

What You Make Possible



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

BRKCOL-2025

Agenda

- Introduction
- WebEx Cloud
- WebEx On-Premise
 - Designing
 - Integration
- Resources
- Appendix



Introduction



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 vs WebEx On-Premise

WebEx Cloud

Enterprise Edition – Meetings, Trainings, Events, Support

Broad range of 3rd party Plug-Ins

Extensive Customisability

Unlimited Scalability

Subscription Model

Global Platform

WebEx On-Premise

Meeting Centre

Outlook Calendaring Plug-In

Limited Customisability
(Logo, PS, TOS, Legal Disclaimer)

2,000 Peak Attendees (Ports)

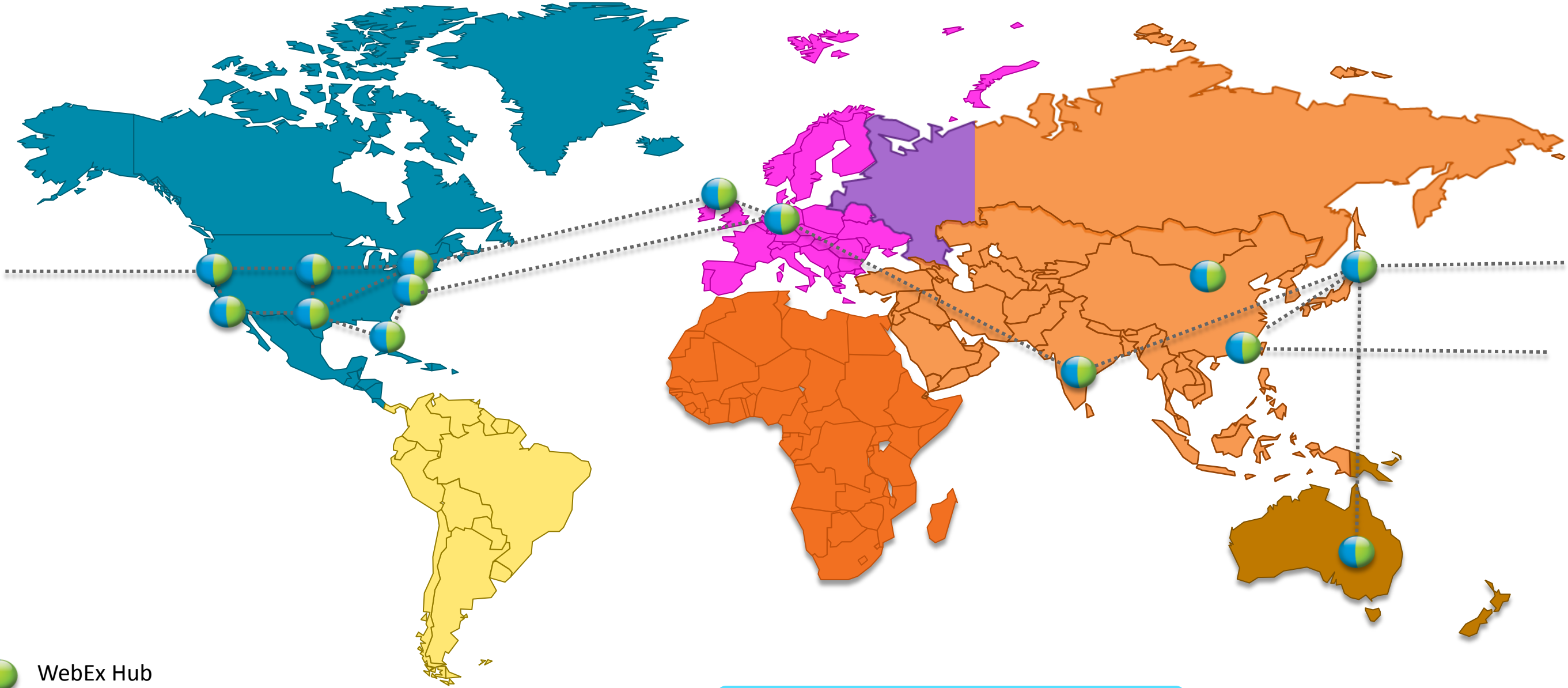
Perpetual User Licenses

Localised instances

WebEx Cloud



Cisco Collaboration Cloud



16 global collaboration hubs

Managing Users - Identities in WebEx

There are five options:

- Manually create users
- Self Registration
- Federated Single Sign On
- Bulk import based upon .CSV
- Automated Bulk Import (API)

[Home](#)

Manage Site
[Site Settings](#)
[Tracking Codes](#)
[Company Addresses](#)
[Email Templates](#)
[Meetings in Progress](#)

Manage Users
[Add User](#)
[Edit User List](#)
[Import/Export Users](#)
[Edit Privileges](#)
[Send Email to All](#)

Session Types
[Add Custom Type](#)

Batch Import Users

To upload a comma- or tab-delimited file, select the file to upload, select the type of delimiter your file uses. If your file contains non-ASCII characters, verify it uses a Unicode comma or tab delimiter.

