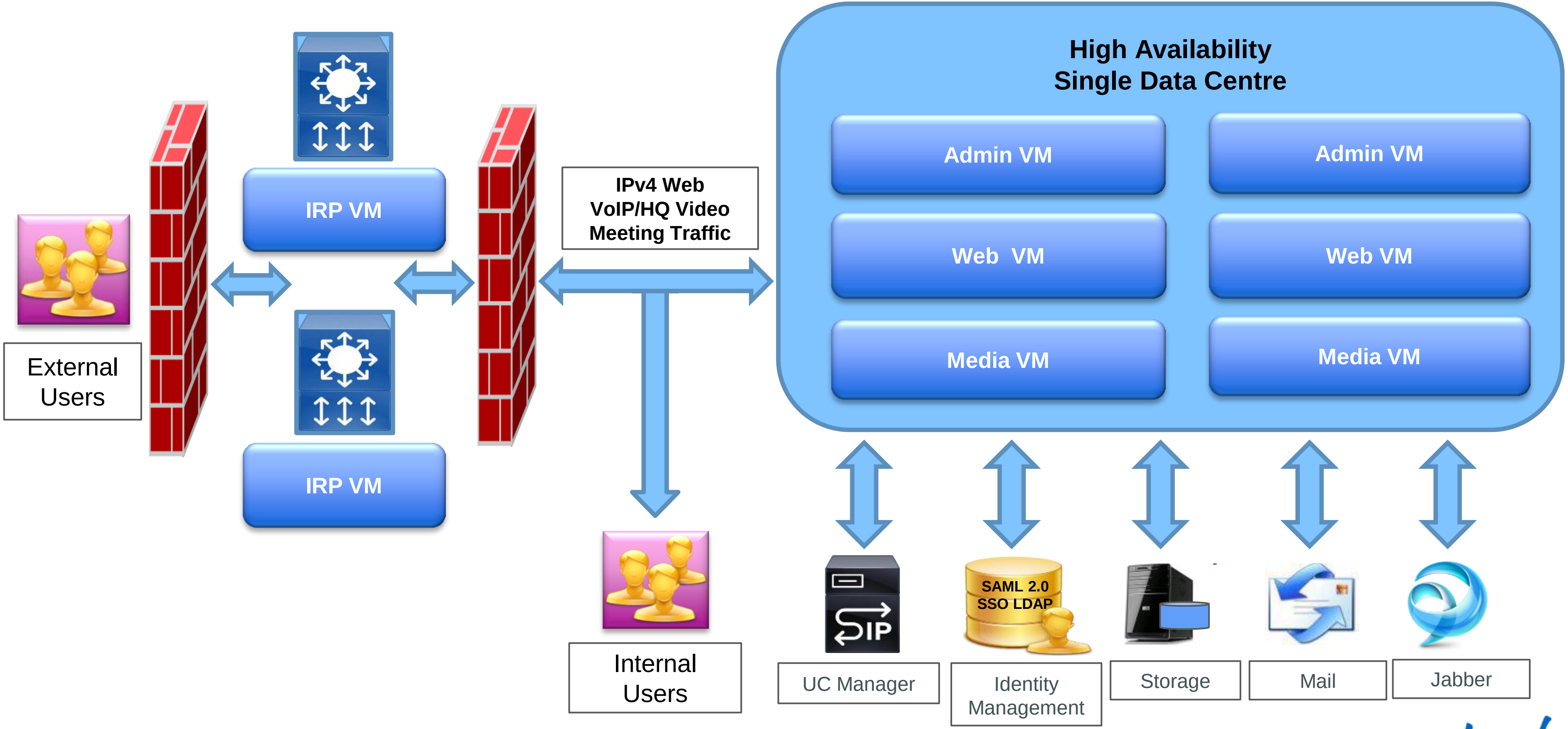
Users View More

Active Users:	70
Directory Integration:	Configured
Next Sync:	Disabled
Authentication:	LDAP

WebEx Meetings Server

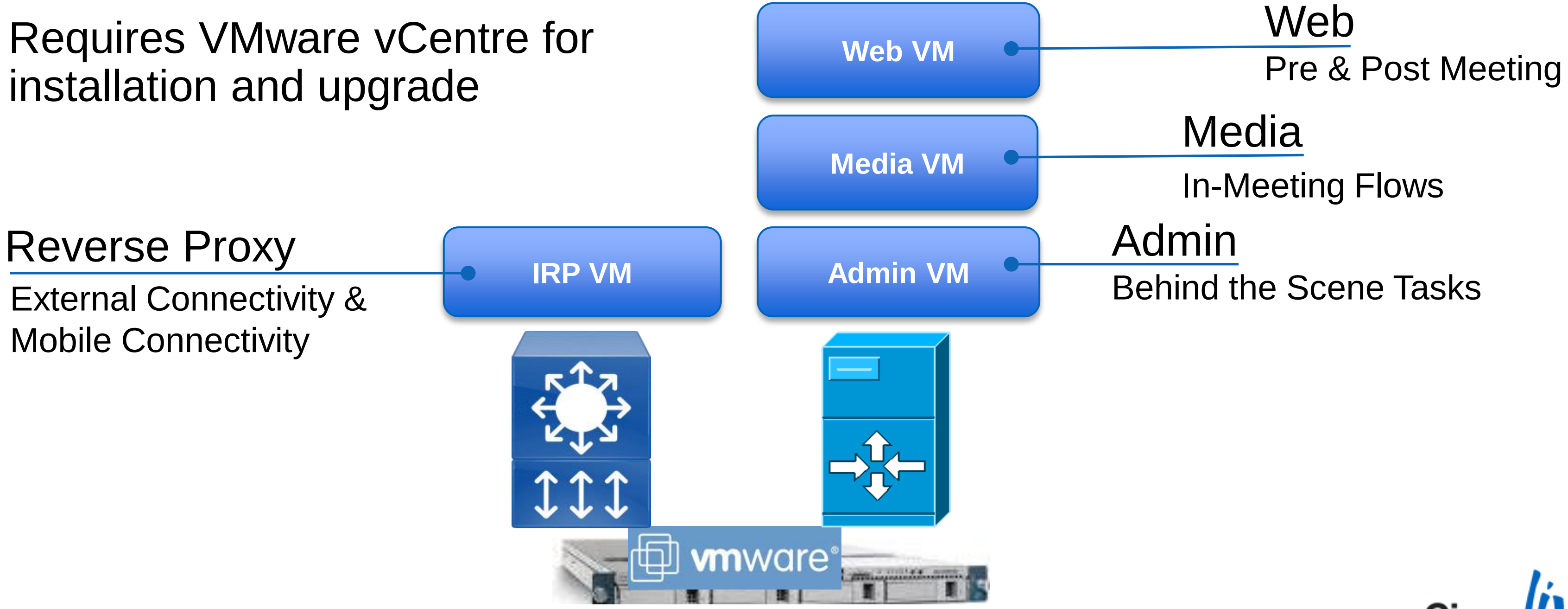
Architecture

Architecture Overview



Components Overview

- Designed for VMware 5/5.1
- Runs on Cisco UCS Servers only
- Requires VMware vCentre for installation and upgrade



Web

Pre & Post Meeting

Media

In-Meeting Flows

Admin

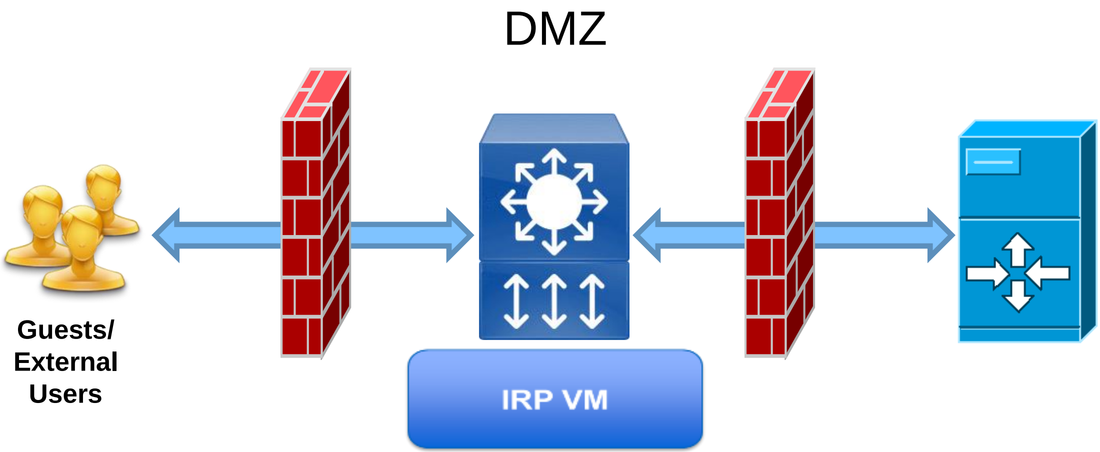
Behind the Scene Tasks

Reverse Proxy

External Connectivity & Mobile Connectivity

Internet Reverse Proxy

- Tunnel established from inside to outside
- Mandatory for External Participants and to provision Mobile access



- Minimum 1 Public IP
- Nat supported
- External Ports:
  - 80 (TCP)
  - 443 (TCP)
  - Internal Flow: 443 (TCP)
- Load balancing
- FIPS security requirements
- SSL encryption/decryption

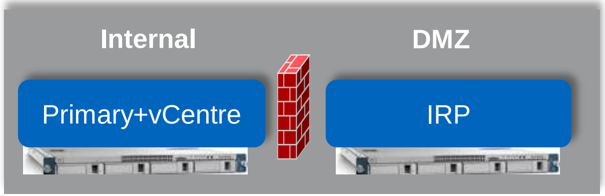
System Capacities

Media Type	50 ports	250 ports	800 ports	2000 ports
100% SIP/PC audio	50	250	800	2000
Encrypted Audio (sRTP) *	50	250	800	2000
Concurrent HQ Video/ Video sharing	25	125	400	1000
Meeting Size	50	100	**250 (HA)**	**250 (HA)**
Data sharing	50	250	800	2000
Concurrent Recording	3	13	40	100

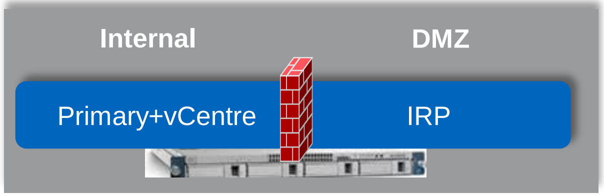
*Includes high fidelity Codecs E.g. G722

50 User Deployment Layout

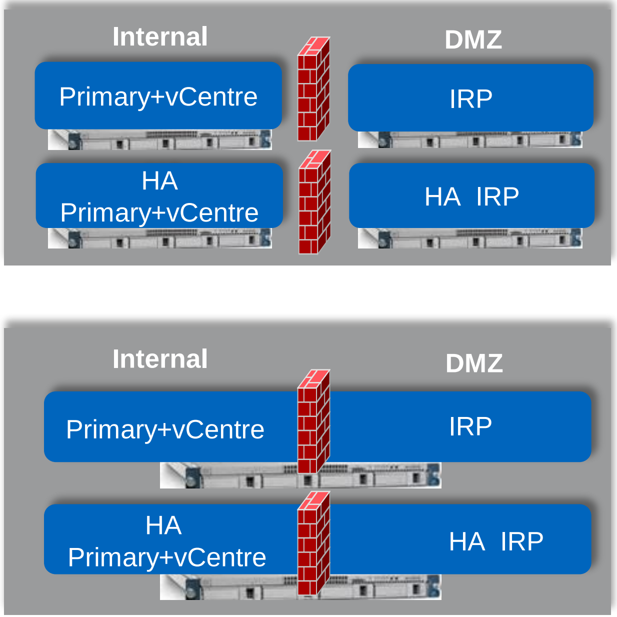
Primary & vCentre CoResident – IRP separate UCS



OR

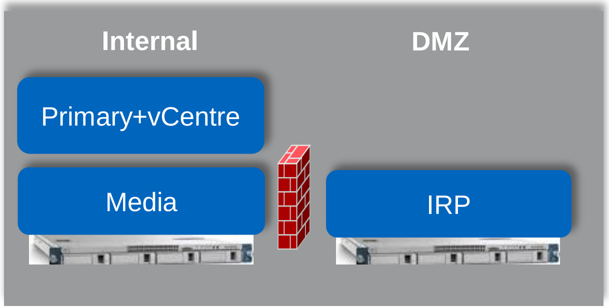


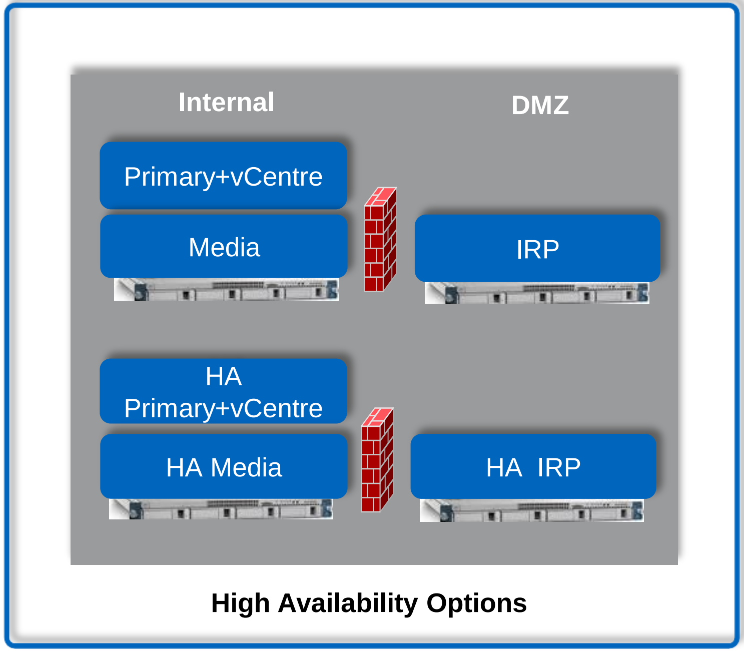
Primary, vCentre, IRP CoResident – Dual homed



High Availability Options

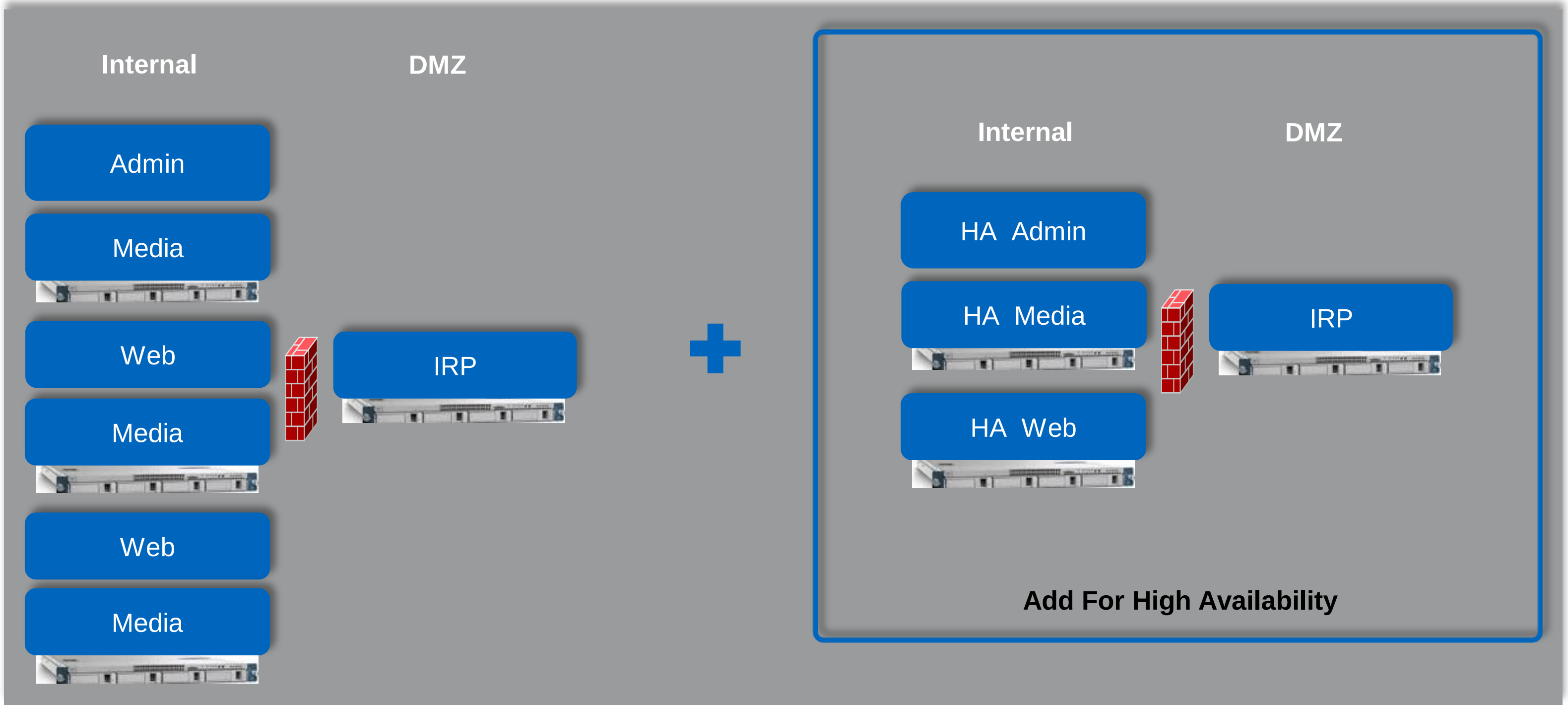
250 & 800 User Deployment Layout



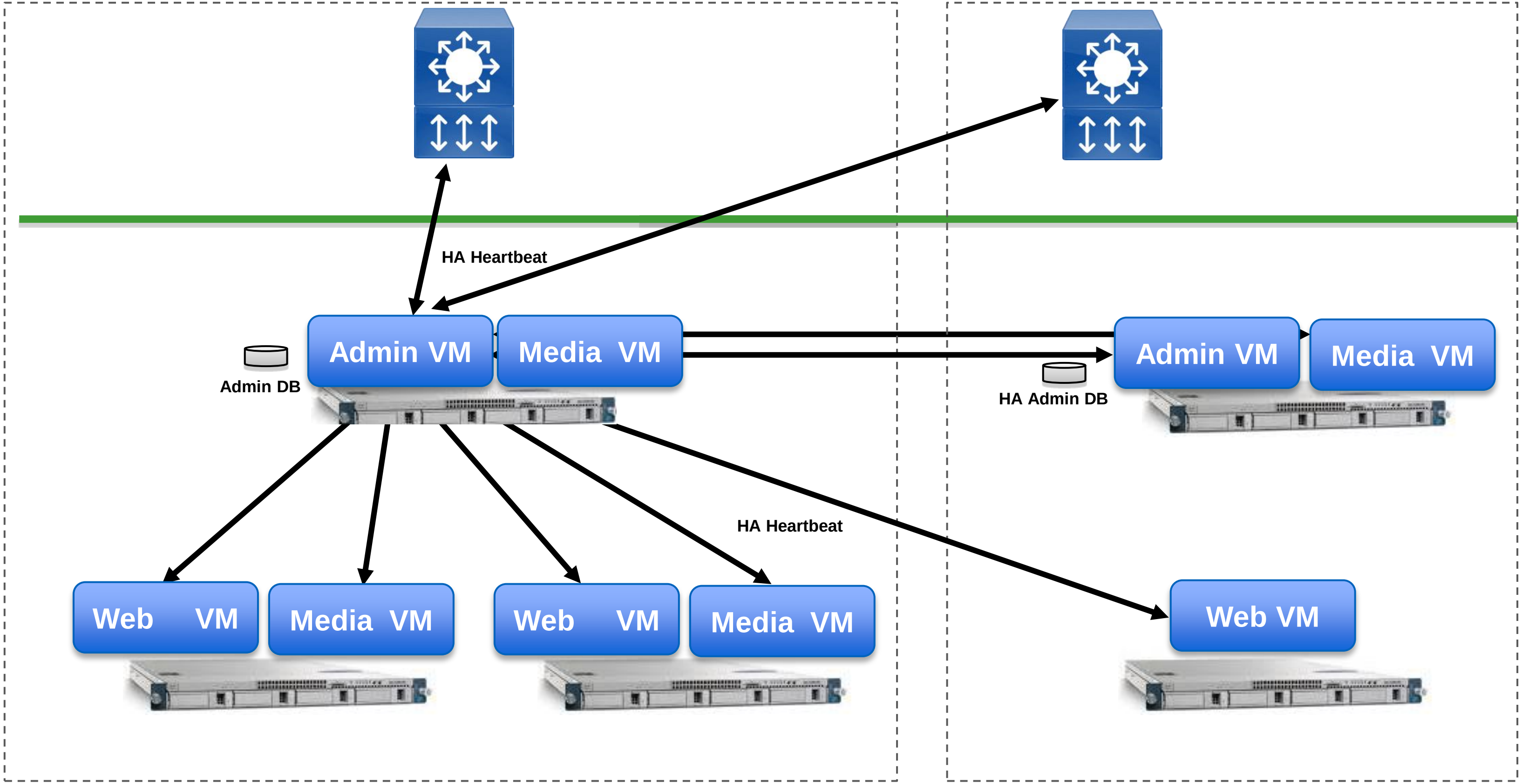


High Availability Options

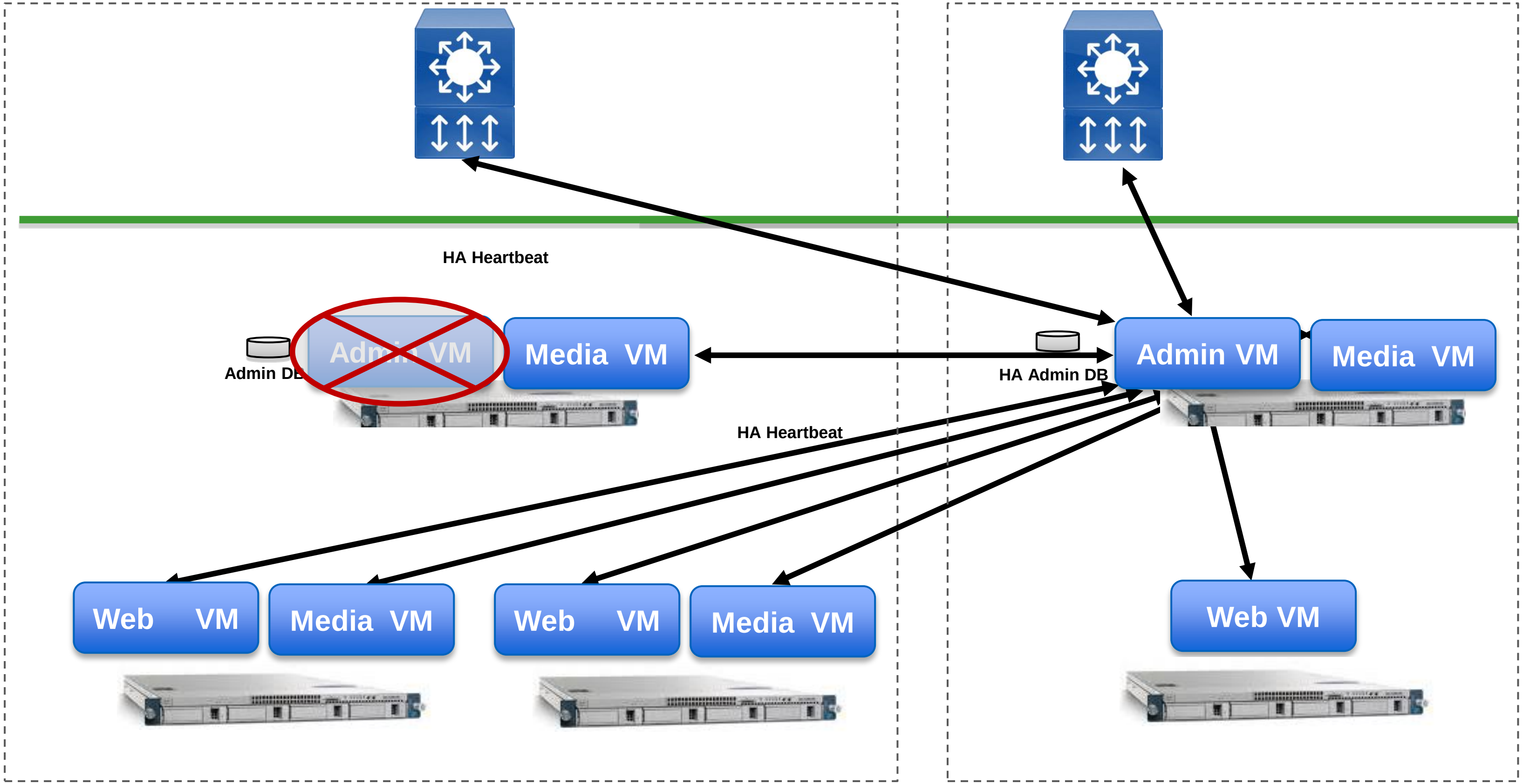
2000 User Deployment Layout



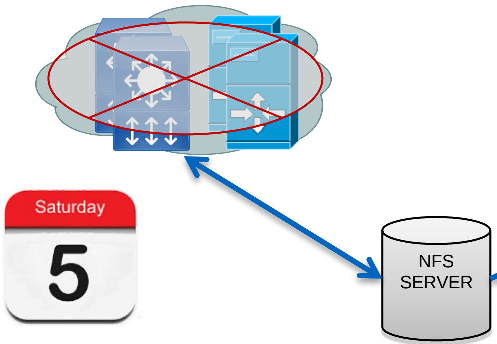
2000 User With High Availability

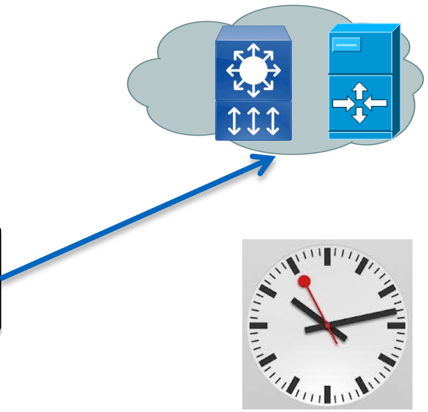


2000 User With High Availability

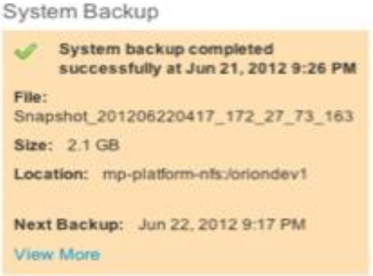


CWMS Disaster Recovery





>30 min



System Backup

System backup completed successfully at Jun 21, 2012 9:26 PM

File: Snapshot_201206220417_172_27_73_163

Size: 2.1 GB

Location: mp-platform-nfs:/oriondev1

Next Backup: Jun 22, 2012 9:17 PM

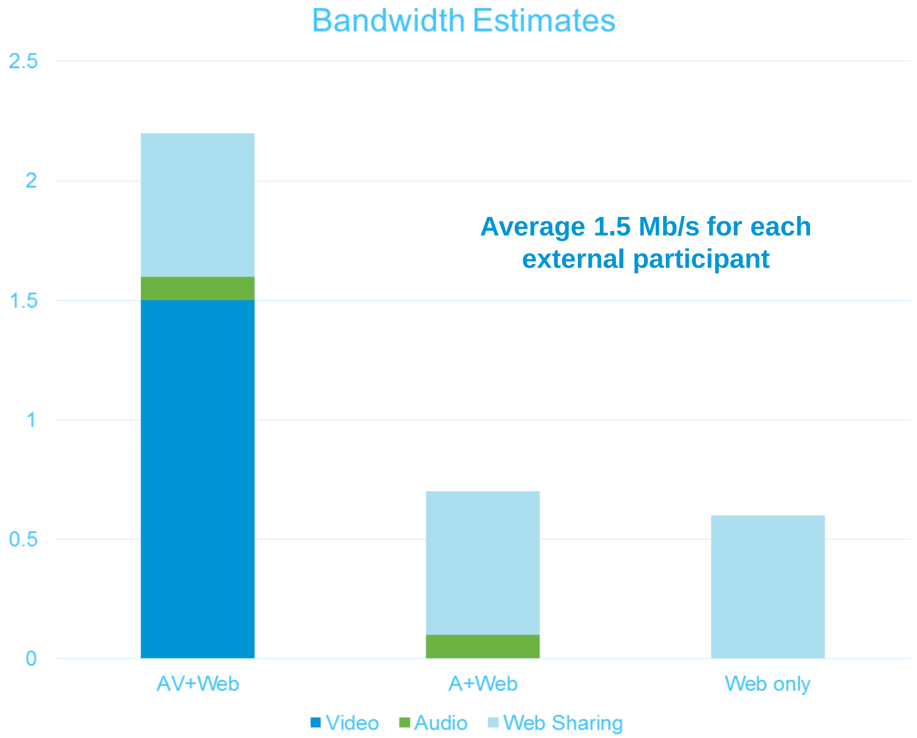
View More

Need Config changes:

- DNS
- Licensing
- SSL certificates (if DR hostnames different)
- CUCM
- SNMP
- SSO

Network Connectivity

- 2.2Mb/s Maximum; 1.5 Mb/s recommended