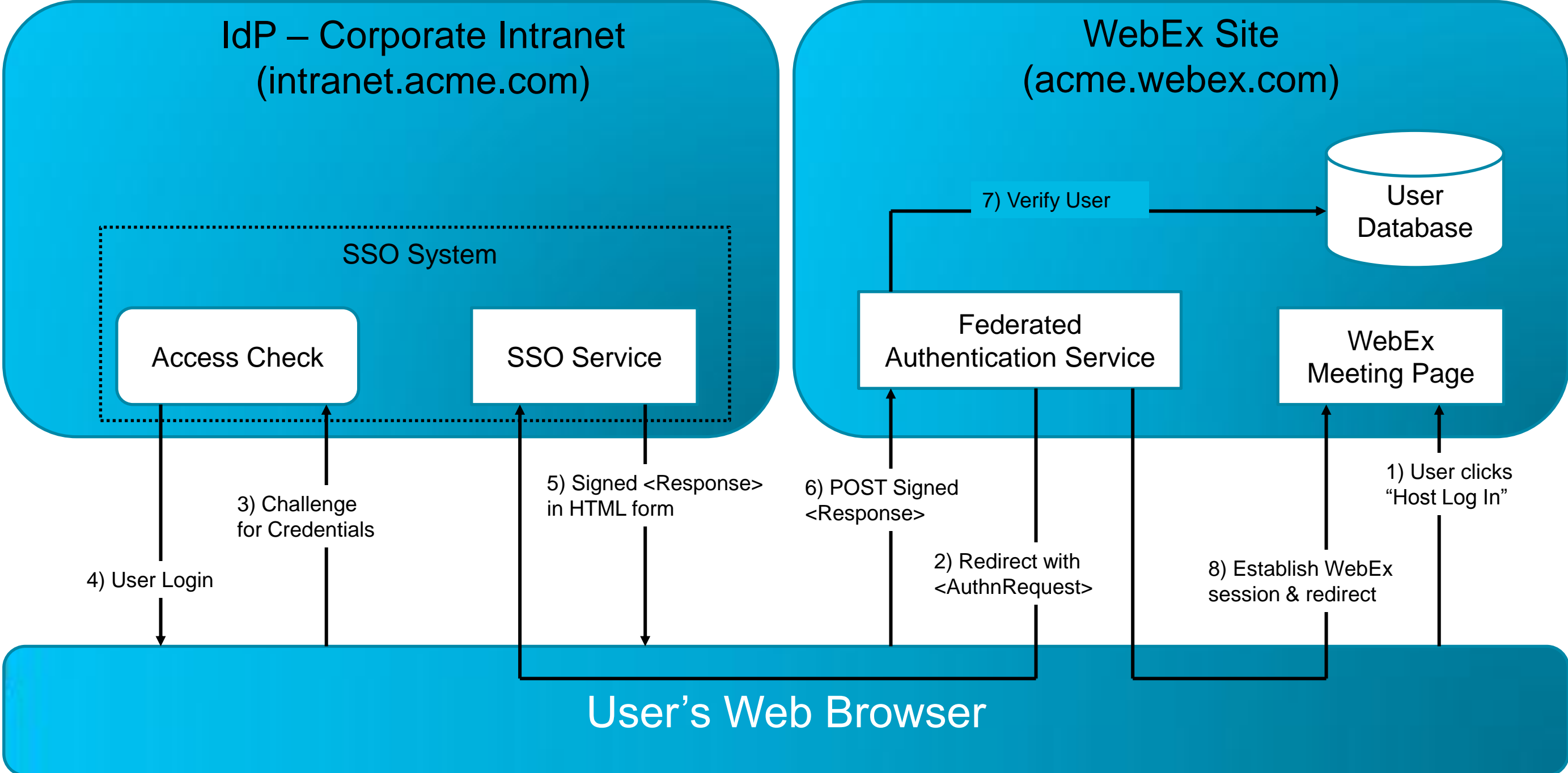
File name: No file chosen

Delimiter: Tab Comma

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



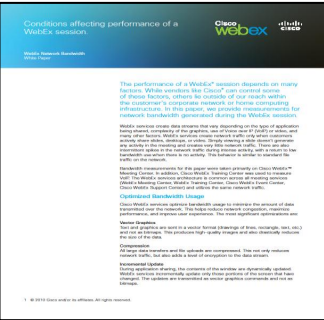
Managing Users - Federated SSO



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 than 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



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

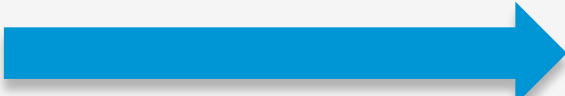
Turn on high-quality video (360p)

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



Managing Video – User Level Control

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



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

Navigation menu:

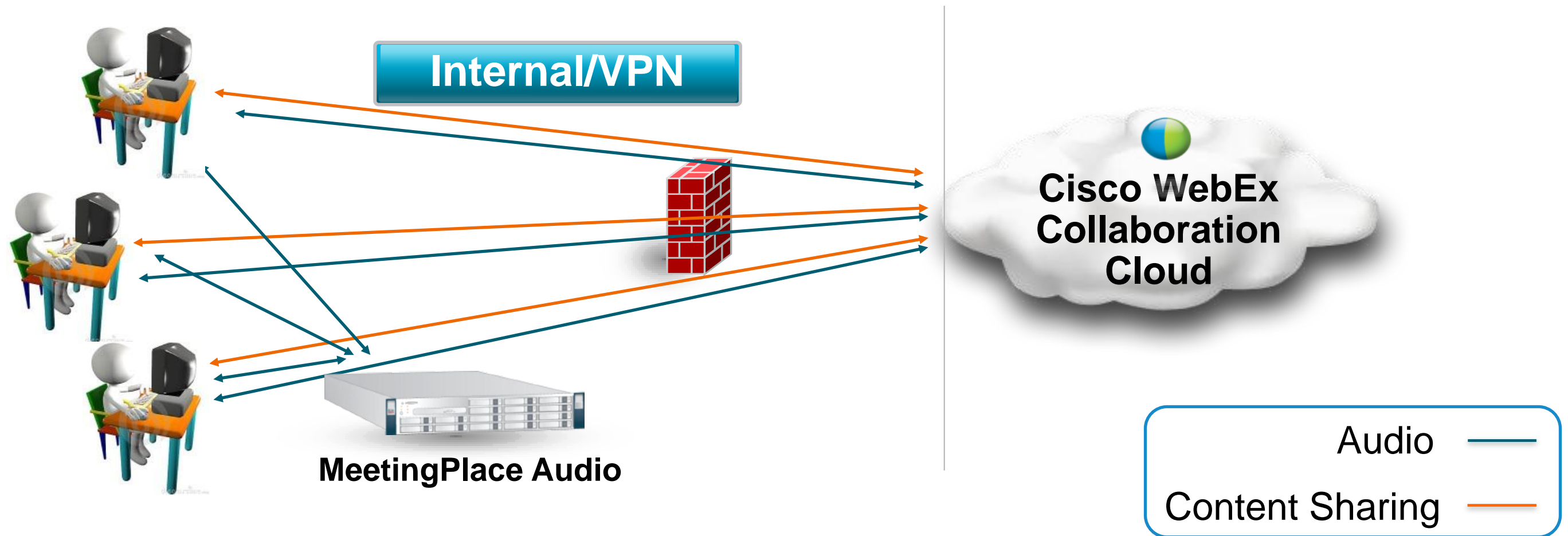
- Required Information
- Date & Time
- Audio Conference
- Invite Attendees
- Registration
- Agenda & Welcome
- Meeting Options**
- Attendee Privileges
- Review

* Enable these options during the scheduling process



Audio – Introducing Meeting Place

- Audio users connect to internal Meeting Place
- Data Sharing & Video is directed to WebEx Cloud



Audio - Meeting Place Configuration

The screenshot shows the Cisco WebEx Site Configuration page. A red oval highlights the configuration fields for the site name, administration user, and password. Another red oval highlights the 'Access Information' table below.

Cisco WebEx Site Configuration

Cisco WebEx configuration is successfully updated.

Cisco WebEx Site Configuration

Cisco WebEx site name * australia

Cisco WebEx site administration user * dhenwood

Cisco WebEx site administration password *

Cisco WebEx site administration password confirm *

Permit attendees to outdial from WebEx meeting Yes

Permit attendees to outdial internationally from WebEx meeting Yes

Permit users to host MeetingPlace reservationless audio meetings Yes

Proxy configuration required No

TSP primary host 64.68.120.146

TSP secondary host 173.243.0.132

Cisco WebEx adapter status Running

Access Information

Details	Label	Phone Number
<input type="checkbox"/> Edit	Sydney Node	61-2-99990000
<input type="checkbox"/> Edit	Melbourne Node	61-3-99990000
<input type="checkbox"/> Edit	Auckland Node	64-9-355-0000

[Delete Selected](#) [Add New](#)

Phone number should be in the format: *country code-area code-number*

Audio - WebEx Site Configuration



[Home](#)

Manage Site

- [Site Settings](#)
- [Tracking Codes](#)
- [Company Addresses](#)
- [Email Templates](#)
- [Meetings in Progress](#)

Manage Users

- [Add User](#)
- [Edit User List](#)
- [Import/Export Users](#)
- [Edit Privileges](#)
- [Send Email to All](#)

Session Types

- [Add Custom Type](#)
- [Session Type List](#)

Assistance

- [Help](#)

[Log out](#)

Site Settings

- Quick Scheduler is default
- Advanced Scheduler is default
- Allow hosts to save their own settings

Service Request Settings

- Allow users to request a service

Cisco Unified MeetingPlace

[View Cisco Unified MeetingPlace Settings](#)

Site Options

- Display banner ad in My Site

Welcome page

Display this service to all users

View Cisco Unified MeetingPlace Integration Settings - Google Chrome

<https://australia.webex.com/adm03061d/viewmpadaptor.do?siteurl=australia>

View Cisco Unified MeetingPlace Integration Settings

Setting name	Setting value
MP Version	8.5
MP Owned Profiles	No
PIN Min Length	5
PIN Max Length	24
PIN Expiration Days	90
Site MP Global Call-back	Yes
Site MP Call-back	Yes
Site MP Call-in	Yes
Audio-only Session	Yes
TSPAdapterURL	cump85.cisco.com
TSP Certificate	View TSP Certificate
Last Modified Time	12/13/11 5:27 pm
Create Time	10/18/11 4:51 pm