- If using non-split-horizon DNS all traffic will be sent to the IRP/DMZ
- Ensure there are enough inbound trunks for all external participants to dial in.



Bandwidth reference document:

http://www.cisco.com/en/US/prod/collateral/ps10352/ps10362/ps10409/white_paper_c11-691351.pdf

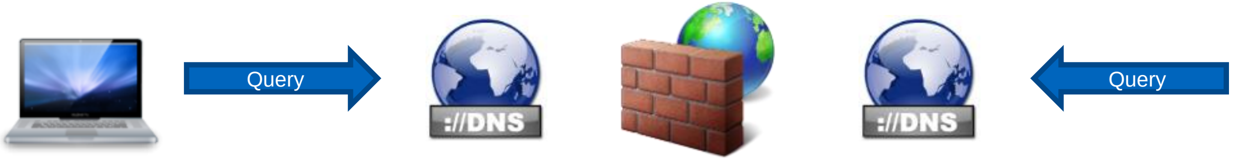
Understanding DNS – Split Horizon

*"In computer networking, **split-horizon DNS**, **split-view DNS**, or **split DNS** is the facility of a Domain Name System (DNS) implementation to provide different sets of DNS information, selected by, usually, the source address of the DNS request.*

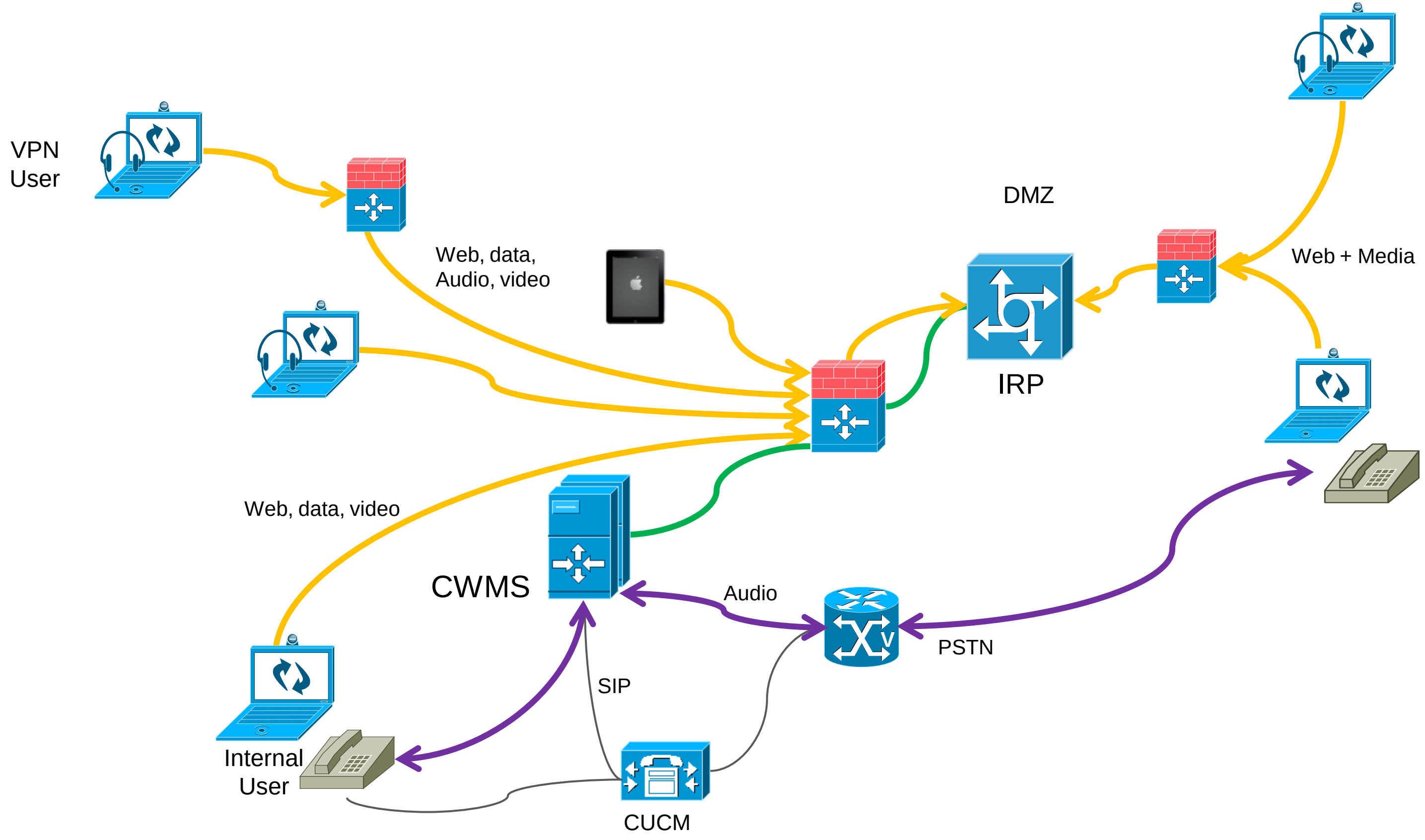
Implementation of split-horizon DNS can be accomplished by running distinct DNS server devices for the desired access granularity within the networks involved."

Name	IP Address
CWMS.acme.com.au	10.20.30.40

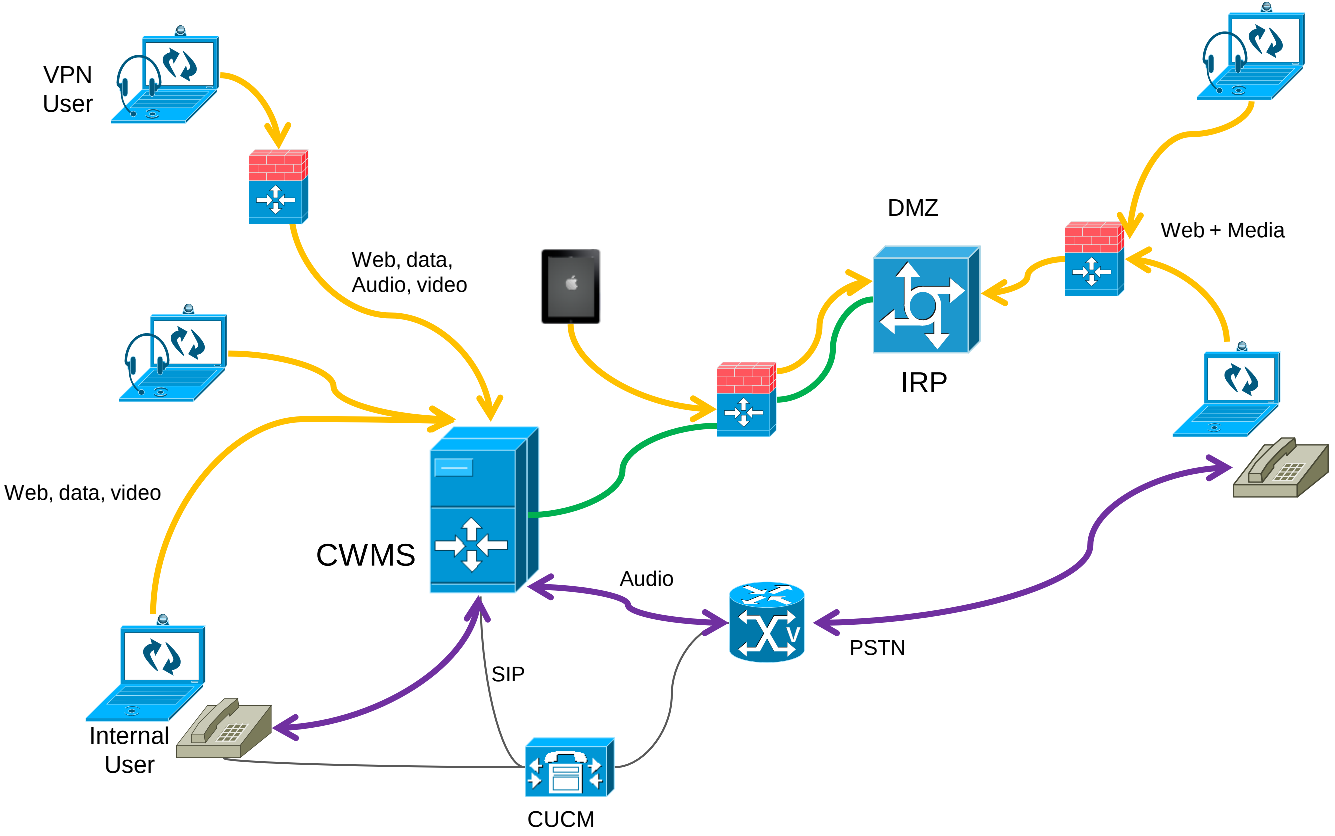
Name	IP Address
CWMS.acme.com.au	64.104.200.40