Audio Broadcast/NBR

NBR Dial-out Number	61-2-99990000
NBR Dial-out Sequence	P2D3#P0D%NBRProfileNumber%#P0D%NBRProfilePassword%#P0D%MeetingID%#P1D1P0
NBR Dial-out Profile Number	*****
NBR Dial-out PIN	*****

MP Phone Numbers

1	Sydney Node	61-2-99990000
2	Melbourne Node	61-3-99990000
3	Auckland Node	64-9-355-0000

Close

Audio - WebEx Site Configuration



[Home](#)

Manage Site

- [Site Settings](#)
- [Tracking Codes](#)
- [Company Addresses](#)
- [Email Templates](#)
- [Meetings in Progress](#)

Manage Users

- [Add User](#)
- [Edit User List](#)
- [Import/Export Users](#)

- [Email Templates](#)
- [Meetings in Progress](#)

Manage Users

- [Add User](#)
- [Edit User List](#)
- [Import/Export Users](#)
- [Edit Privileges](#)
- [Send Email to All](#)

Session Types

- [Add Custom Type](#)
- [Session Type List](#)

Assistance

- [Help](#)

[Log out](#)

Edit User

Account Type:

Host Site administrator Site Admin - View only

* Denotes required fields

Account Information:

First name:	<input type="text" value="Darren"/>
Last name:	<input type="text" value="Henwood"/>
User name:	<input type="text" value="dhenwood"/>

Telephony privileges:

- Cisco Unified MeetingPlace Audio Conferencing
 - Call-in teleconferencing
 - Call-back teleconferencing
 - Global call-back teleconferencing
- WebEx Teleconference Service
 - Call-in teleconferencing
 - Toll
 - Toll free
 - Toll & Toll free
 - Allow access to teleconference via global call-in numbers
 - Enable teleconferencing CLI authentication
 - Host and attendees must have PIN enabled
 - Call-back teleconferencing
 - Global call-back teleconferencing
 - Other teleconference service
 - Integrated VoIP



Audio - Outlook Scheduling

- WebEx Meeting Number is the same as MP Audio Meeting ID
- Password protected secure meetings

Cc:

Subject: Please join now, meeting in progress: Cisco Update

Topic: Cisco Update
Date: Tuesday, December 13, 2011
Time: 5:33 pm, Australia Eastern Daylight Time (Sydney, GMT+11:00)
Meeting Number: 861 692 982
Meeting Password: cisco

To join the online meeting (Now from mobile devices!)

1. Go to <https://australia.webex.com/australia/e.php?AT=MI&EventID=189033567&UID=1218057297&PW=NYmE2Y2YxZTVk&RT=MiM1NQ%3D%3D>
2. If requested, enter your name and email address.
3. If a password is required, enter the meeting password: cisco
4. Click "Join".
5. Follow the instructions that appear on your screen.

To view in other time zones or languages, please click the link:
<https://australia.webex.com/australia/e.php?AT=MI&EventID=189033567&UID=1218057297&PW=NYmE2Y2YxZTVk&ORT=MiM1NQ%3D%3D>

To join the audio conference only

1. Please call one of the following numbers:
Sydney Node: 61-2-99990000
Melbourne Node: 61-3-99990000
Auckland Node: 64-9-355-0000
2. Follow the instructions that you hear on the phone.
Your Cisco Unified MeetingPlace meeting ID: 861 692 982

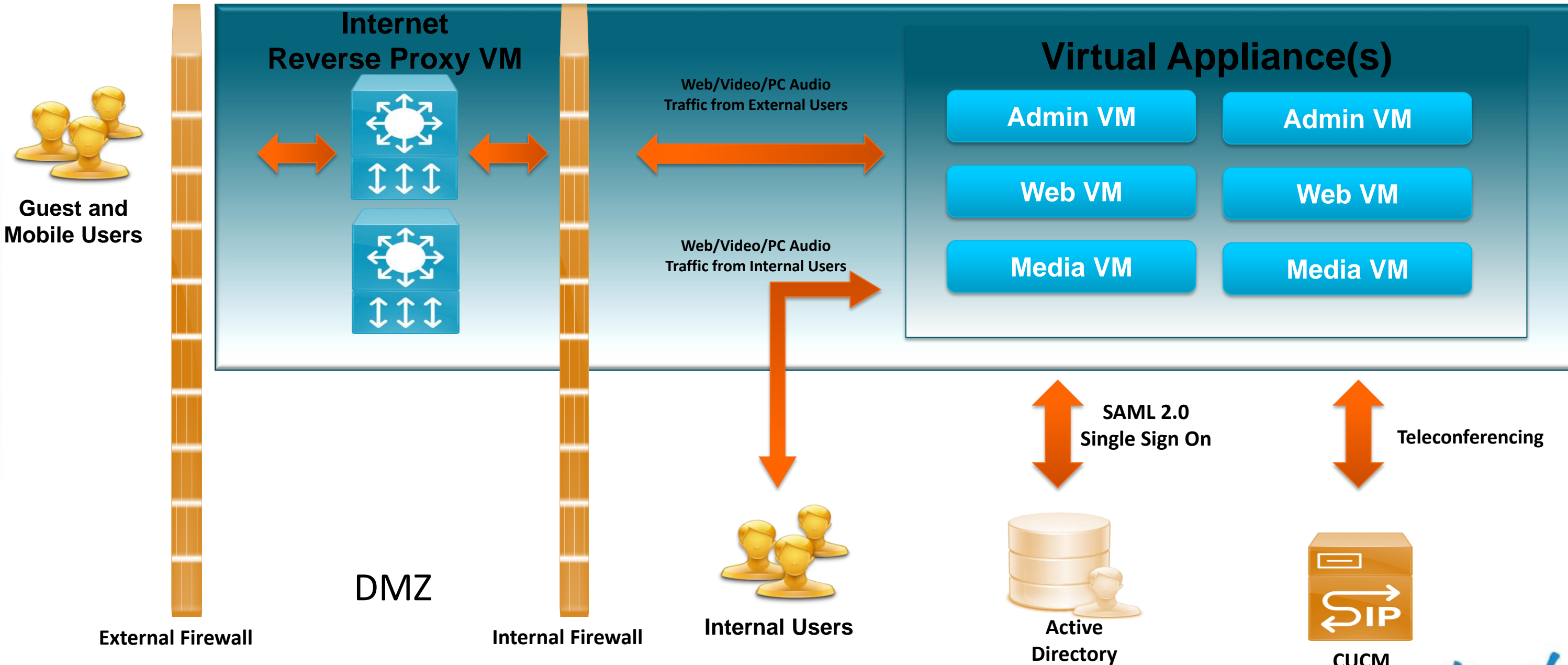
For assistance

WebEx On-Premise

Cisco WebEx Meeting Server (CWMS)



CWMS High-Level System Architecture



System Capacities

Media Type	50 Port	250 Port	800 Port	2000 Port
100% SIP/PC Audio	50	250	800	2000
Encrypted Audio (sRTP) *	50	250	800	2000
Secured Desktop sharing (SSL)	50	250	800	2000
Maximum concurrent HQ video users	25	125	400	1000
Single Meeting Maximum Size**	50	100	100	100
Maximum simultaneous recordings (=5%)	3	13	40	100
Maximum Active User Profiles in database	250,000	250,000	250,000	250,000

*Includes high fidelity Codecs E.g. G722

**For larger Meetings customer can order Event Centre directly



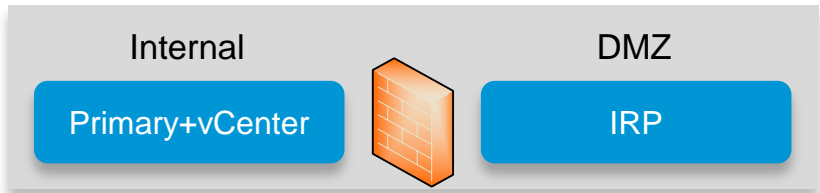
Server Sizing Guidelines

Model Size Simultaneous Users	Company Knowledge Workers based on usage	Average Minutes Per Month Ranges
50 Ports	~ 500 heavy (10 to 1) ~ 1,000 avg. (20 to 1) ~ 1,500 light (30 to 1)	50-125 K (2500 min/port)
250 Ports	~ 2,500 heavy (10 to 1) ~ 5,000 avg. (20 to 1) ~ 7,500 light (30 to 1)	130-750 K (3000 min/port)
800 Ports	~ 8,000 heavy (10 to 1) ~ 16,000 avg. (20 to 1) ~ 24,000 light (30 to 1)	1000 K - 2.8 M (3500 min/port)
2000 Ports	~ 20,000 heavy (10 to 1) ~ 40,000 avg. (20 to 1) ~ 60,000 light (30 to 1)	3-8 M (4000 min/port)

* Actual usage may vary based on conferencing. Ensure to account for growth

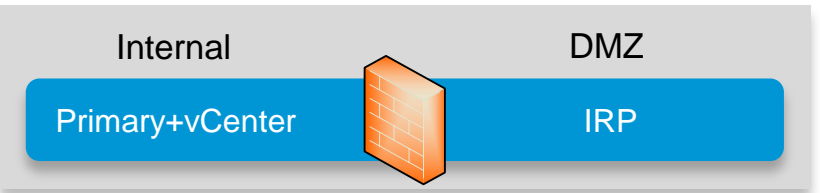
Deployment Layouts

50 Concurrent Users



Primary & vCenter CoResident – IRP separate UCS

or



Primary, vCenter, IRP CoResident – Dual homed

or

Internal: Primary+vCenter, HA Primary
DMZ: IRP, HA IRP

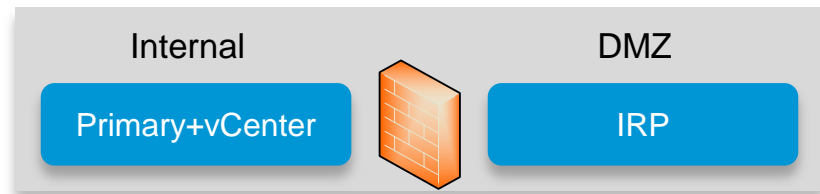
High Availability Options



Deployment Layouts

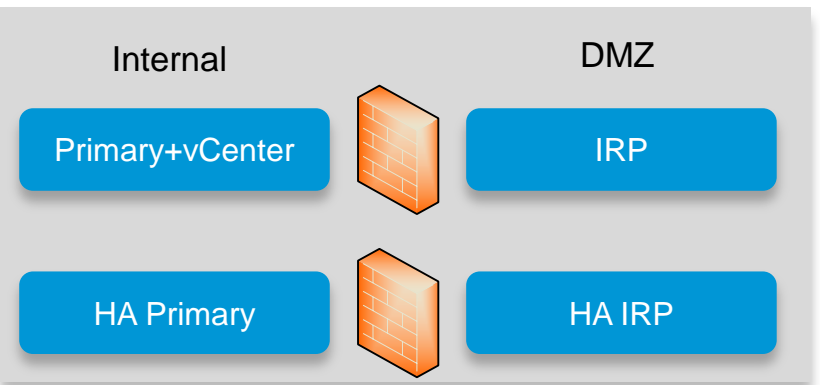
For DR - mirror layout in second DC

250 Concurrent Users



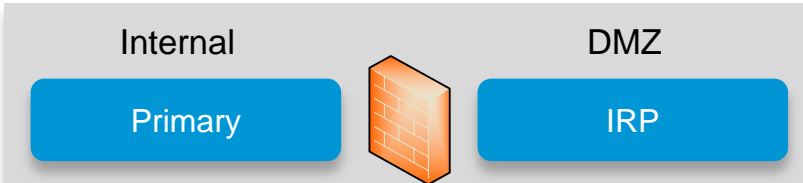
Primary & vCenter CoResident – IRP separate UCS

or



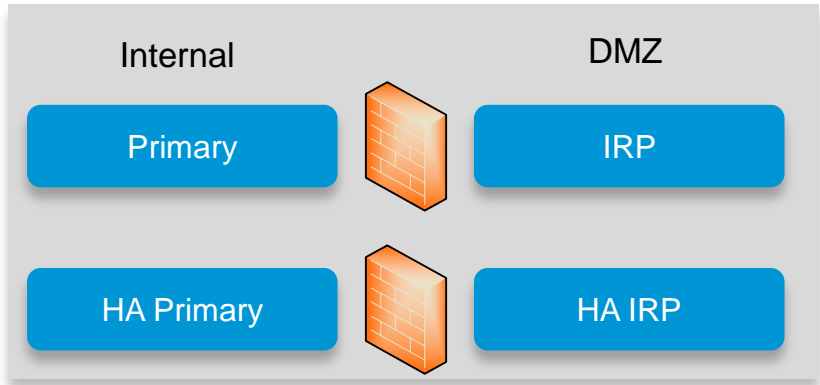
High availability – single DC
Primary can be reside with vCenter