Non-Split Horizon CWMS DNS Model



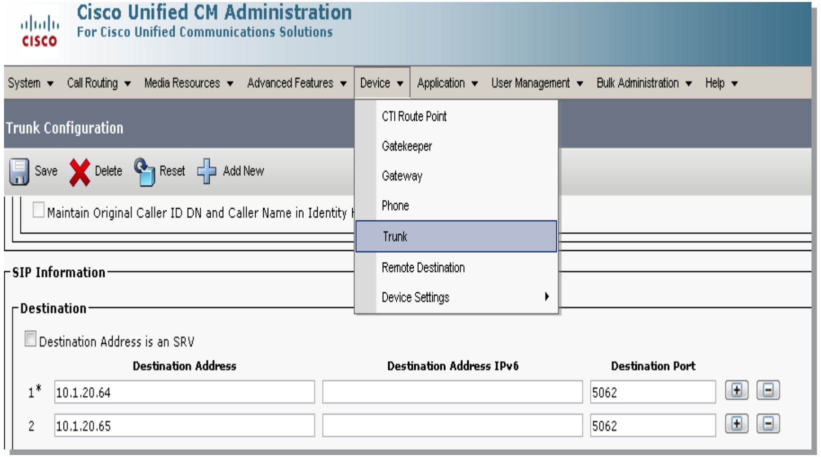
Split-Horizon CWMS DNS Model



CUCM Integration

- Call-back Teleconferencing
  - Join Web session first, then use Callback
  - Controlled via SIP trunk to CUCM /SME
  - Can be disabled

- Dial In Operations
  - SIP Trunks
  - Usually deployed with 3 phone numbers: **toll free**, **toll** and **internal dial** numbers pointed to SIP trunks inbound to CWMS
  - Uses SIP Refer to provide load balancing across redundant systems



Trunk Configuration

☐ Maintain Original Caller ID DN and Caller Name in Identity

SIP Information

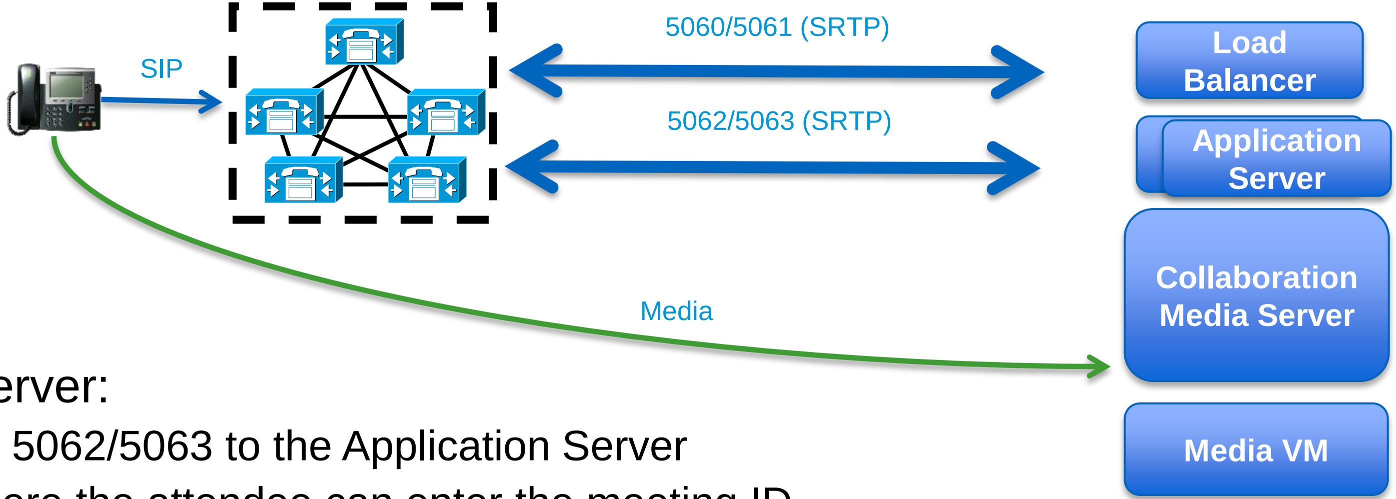
Destination

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.1.20.64		5062
2	10.1.20.65		5062

SIP Trunks CWMS

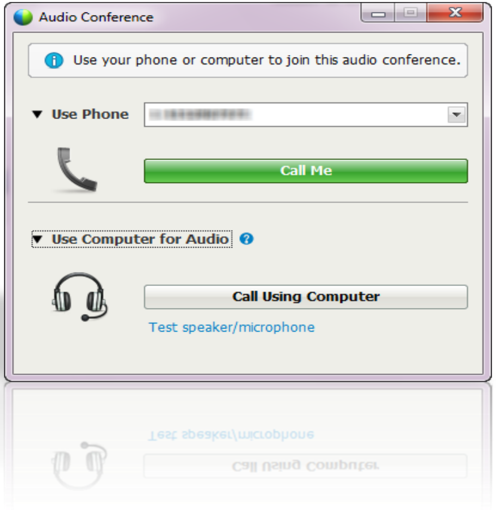
Load Balancing



- Load Balancer Server:
  - Redirects on port 5062/5063 to the Application Server
  - (IVR function) where the attendee can enter the meeting ID
  - Call-in from CUCM to CWMS via the associated access number (ex:3116)

Audio Parameters

- G.711-G722-G729 no capacity loss
- No echo cancellation built into CWMS
  - ISR Voice Gateway use DSP Echo Cancellation modules
  - CUBE can also be used for Echo cancellation
- SIP QoS Audio – Call-back
- CWMS has TLS/SRTP audio encryption available



Audio Conference

Use your phone or computer to join this audio conference.

▼ Use Phone [redacted]

Call Me

▼ Use Computer for Audio

Call Using Computer

Test speaker/microphone

CWMS Single Sign On

- Users do not need to remember WebEx usernames or password
- No user passwords are stored
- Requires an Identity and Access Management (IAM) system that conforms to Security Assertion Markup Language (SAML) 2.0
- Customers use native ‘Attribute/Group’ filtering capabilities found in the IDMS to allow groups of users access permissions
- WebEx Server Internet Reverse Proxy (IRP) allows authentication through firewall as long as IAM will allow authentication from outside firewall.
- X.509 Security Certificate uploaded into WebEx Server

External Storage Sizing

- Recording
  - 50 to 100 MB (if using video at 180 p) per hour *
  - No automated process to delete them
  - If deleted from CWMS, recording remains in the storage server for 6 additional months
- Backup
  - NFS also used to store system backup (~400MB) when deploying a cold stand by system in second DC

* More details in the bandwidth white paper

http://www.cisco.com/en/US/prod/collateral/ps10352/ps10362/ps10409/white_paper_c11-691351.pdf

WebEx Meetings Server

Deployment & Upgrades

General Requirements

Category	System Requirements
UCS	• UCS only - Support for 3rd party servers planned • No Co-Residency - vCentre can be co-resident in certain deployment types
VMware	• VMware 5.0 and 5.1 • vSphere 5.0 or 5.1 Standard for lower scale deployments (50-250 ports) • vSphere 5.0 Enterprise Plus or 5.1 Enterprise for higher scale deployments(800-2000 ports) • vCentre mandatory • One VMware License per processor socket
Networking	• LAN • DNS must be configured prior to deployment • NTP required on ESXi Host • Redundant configurations must have all NIC interfaces duplicated and connected to independent switching fabric to support LAN Fault tolerance • WAN • Similar to SaaS WebEx for HQ Video, Web Share etc. • Plan assuming 80-20 distribution in-company users (LAN) and internet users (WAN)
Storage (NAS)	• External one needed only if customer wants to record meetings and keep system snapshots (for DR) • NAS and SAN supported for VMs on UCS
Teleconferencing	• CUCM 7.1, 8.6, 9.0 ,9.1 and 10 for SIP Trunk based Teleconferencing
SSO	• If using ADFS 2.0 as iDP then customer needs AD (Active Directory) 2008R2 • Other SAML 2.0 SSO Compliant iDP also supported – same as SaaS WebEx • PingFederation V6.5.2, ADFS V2, OpenAM V9.5.4

UCS Requirements

<table>
<tr><th colspan="5">50 Port
Example UCS Model: C220 M3 or B200 M3</th></tr>
<tr><td rowspan="2"><b>Admin</b>
• 4 cores (ESXi 5.0)
• 6 cores (ESXi 5.1)
• 24 GB RAM
• 2 NIC</td><td rowspan="2"><b>IRP</b>
• 4 cores (ESXi 5.0)
• 6 cores (ESXi 5.1)
• 20 GB RAM
• 2 NIC</td><th colspan="3">Co-Resident Configurations</th></tr>
<tr><td><b>Admin + vCentre</b>
• 8 cores (ESXi 5.0)
• 10 cores (ESXi 5.1)
• 36 GB RAM
• 2 NIC</td><td><b>Admin + IRP</b>
• 8 cores
• 36 GB RAM
• 2 NIC</td><td><b>Primary + IRP + vCentre</b>
• 12 cores
• 40 GB RAM
• 5 NIC</td></tr>
<tr><th colspan="5">250 Port
Example UCS Model: C240 M3 or B200 M3</th></tr>
<tr><td colspan="2" rowspan="2"><b>Admin &amp; Media</b>
• 12 Cores
• 52 GB RAM
• 2 NIC</td><td colspan="2" rowspan="2"><b>IRP</b>
• 12 Cores
• 36 GB RAM
• 2 NIC</td><th>Co-Resident Configuration</th></tr>
<tr><td><b>Admin &amp; Media + vCentre</b>
• 16 Cores
• 56 GB RAM
• 3 NIC</td></tr>
<tr><th colspan="5">800 or 2000 Port
Example UCS Model: C460 M2 or B440 M2</th></tr>
<tr><td colspan="3">Admin & Media
• 40 Cores
• 80 GB RAM
• 2 NIC</td><td colspan="2">IRP
• 40 Cores
• 36 GB RAM
• 2 NIC</td></tr>
</table>

Please refer to the CWMS System Requirements document for the most up to date requirements

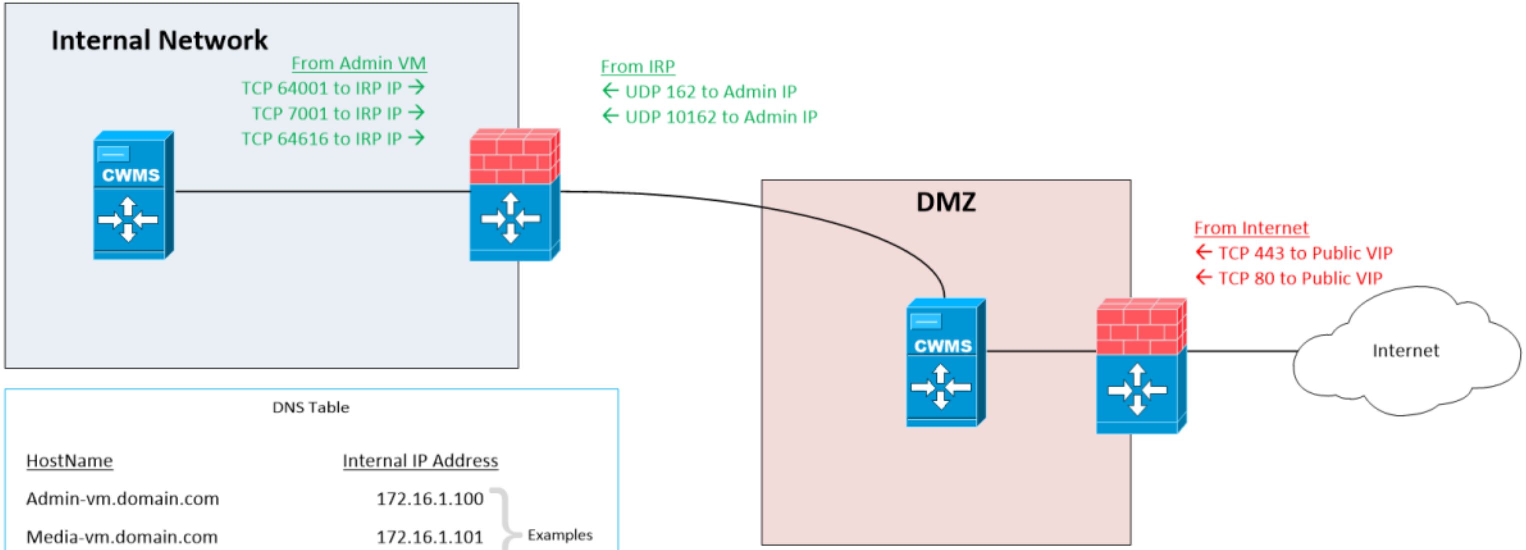
End User Requirements

Category	System Requirements
Web User Interface	Browsers • Internet Explorer 8 to 10 (32-bit/64-bit) ; IE 11 on Windows 7 SP1 only • Firefox 10 to 25 (Mac/Windows) • Safari 6 for Snow Leopard and Lion, Mountain Lion (Mac) • Chrome 23 through 31 (Mac/Windows)
Desktop Operating Systems	• Windows XP SP3 and later • Windows Vista (32-bit/64-bit) • Windows 7 (32-bit/64-bit) • **Windows 8** • Windows Server 2008 (64-bit) • Mac OS 10.6 Snow Leopard, 10.7 Lion, and 10.8 Mountain Lion
Productivity Tools	• Outlook 2007 SP2 and later • Outlook 2010 (32 and 64-bits, all service packs) • Outlook 2013 • OCS 2007 and 2007 R2 / Lync 2010 and 2013 • **Office 365**
Mobile Platform	• iOS v5.1 or later (iPhone and iPad) • **Android 2.1 and later**