800 Concurrent Users



Primary – IRP separate UCS
vCenter still required, but cannot be CoResident

or



High availability – single DC
vCenter still required, but cannot be CoResident

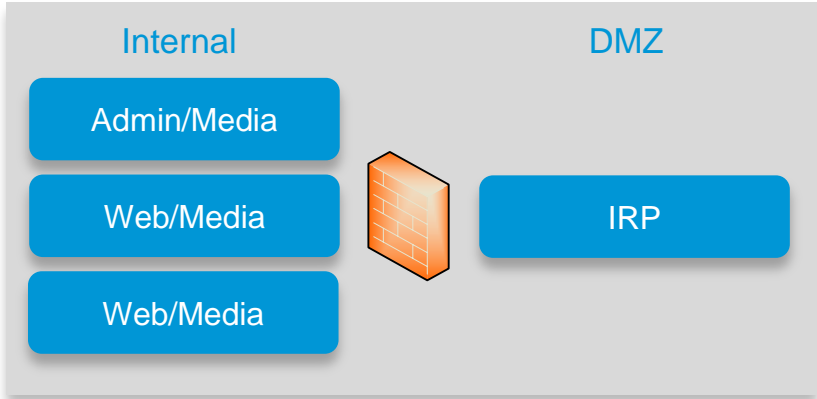
Data Center ESXi Host



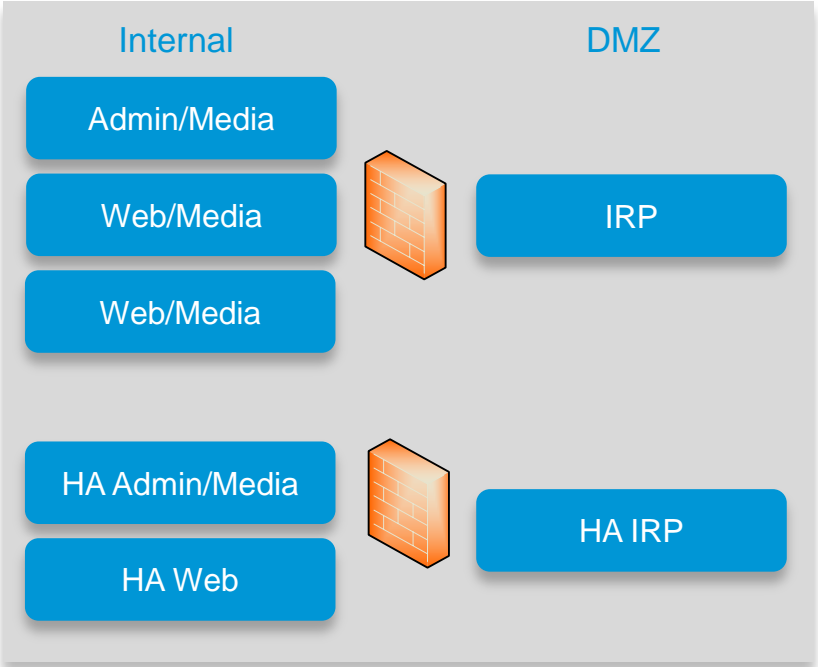
Deployment Layouts

2000 Concurrent Users

For DR - mirror layout in second DC



or



High Availability Option



Network Requirements



General Requirements

Category	System Requirements
UCS	<ul style="list-style-type: none"> • UCS only, support for 3rd party servers planned • No Co-Residency in V1 (vcenter can be co-resident in certain deployment types)
VMware	<ul style="list-style-type: none"> • VMware 5.0 <ul style="list-style-type: none"> • vSphere 5.0 Standard for lower scale deployments • vSphere 5.0 Enterprise Plus for higher scale deployments • vCenter mandatory • One License per socket
Networking	<ul style="list-style-type: none"> • LAN <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Similar to WebEx Cloud for HQ Video, Web Sharing, etc.
Storage (Network Attached Storage)	<ul style="list-style-type: none"> • Needed only if customer wants to record meetings and keep system snapshots (for DR)
Teleconferencing	<ul style="list-style-type: none"> • CUCM 7.1, 8.6, 9.0 for SIP Trunk based Teleconferencing
SSO (Single Sign On)	<ul style="list-style-type: none"> • If using ADFS 2.0 as IdP then customer needs AD (Active Directory) 2008 • Other SAML 2.0 SSO Compliant IdP also supported – same as WebEx Cloud • PingFederation V6.5.2, ADFS V2, OpenAM V9.5.4

UCS Requirements

Common Requirements				
<ul style="list-style-type: none"> UCS M2 Gen or above (Westmere-EX Processor or above) w/AES-NI 2.4GHz Processor or above vSphere ESXi version 5 Additional NIC recommended for VMware Management Network 		<ul style="list-style-type: none"> vCenter version 5 DAS minimum 4 Drives - RAID 10 SAN Supported RAID Battery Backup 		
50 Port				
Recommended host C220-M3, vSphere Standard, 7200RPM HDD, 1GB NIC, 1TB HDD, Built in RAID				
Primary	IRP	Co-Resident Configurations		
<ul style="list-style-type: none"> 4 cores 26 GB RAM 1 NIC 	<ul style="list-style-type: none"> 4 cores 20 GB RAM 1 NIC 	Primary + vCenter <ul style="list-style-type: none"> 8 cores 36 GB RAM 1 NIC 	Primary + IRP <ul style="list-style-type: none"> 8 cores 40 GB RAM 2 NIC 	Primary + IRP + vCenter <ul style="list-style-type: none"> 12 cores 42 GB RAM 2 NIC
250 Port				
Recommended host C220-M3, vSphere Standard, 7200RPM HDD, 1GB NIC, 1TB HDD, Built in RAID				
Primary	IRP	Co-Resident Configuration		
<ul style="list-style-type: none"> 12 Cores 56 GB RAM 1 NIC 	<ul style="list-style-type: none"> 12 Cores 36 GB RAM 1 NIC 	Primary + vCenter <ul style="list-style-type: none"> 16 Cores 56 GB RAM 1 NIC 		
800 or 2000 Port				
Recommended host C460-M2, vSphere Enterprise Plus, 10,000RPM SAS, 10Gbps NIC, 1TB HDD, LSI 9260-8i				
Primary <ul style="list-style-type: none"> 40 Cores 80 GB RAM 4 NIC 		IRP <ul style="list-style-type: none"> 40 Cores 36 GB RAM 4 NIC 		

End User Requirements

Category	System Requirements
Web User Interface	<p>Browsers</p> <ul style="list-style-type: none">• Internet Explorer 8+ (32-bit/64-bit)• Firefox 9+ (Mac/Windows)• Safari for Snow Leopard and Lion, Mountain Lion (Mac)• Chrome Latest Releases (Mac/Windows)
Desktop Operating Systems	<ul style="list-style-type: none">• Windows XP SP3 and later• Windows Vista (32-bit/64-bit)• Windows 7 (32-bit/64-bit)• <i>Windows 8 Planned</i>• Windows Server 2008 (64-bit)• Mac OS 10.6 Snow Leopard, 10.7 Lion, and 10.8 Mountain Lion
Calendaring Interfaces	<ul style="list-style-type: none">• PC: Microsoft Outlook 2007 SP2+ and 2010 SP1+ (32-bit/64-bit)• PC & Mac: Web Calendaring• Mobile: iOS WebEx App
Mobile Platform	<ul style="list-style-type: none">• iOS v5.1 or later (iPhone and iPad) – same Mobile Meeting Centre Client download as SaaS WebEx• <i>Android Planned</i>

Network Bandwidth Sizing

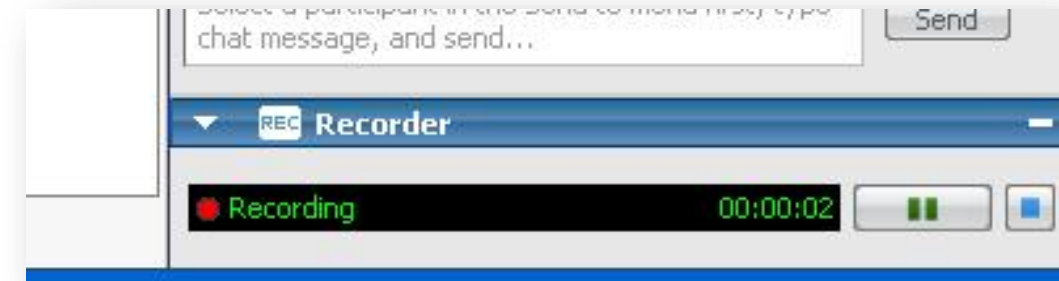
- 1Mb per use base assumption (Audio/Web/Video)
- Typical Enterprise Usage 80% Internal & 20% External
 - Actual customer usage may vary on how they use conferencing and their business practices...some enterprises may be 60/40 or 70/30 or 90/10
 - 800 Port system - Assume 80% internal/20% External
 - Internal = 800 x 80% = 640 x 1 MB = 640 MB on LAN/WAN maximum**
 - External = 800 x 20% = 160 x 1 MB = 160 Mb on Internet Proxies/Firewalls maximum**



WebEx Network Bandwidth Whitepaper
www.webex.com/pdf/wp_bandwidth.pdf

Storage Sizing

- Customer Provided NFS
- Recording
 - Average Daily Meetings(AVG) ??
 - Business Days per Month(BDM) 22 weekdays
 - % of meetings recorded per month(MR) 5%
 - Application Sharing(AS) 36MB/HR
 - Audio(A) 30MB/HR
 - Video(V) 104MB/HR
 - Retention in Months(R) ??
- $AVG \times BDM \times MR \times (AS \times \% \text{ of meetings using app sharing}) \times (A \times \% \text{ of meetings using audio}(100\%)) \times (V \times \% \text{ of meetings using Video}) \times R$
- NFS also used to store system backup (~400MB)