Before You Start

- List of hostnames and IP addresses to use for the actual VMs
- Know how you want to place each VM on which blade
- Private VIP
- Public VIP if using a DMZ
- Extra DNS entry for admin URL
- Extra DNS entry for site URL (or 2 if using split horizon)
- Logon information for vCentre
- SMTP server for the new account emails
- Email address for the primary administrator

Network Port Requirements



DNS Table

HostName	Internal IP Address	
Admin-vm.domain.com	172.16.1.100	Examples
Media-vm.domain.com	172.16.1.101	
IRP-VM.domain.com	172.16.2.102	
User-Site.domain.com	Public VIP	
Admin-Site.domain.com	Private VIP	

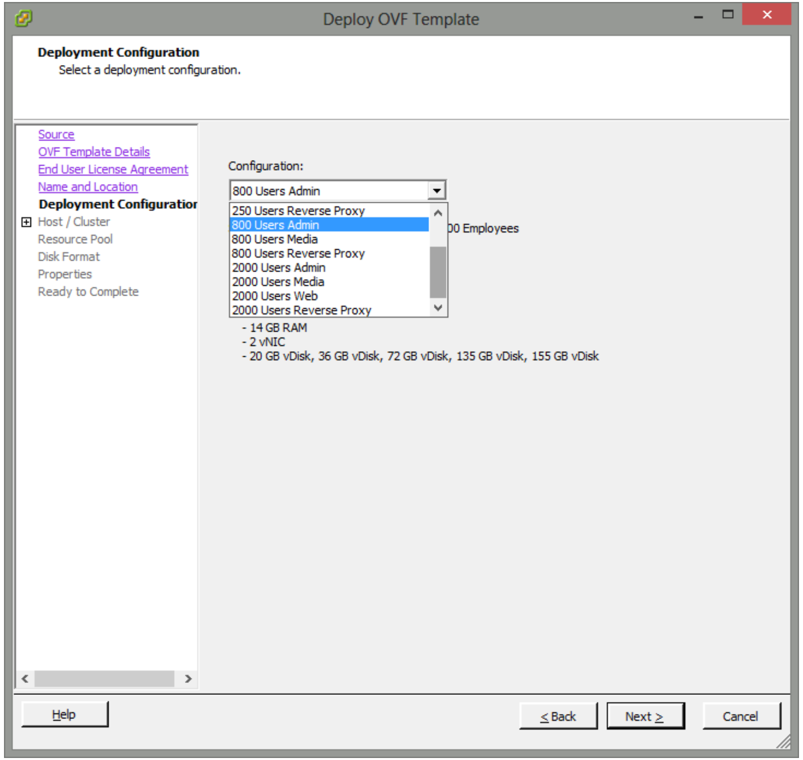
Notes:
Private VIP must be in the same subnet as Admin/Media VM
Public VIP must be in the same subnet as IRP VM

Internet Reverse Proxy (IRP) recommended in the DMZ

Ports 443 and 80 will need to be open inbound to the IRP.

Other ports (listed) will need to be open inbound from the IRP to CWMS and outbound from CWMS to the IRP.

Deploy OVA Steps



Deployment Configuration

Select a deployment configuration.

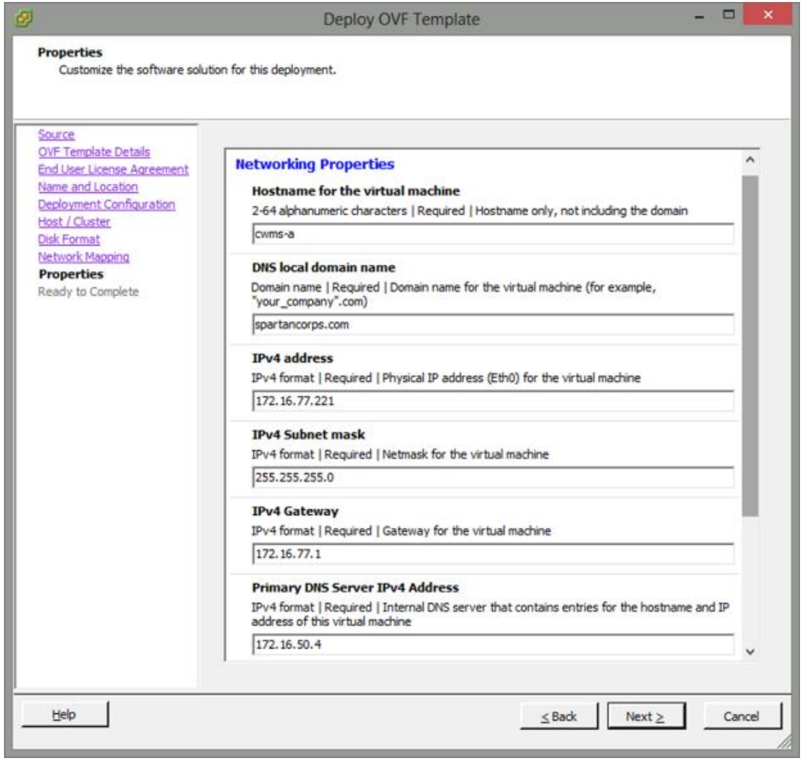
Configuration:

800 Users Admin

250 Users Reverse Proxy
800 Users Admin
800 Users Media
800 Users Reverse Proxy
2000 Users Admin
2000 Users Media
2000 Users Web
2000 Users Reverse Proxy

00 Employees

- 14 GB RAM
- 2 vNIC
- 20 GB vDisk, 36 GB vDisk, 72 GB vDisk, 135 GB vDisk, 155 GB vDisk



Properties

Customize the software solution for this deployment.

Networking Properties

Hostname for the virtual machine
2-64 alphanumeric characters | Required | Hostname only, not including the domain
cwms-a

DNS local domain name
Domain name | Required | Domain name for the virtual machine (for example, "your_company".com)
spartancorps.com

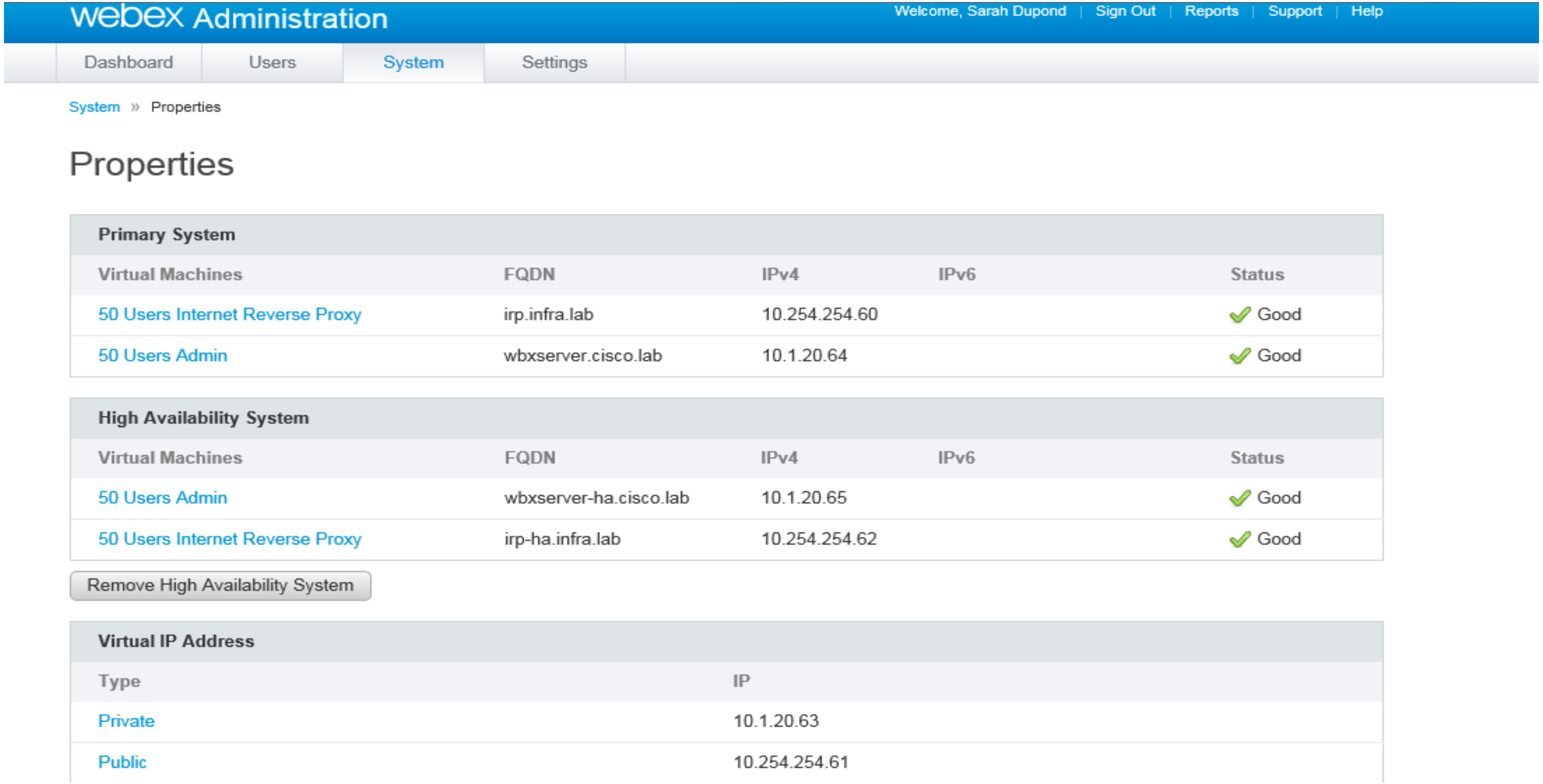
IPv4 address
IPv4 format | Required | Physical IP address (Eth0) for the virtual machine
172.16.77.221

IPv4 Subnet mask
IPv4 format | Required | Netmask for the virtual machine
255.255.255.0

IPv4 Gateway
IPv4 format | Required | Gateway for the virtual machine
172.16.77.1

Primary DNS Server IPv4 Address
IPv4 format | Required | Internal DNS server that contains entries for the hostname and IP address of this virtual machine
172.16.50.4

System deployed with HA and IRP



webex Administration
Welcome, Sarah Dupond | Sign Out | Reports | Support | Help
Dashboard
Users
System
Settings
System » Properties

Properties

Primary System

Virtual Machines	FQDN	IPv4	IPv6	Status
50 Users Internet Reverse Proxy	irp.infra.lab	10.254.254.60		✓ Good
50 Users Admin	wbxserver.cisco.lab	10.1.20.64		✓ Good

High Availability System

Virtual Machines	FQDN	IPv4	IPv6	Status
50 Users Admin	wbxserver-ha.cisco.lab	10.1.20.65		✓ Good
50 Users Internet Reverse Proxy	irp-ha.infra.lab	10.254.254.62		✓ Good

Remove High Availability System

Virtual IP Address

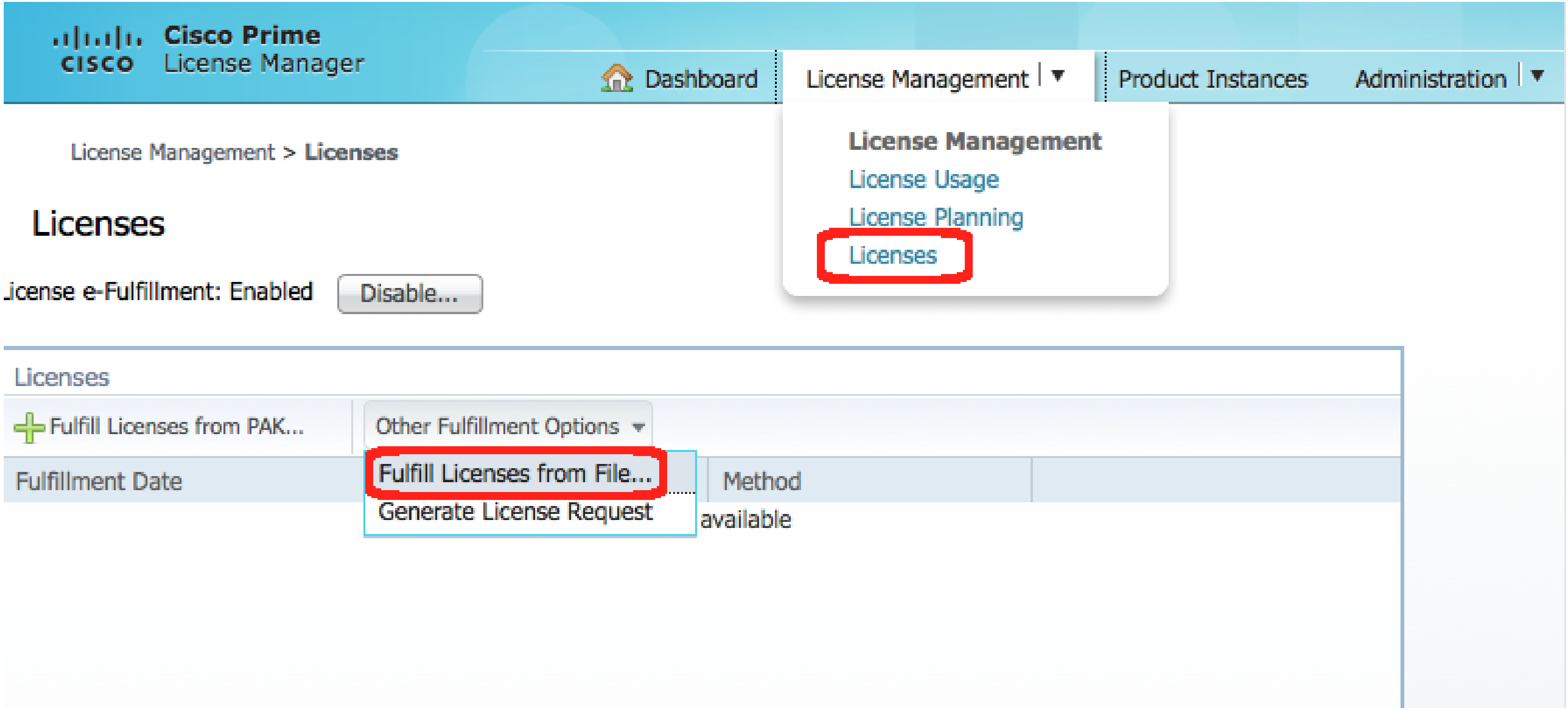
Type	IP
Private	10.1.20.63
Public	10.254.254.61

https://communities.cisco.com/docs/DOC-30980

Licensing in the CWMS 2.0 system

- CWMS 2.0 integrates the latest release of Cisco Prime License Manager (PLM)
- PLM supports two methods of license fulfillment
  1. File-based fulfillment, as available in previous releases of CWMS
  2. e-fufillment, which allows a customer to fulfill licenses through the license manager interface using a Product Authorisation Key (PAK) and their CEC account
- New license manager user experience is different
- Upgraded system requires a new set of licenses since new VMs are created

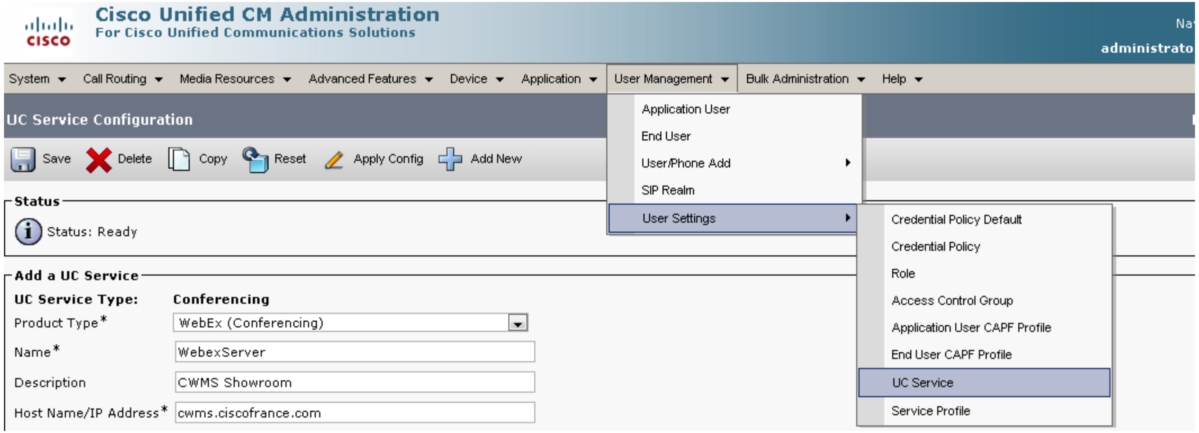
Licensing Screenshot



License e-Fulfillment: Enabled

Cisco Jabber integration

- For Cisco Unified Presence (CUP) 8.6 and lower in application-Cisco Jabber-Conferencing server
- From CUCM 9 in user settings-UC service
- Then assign profile to users



Status

Status: Ready

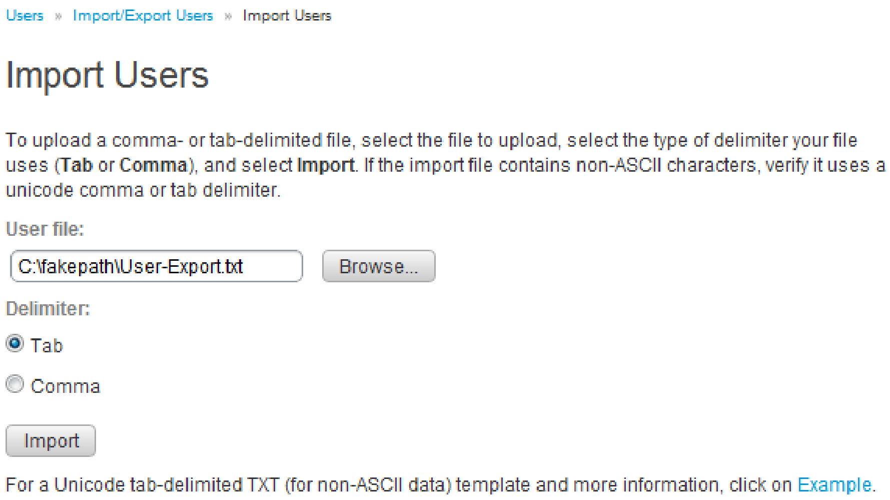
Add a UC Service

UC Service Type: Conferencing

Product Type*	WebEx (Conferencing)
Name*	WebexServer
Description	CWMS Showroom
Host Name/IP Address*	cwms.ciscofrance.com

Managing Users Profiles

- Manually by the administrator
- Bulk import based upon .CSV/.TXT
- LDAP integration via CUCM
- Federated SSO (Automated
  - SAML 2.0 SSO End User Authentication
  - Auto-Create Profile (Option)



Users » Import/Export Users » Import Users

Import Users

To upload a comma- or tab-delimited file, select the file to upload, select the type of delimiter your file uses (**Tab** or **Comma**), and select **Import**. If the import file contains non-ASCII characters, verify it uses a unicode comma or tab delimiter.

User file: C:\fakepath\User-Export.txt

Delimiter:

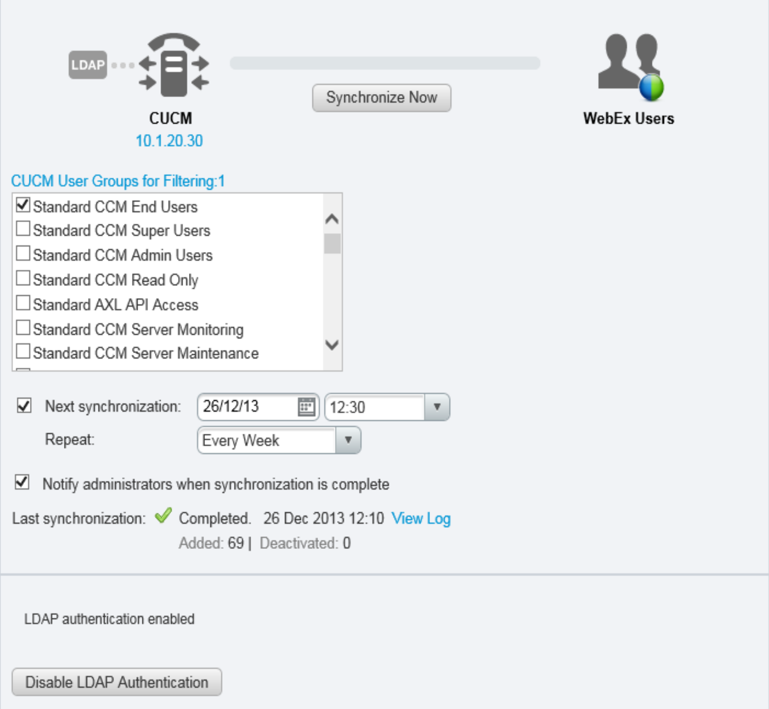
● Tab

○ Comma

For a Unicode tab-delimited TXT (for non-ASCII data) template and more information, click on Example.

Directory Integration via CUCM

- Set up LDAP Integration in 4 easy steps
  - Set up CUCM
  - Perform Directory Sync
  - Turn on LDAP Authentication (Optional)
  - Notify Users (Optional)
- Secure (SOAP over HTTPS)
- Filters based on CUCM user groups



CUCM User Groups for Filtering:1

☑ Standard CCM End Users
☐ Standard CCM Super Users
☐ Standard CCM Admin Users
☐ Standard CCM Read Only
☐ Standard AXL API Access
☐ Standard CCM Server Monitoring
☐ Standard CCM Server Maintenance

☑ Next synchronization: 26/12/13 12:30

Repeat: Every Week

☑ Notify administrators when synchronization is complete

Last synchronization: ✓ Completed. 26 Dec 2013 12:10 View Log

Added: 69 | Deactivated: 0

LDAP authentication enabled

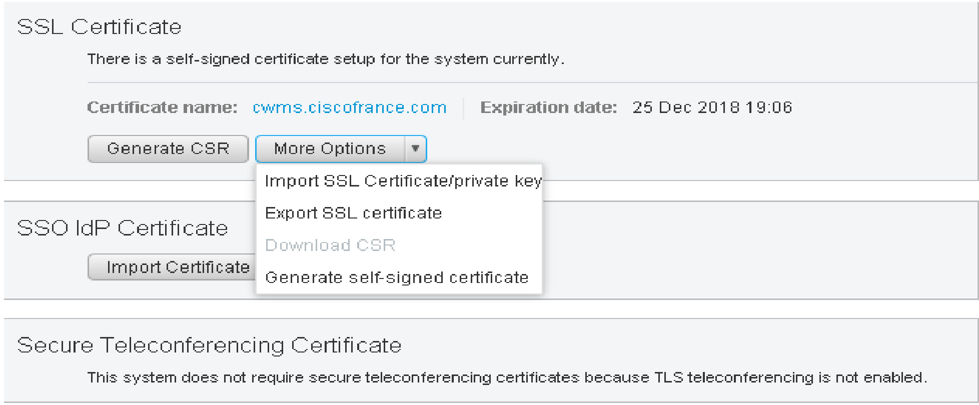
Managing certificates

Wildcard (valid for all hosts in the domain) or SAN certificates (all hosts listed except IRP)

Invalid after expansion-upgrade-HA

CWMS can generate self-signed one

(also after restore, expansion…)



SSL Certificate

There is a self-signed certificate setup for the system currently.

Certificate name: cwms.ciscofrance.com | Expiration date: 25 Dec 2018 19:06

Secure Teleconferencing Certificate

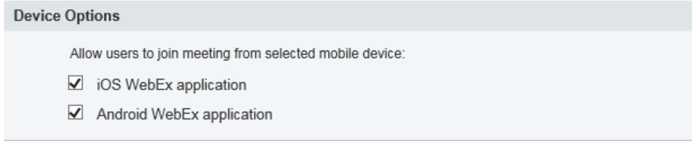
This system does not require secure teleconferencing certificates because TLS teleconferencing is not enabled.

X509 format only, can be encoded as

- -DER (only to upload one certificate)
- -PEM : to upload certificate chains or certificate + private key
- -PKCS#12: same as PEM , must be password protected (.p12 or .pfx)

Managing the system

Mobility



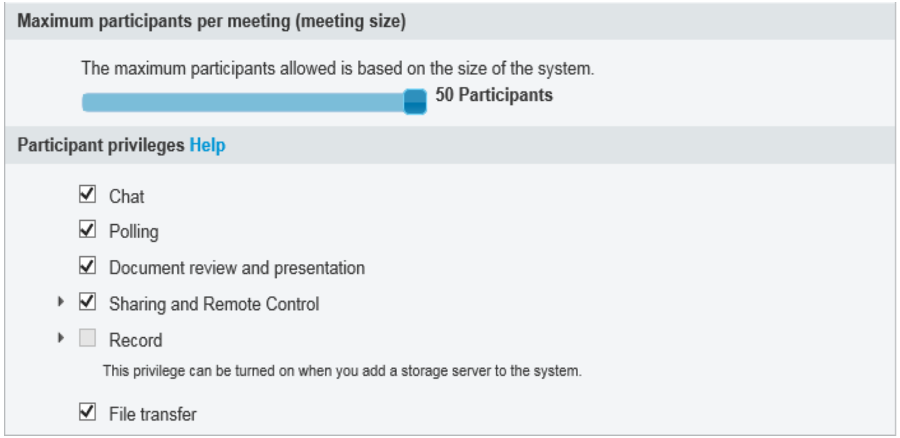
Device Options

Allow users to join meeting from selected mobile device:

☑ iOS WebEx application

☑ Android WebEx application

Meetings size and privileges



Maximum participants per meeting (meeting size)

The maximum participants allowed is based on the size of the system.