Understanding DNS – Split Horizon

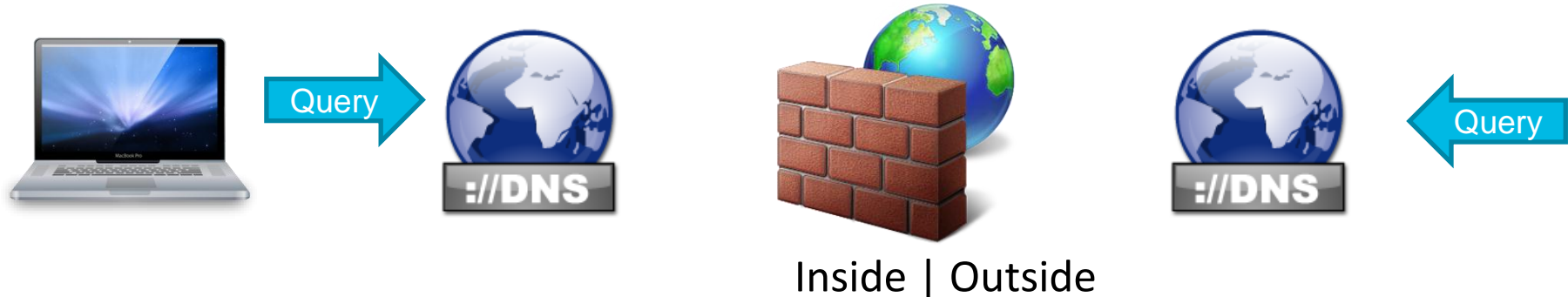


“In computer networking, **split-horizon DNS**, **split-view DNS**, or **split DNS** is the facility of a Domain Name System (DNS) implementation to provide different sets of DNS information, selected by, usually, the source address of the DNS request.

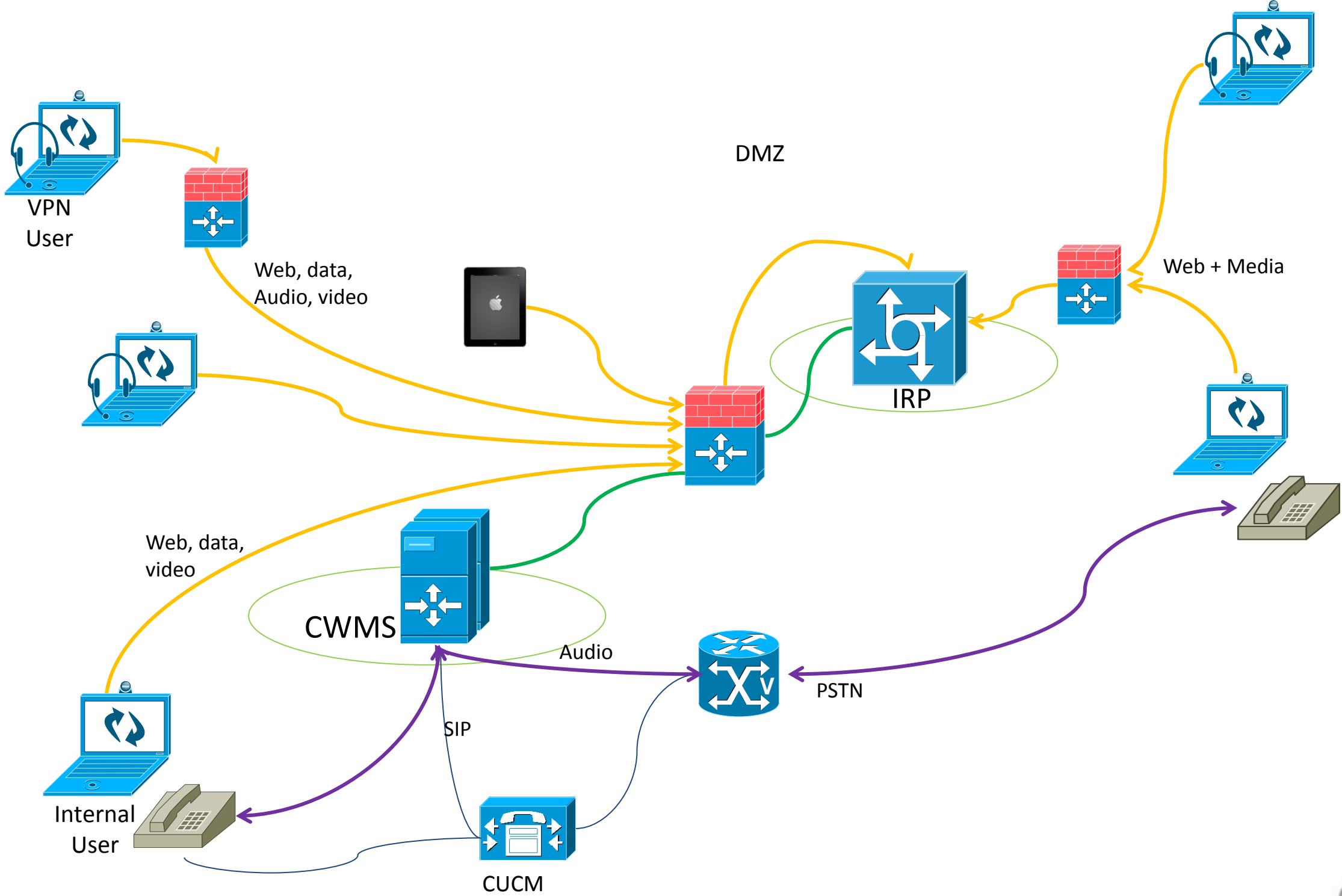
Implementation of split-horizon DNS can be accomplished by running distinct DNS server devices for the desired access granularity within the networks involved.”

Name	IP Address
CWMS.acme.com.au	10.20.30.40

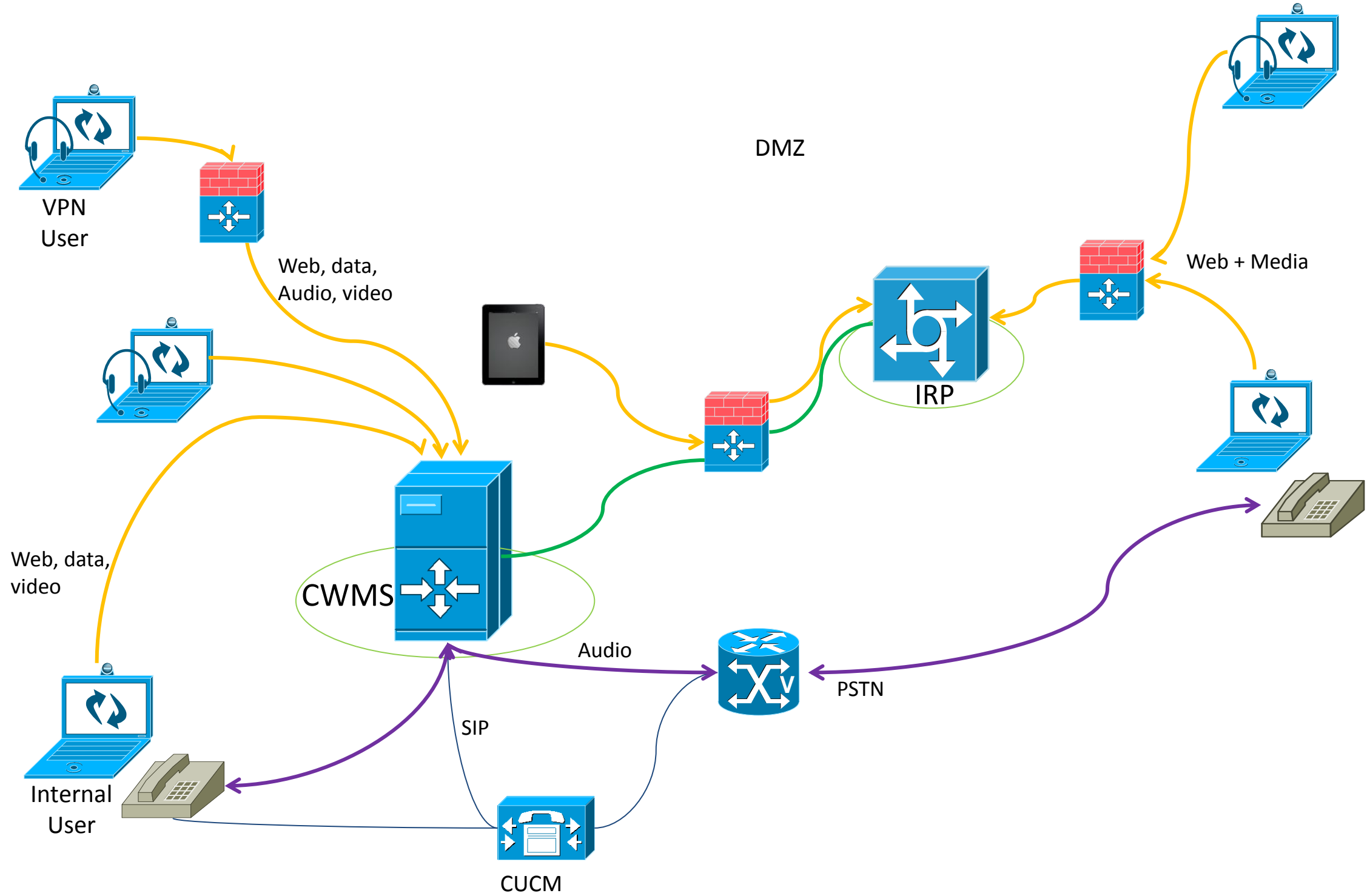
Name	IP Address
CWMS.acme.com.au	64.104.200.40