50 Participants

Participant privileges Help

☑ Chat

☑ Polling

☑ Document review and presentation

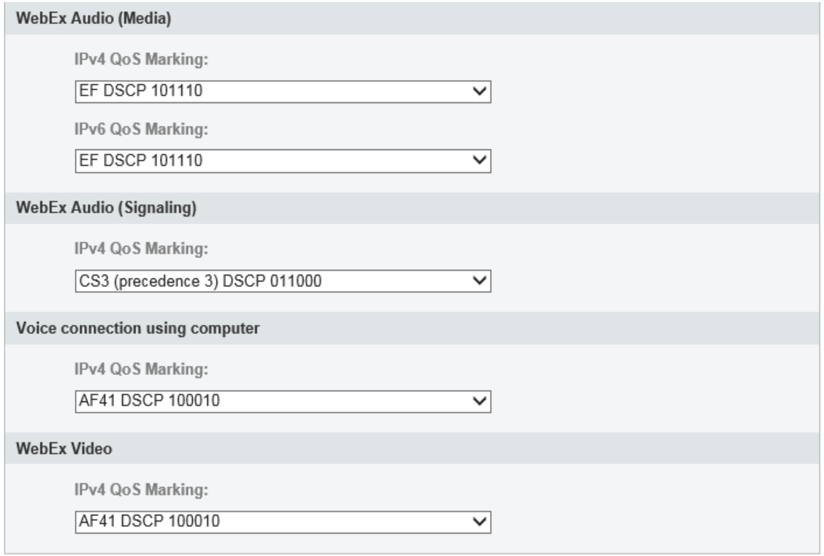
☑ Sharing and Remote Control

□ Record

This privilege can be turned on when you add a storage server to the system.

☑ File transfer

Quality of service



WebEx Audio (Media)

IPv4 QoS Marking: EF DSCP 101110

IPv6 QoS Marking: EF DSCP 101110

WebEx Audio (Signaling)

IPv4 QoS Marking: CS3 (precedence 3) DSCP 011000

Voice connection using computer

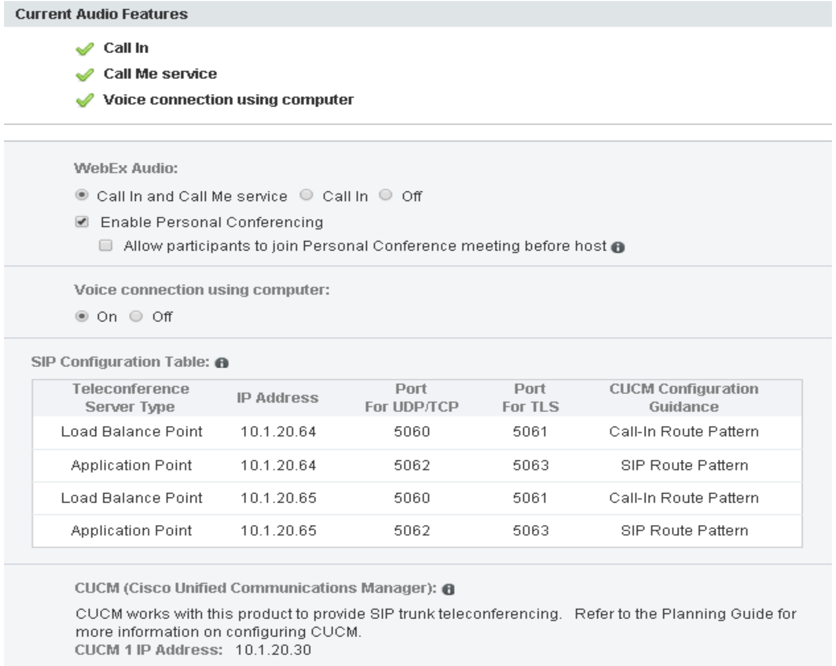
IPv4 QoS Marking: AF41 DSCP 100010

WebEx Video

IPv4 QoS Marking: AF41 DSCP 100010

Audio configuration

- Global settings for call-in, call back, VoIP and PCN



Current Audio Features

✓ Call In
✓ Call Me service
✓ Voice connection using computer

WebEx Audio:

● Call In and Call Me service ○ Call In ○ Off

☑ Enable Personal Conferencing

□ Allow participants to join Personal Conference meeting before host

Voice connection using computer:

● On ○ Off

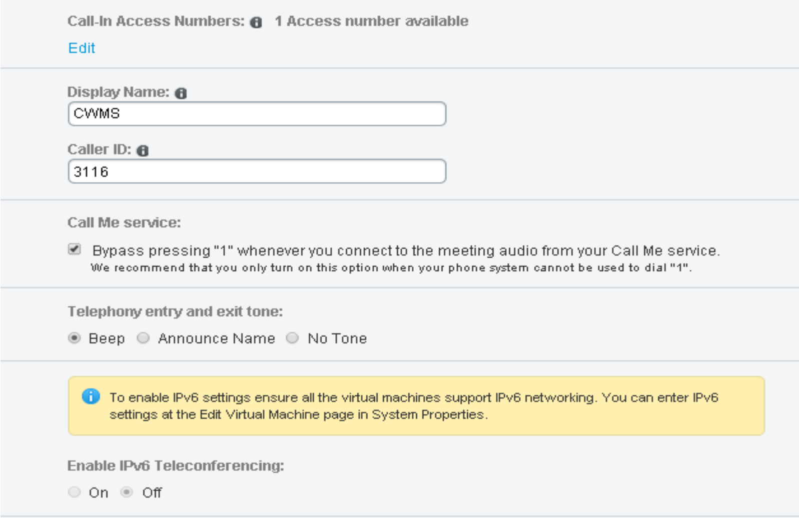
SIP Configuration Table:

Teleconference Server Type	IP Address	Port For UDP/TCP	Port For TLS	CUCM Configuration Guidance
Load Balance Point	10.1.20.64	5060	5061	Call-In Route Pattern
Application Point	10.1.20.64	5062	5063	SIP Route Pattern
Load Balance Point	10.1.20.65	5060	5061	Call-In Route Pattern
Application Point	10.1.20.65	5062	5063	SIP Route Pattern

CUCM (Cisco Unified Communications Manager):

CUCM works with this product to provide SIP trunk teleconferencing. Refer to the Planning Guide for more information on configuring CUCM.
CUCM 1 IP Address: 10.1.20.30

- Call-in numbers set at CUCM level
- Display name : on user IP phones when called back



Call-In Access Numbers: 1 Access number available
Edit

Display Name: CWMS

Caller ID: 3116

Call Me service:

☑ Bypass pressing "1" whenever you connect to the meeting audio from your Call Me service.
We recommend that you only turn on this option when your phone system cannot be used to dial "1".

Telephony entry and exit tone:

● Beep ○ Announce Name ○ No Tone

To enable IPv6 settings ensure all the virtual machines support IPv6 networking. You can enter IPv6 settings at the Edit Virtual Machine page in System Properties.

Enable IPv6 Teleconferencing:

○ On ● Off

Upgrading to 2.0

Customers who wish to upgrade their CWMS 1.x systems to the latest version, CWMS 2.0, must do so using the replacement upgrade procedure.

Two upgrade methods are available:

- **Automatic upgrade**
  - The preferred upgrade method
  - Requires vCentre credentials (with required privileges to create/modify VMs)
  - Automatically creates VMs (including IRP and HA VMs) needed for the new system
  - Automatically transfers data from the old to the new system
- **Manual upgrade**
  - Must be used if vCentre credentials cannot be provided
  - Very similar to CWMS 1.0/1.1/1.5 system expand procedure

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com cisco™

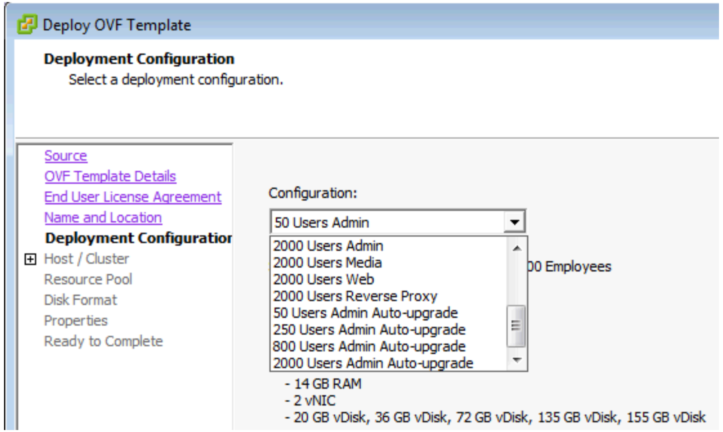
Appendix

Features Comparison

Category	MeetingPlace 8.6	Cisco WebEx Meetings Server	WebEx SaaS
Scalability	• Scale up to 14,400 total concurrent users • max 500 audio users per meeting. • HA solutions including multinode	• Scale up to 2,000 total concurrent users • max 250 audio/web users per meeting • HA solution (within a Data Centre)	• no limit on total concurrent users • max 500 web, 1,000 audio users per meeting • Global high availability cloud
Audio conferencing features	• IP Telephony • Personal/Reservationless • blast dial, continuous mtgs, vanity number, helpdesk	• Integrated VoIP & telephony • Personal conferencing	• Integrated VoIP & telephony • Personal conferencing
Languages and prompts	• Localise in 13+ languages • IVR language selection available • Prompt customisation available	• Localise in 13 languages • One IVR language per system	• Localise in 13 languages • One IVR language per access num
Video and TelePresence	• WebEx client/webcam video • SIP, H.323, and SCCP endpoints	• WebEx client/webcam video	• WebEx client/webcam video • WebEx Enabled TelePresence
Clients, Tools, and Mobility	• Only when combined with WebEx SaaS	• Desktop Clients for win/mac • Mobile clients for Apple, Android • Outlook PT for Windows;	• Desktop Clients for win/mac/linux • Mobile clients for Apple, Android, Blackberry, Windows Mobile • Outlook PT for Windows, Outlook PT for Mac (wx11), Lotus Notes PT for Windows (classic)
Security features	• LDAP<-->CUCM<-->MP • Federated SSO • JITC Certification (8.5) • Meetings option to allow only authenticated users	• LDAP<-->CUCM<-->CWMS • Federated SSO • JITC Certification (in progress) • Recordings/user data on prem	• Federated SSO • Meetings option to allow only authenticated users • Recordings/user data in cloud

Upgrading CWMS 1.x to 2.0

- Auto-upgrade VMs (HA-IRP if on original) to be created on same ESXi than primary admin VM
- Power up new 2.0 admin VM
- Use 1.x admin credentials and vCentre ones to deploy all VMs, automatic
- All original 1.x VMs then go down
- Copy archive data from source via VMDK
- Auto-upgrade admin VM will then use original admin hostname/IP
- Within 180 days, re-host and update your user licenses



Deploy OVF Template

Deployment Configuration

Select a deployment configuration.

Configuration:

50 Users Admin

2000 Users Admin
2000 Users Media
2000 Users Web
2000 Users Reverse Proxy
50 Users Admin Auto-upgrade
250 Users Admin Auto-upgrade
800 Users Admin Auto-upgrade
2000 Users Admin Auto-upgrade

00 Employees

- 14 GB RAM
- 2 vNIC
- 20 GB vDisk, 36 GB vDisk, 72 GB vDisk, 135 GB vDisk, 155 GB vDisk

Upgrading from 1.x to 2.0 requires 600 GB of free disk space on each ESXi host can be local (DAS) or external (SAN/NAS)

Automatic Upgrade Flow

The Automatic Upgrade process can be divided into different stages:

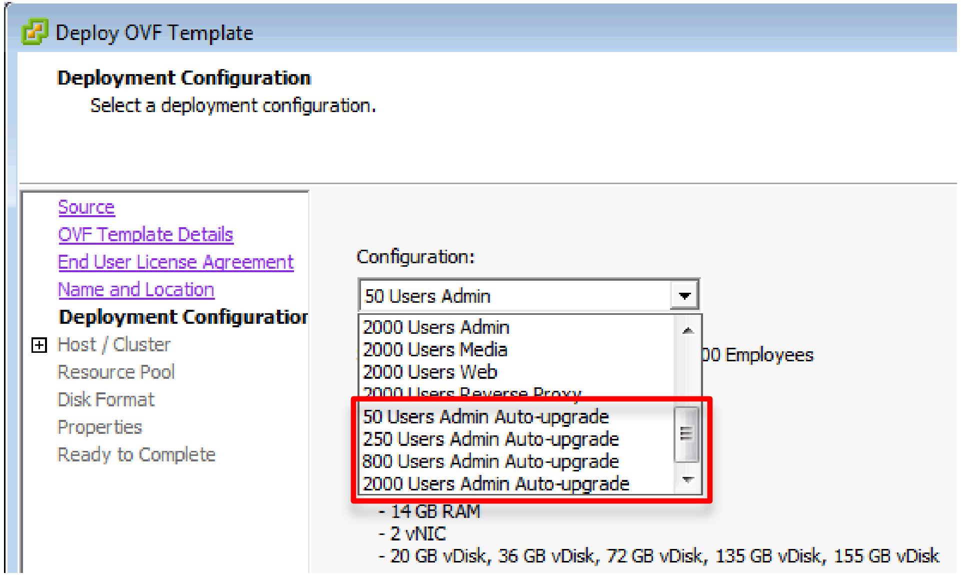
- Create the CWMS 2.0 auto-upgrade admin VM *
- Start the upgrade *
- New system setup **
- Finish the upgrade **
- Licensing in the CWMS 2.0 system
- Long pauses can exist be between 1 & 2 and 2 & 3

** Existing CWMS 1.x system remains in service*

*** Existing CWMS 1.x system not in service*

New VM Type for Auto-Upgrade

- Four new VM types defined
- Select the Auto-upgrade VM type that matches your existing system’s size



Deployment Configuration

Select a deployment configuration.

Configuration: 50 Users Admin

2000 Users Admin
2000 Users Media
2000 Users Web
2000 Users Reverse Proxy
50 Users Admin Auto-upgrade
250 Users Admin Auto-upgrade
800 Users Admin Auto-upgrade
2000 Users Admin Auto-upgrade

00 Employees

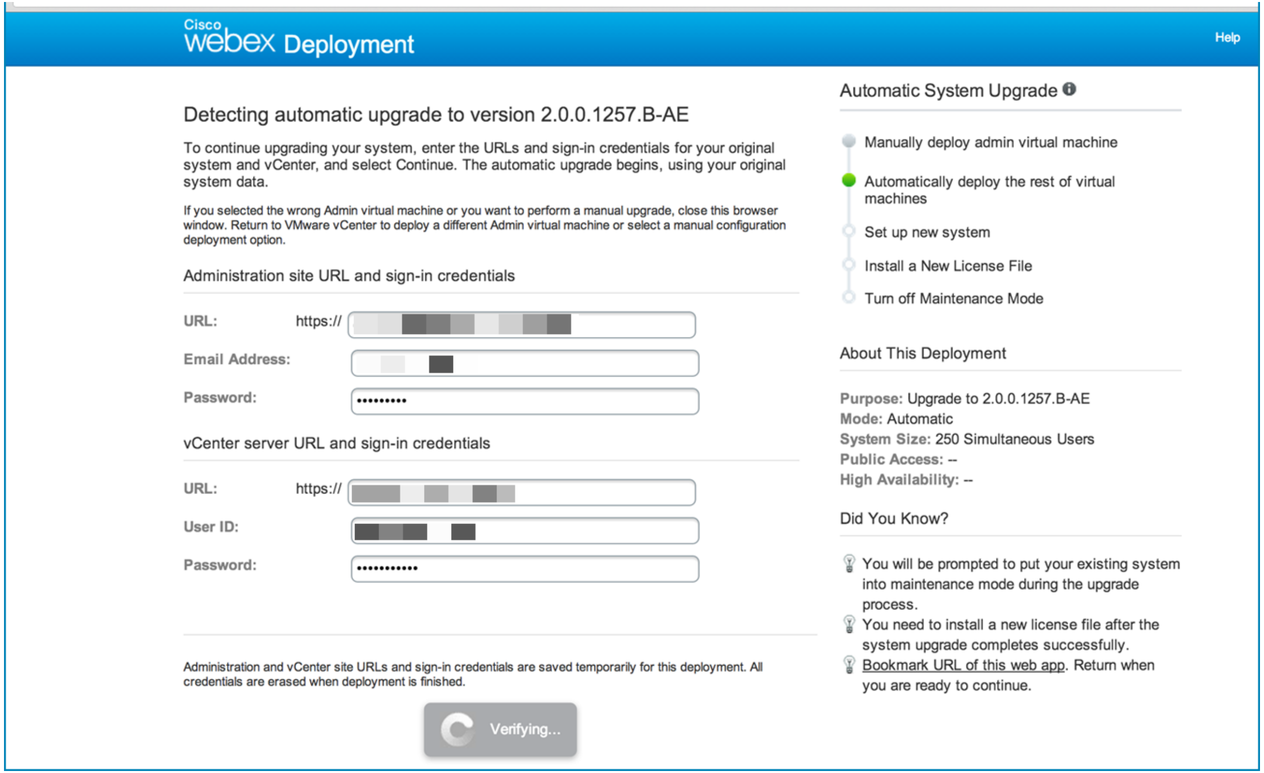
- 14 GB RAM
- 2 vNIC
- 20 GB vDisk, 36 GB vDisk, 72 GB vDisk, 135 GB vDisk, 155 GB vDisk

Create the CWMS 2.0 auto-upgrade admin VM

Overview and Steps

- No meeting service disruption during this operation
- Manually create the CWMS 2.0 auto upgrade admin VM **first** in vCentre using the 2.0 OVA
- Select from four new CWMS 2.0 auto-upgrade admin VM types
- VM is pre-configured to have zero CPU and memory reservations. Therefore, on some systems (e.g. a micro running on a 4-core blade) the upgrade may run slowly
- Must create it on the same ESXi host containing the primary admin VM of CWMS 1.x
- Requires a temporary IP/hostname for the VM on the same subnet as the primary admin VM of CWMS 1.x
- Power up the new 2.0 admin VM created earlier and open its console in vSphere Client

Start the upgrade - screenshot



Detecting automatic upgrade to version 2.0.0.1257.B-AE

To continue upgrading your system, enter the URLs and sign-in credentials for your original system and vCenter, and select Continue. The automatic upgrade begins, using your original system data.

If you selected the wrong Admin virtual machine or you want to perform a manual upgrade, close this browser window. Return to VMware vCenter to deploy a different Admin virtual machine or select a manual configuration deployment option.

Administration site URL and sign-in credentials

URL:	https:// [redacted]
Email Address:	[redacted]
Password:	•••••••••

vCenter server URL and sign-in credentials

URL:	https:// [redacted]
User ID:	[redacted]
Password:	•••••••••••

Administration and vCenter site URLs and sign-in credentials are saved temporarily for this deployment. All credentials are erased when deployment is finished.

Automatic System Upgrade

- ○ Manually deploy admin virtual machine
- ● Automatically deploy the rest of virtual machines
- ○ Set up new system
- ○ Install a New License File
- ○ Turn off Maintenance Mode

About This Deployment

Purpose: Upgrade to 2.0.0.1257.B-AE
Mode: Automatic
System Size: 250 Simultaneous Users
Public Access: --
High Availability: --

Did You Know?

- You will be prompted to put your existing system into maintenance mode during the upgrade process.
- You need to install a new license file after the system upgrade completes successfully.
- Bookmark URL of this web app. Return when you are ready to continue.

Start the upgrade

Browser Enhancements

- No meeting service disruption during this operation
- Upgrade process status not lost if browser session is closed
- Multiple system admins can simultaneously view the upgrade status
- Continuous progress update and remaining time estimate provided (browser and VM console)
- Estimated remaining time for backend operations
- Uses the CWMS 1.x admin credentials and vCentre privileged credentials to read 1.x system information, auto create VMs

Start the upgrade

Steps

- Type the Deployment URL displayed in the VM console into a web browser
- In the first page
  - Provide access information to the CWMS 1.x system
  - Provide access information to vCentre
- These are automatically reused at a later stage during the upgrade (refer screenshot)
- Click continue and the system auto-creates all the 2.0 VMs (including HA VMs, IRP VMs)
- Auto-created VMs remain powered down for now

New system setup

Overview

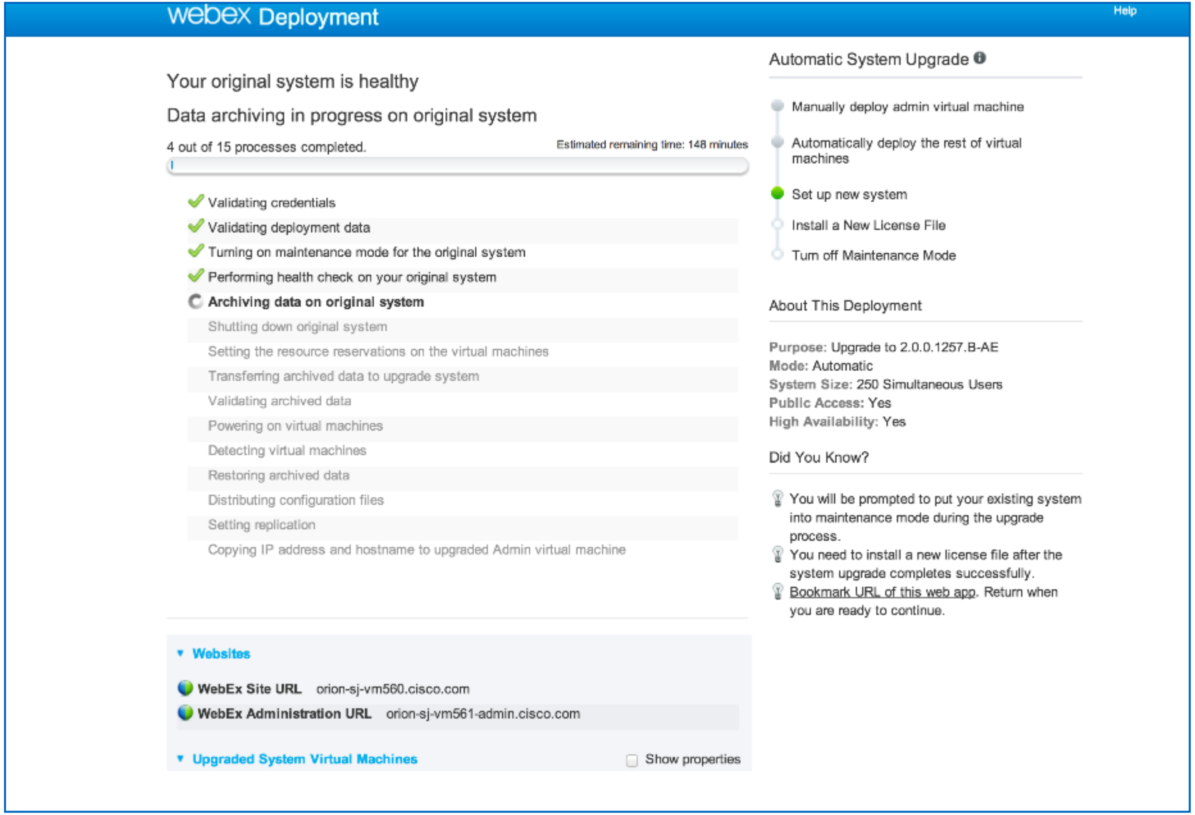
- Once the 2.0 VMs have all been auto-created successfully, user is asked to confirm proceeding to the next stage
- Upon confirmation, existing CWMS 1.x system will go down
- Continuous progress update and remaining time estimate provided (browser and VM console)

New System Setup

Steps (automatically performed)

- Put old system into Maintenance Mode
- Prepare old system for upgrade
- Power down old system
- Copy archive data from source system to the target system via VMDK
- Reset the 2.0 Admin VM’s CPU and memory reservations
- DB Operations
  - Restore the data transferred from the source system to the target system
  - Update the DB schema and data
  - In case the target system has HA, DB replication will be set up between the its primary and secondary admin VMs

New System Setup



Your original system is healthy

Data archiving in progress on original system

4 out of 15 processes completed. Estimated remaining time: 148 minutes

- ✓ Validating credentials
- ✓ Validating deployment data
- ✓ Turning on maintenance mode for the original system
- ✓ Performing health check on your original system
- **Archiving data on original system**
- Shutting down original system
- Setting the resource reservations on the virtual machines
- Transferring archived data to upgrade system
- Validating archived data
- Powering on virtual machines
- Detecting virtual machines
- Restoring archived data
- Distributing configuration files
- Setting replication
- Copying IP address and hostname to upgraded Admin virtual machine

▾ **Websites**

WebEx Site URL orion-sj-vm560.cisco.com

WebEx Administration URL orion-sj-vm561-admin.cisco.com

▾ **Upgraded System Virtual Machines** □ Show properties

Automatic System Upgrade

- ○ Manually deploy admin virtual machine
- ○ Automatically deploy the rest of virtual machines
- ● Set up new system
- ○ Install a New License File
- ○ Turn off Maintenance Mode

About This Deployment

Purpose: Upgrade to 2.0.0.1257.B-AE
Mode: Automatic
System Size: 250 Simultaneous Users
Public Access: Yes
High Availability: Yes

Did You Know?

- You will be prompted to put your existing system into maintenance mode during the upgrade process.
- You need to install a new license file after the system upgrade completes successfully.
- Bookmark URL of this web app. Return when you are ready to continue.

Finish the upgrade

- Congratulations on the upgrade!
- Click the “Sign-In” button to go to CWMS 2.0 administration URL
- Sign in with the same admin credentials as the 1.x system
- The 2.0 system will be in maintenance mode
- Take it out of maintenance mode when ready to use the system
- When you exit maintenance mode (causes a reboot)
  - The temporary IP bound to eth0 is released
  - The auto-upgrade admin VM is changed to use the original system’s primary admin hostname / IP

cisco™