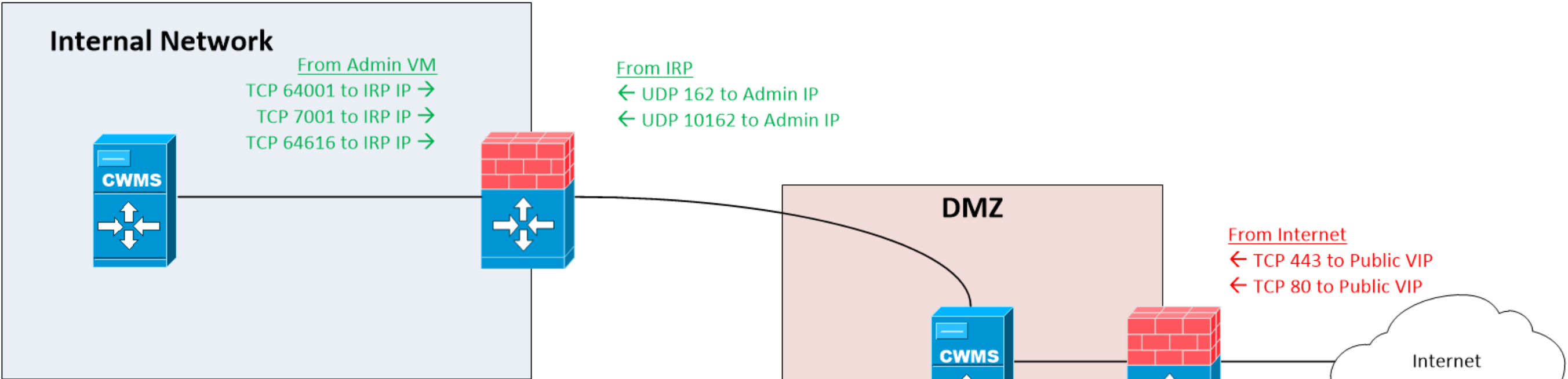
Non-Split Horizon CWMS DNS Model



Split-Horizon CWMS DNS Model



Network Port Requirements



DNS Table

HostName	Internal IP Address
Admin-vm.domain.com	172.16.1.100
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.



Deployment Steps

- 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 vCenter
- SMTP server for the new account emails
- Email address for the primary administrator



Audio Integration



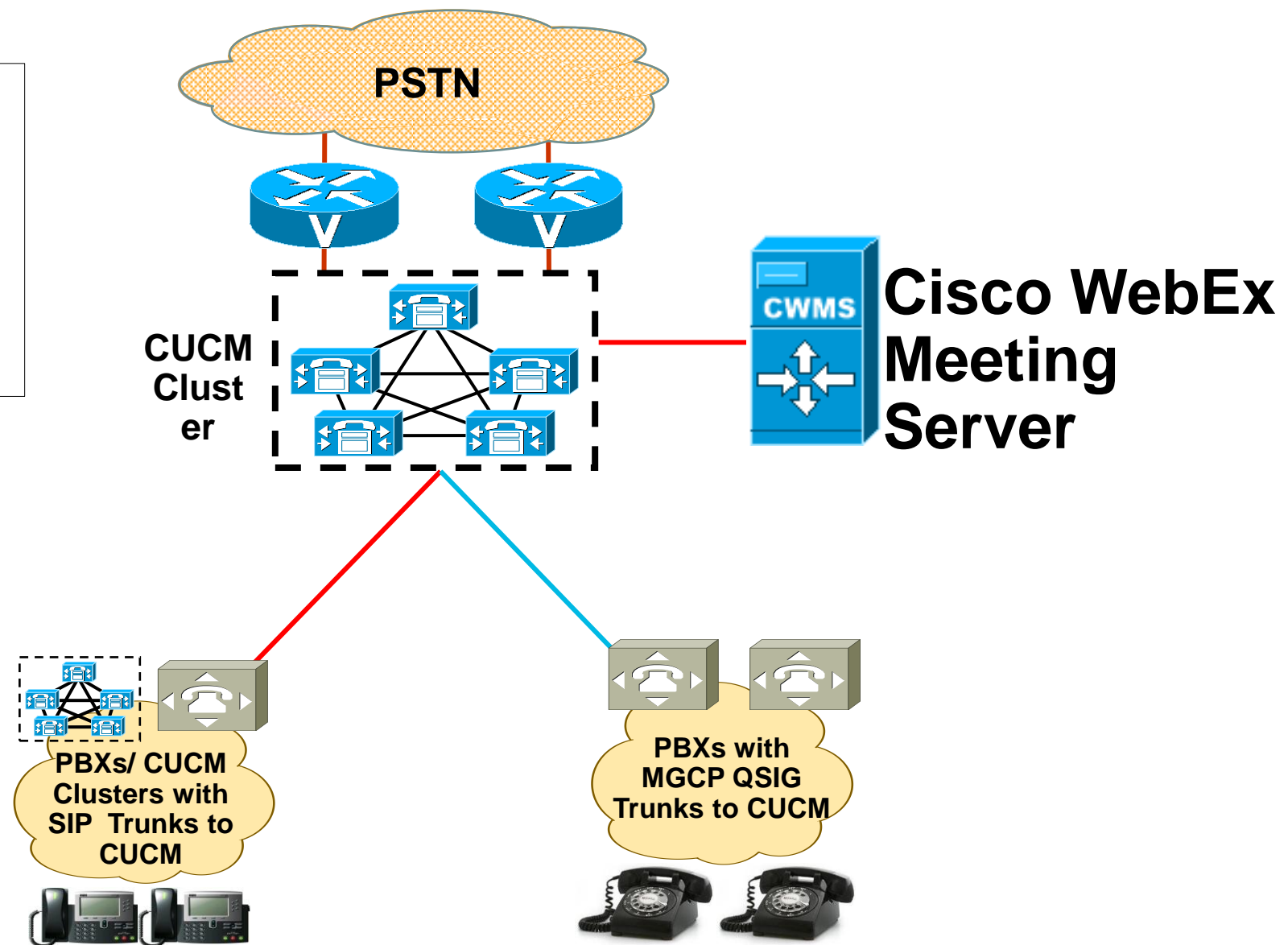
Audio Deployment

Dial-In Examples:

1800 123 456
(03) 9999 0000
x5000

Toll Free
Direct
Internal

Or CallBack



- CWMS requires a SIP trunk to CUCM. Any supported connection from CUCM to a destination is then available; such as H323, MGCP, QSIG, SIP, etc.
- Alternatively, CWMS supports using your PC's audio - VoIP

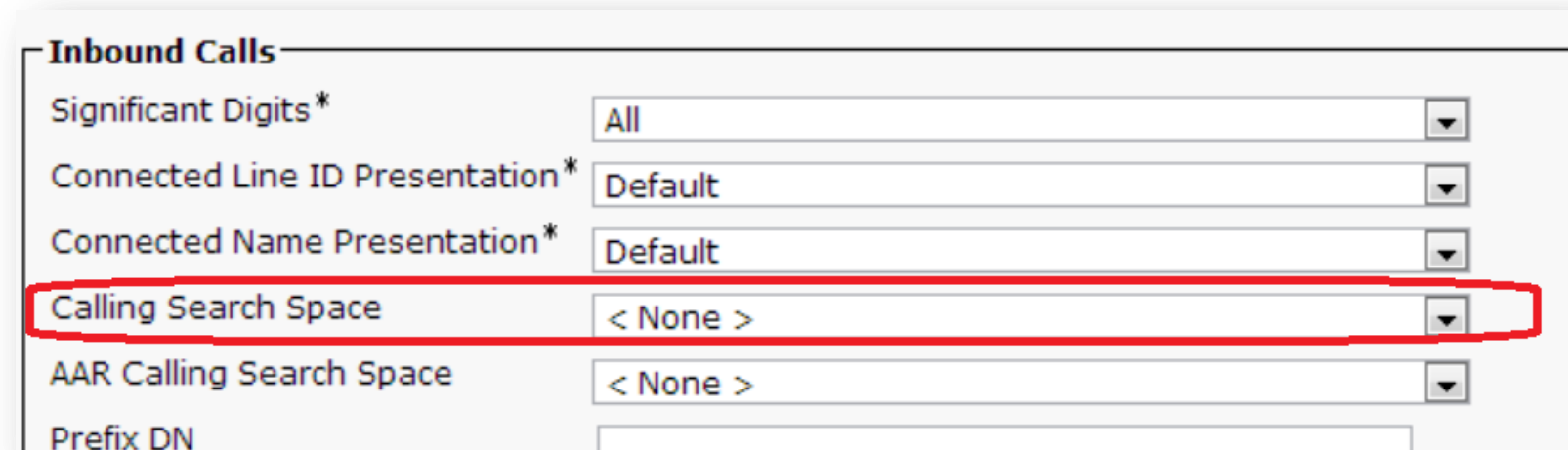
Call Control – Inbound/Outbound

- Call-back Teleconferencing

- Best End User experience to Join Web session first, then use Callback
- Most efficient call processing methodology
- Controlled via SIP trunk outbound to CUCM
- Can be disabled

- Dial In Teleconferencing

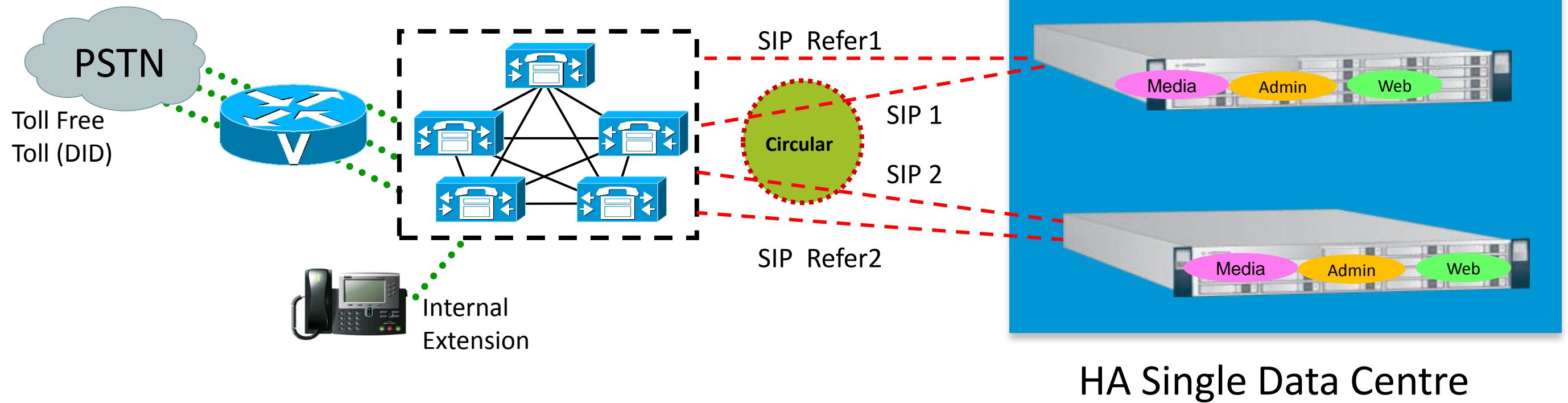
- SIP Trunks
- Inbound Calling can be from unlimited number of CUCM clusters OR via intercluster trunks (ICT) between all clusters to a centralised CUCM
- Typical customer deployments are with 3 phone numbers: toll free, toll and internal dial numbers pointed to SIP trunks inbound to CWMS system.
- Uses SIP Refer to provide load balancing across redundant systems



The image shows a configuration window titled "Inbound Calls" with several dropdown menus. The "Calling Search Space" dropdown is highlighted with a red rectangle and is currently set to "< None >". Other settings include "Significant Digits*" set to "All", "Connected Line ID Presentation*" set to "Default", "Connected Name Presentation*" set to "Default", "AAR Calling Search Space" set to "< None >", and "Prefix DN" which is empty.

Field	Value
Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

SIP Trunking to CUCM



SIP Trunking to CUCM

System ▾ Call Routing ▾ Media Resources ▾ Advanced F

Route Pattern Configuration

Save **X** Delete Copy Add New

Pattern Definition

Route Pattern* 3000

Route Partition < None >



Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.66.120.224		5060

TP Preferred Originating Codec* 711ulaw

LF Presence Group* Standard Presence group

IP Trunk Security Profile* **Non Secure SIP Trunk Profile 5060**

erouting Calling Search Space < None >

ut-Of-Dialog Refer Calling Search Space < None >

SIP Route Pattern Configuration

Save **X** Delete Copy Add N

- Status -

i Status: Ready

- Pattern Definition -

Pattern Usage IPAddress Routing

IPv4 Pattern* 10.66.120.224



Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.66.120.224		5062

TP Preferred Originating Codec* 711ulaw

LF Presence Group* Standard Presence group

IP Trunk Security Profile* **Non Secure SIP Trunk Profile 5062**

erouting Calling Search Space < None >

ut-Of-Dialog Refer Calling Search Space < None >

- SIP Trunk Security Profile Information -

Name* Non Secure SIP Trunk Profile 5062

Description Non Secure SIP Trunk Profile authen

Device Security Mode Non Secure

Incoming Transport Type* TCP+UDP

Outgoing Transport Type TCP

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name

Incoming Port* 5062

Enable Application level authorization

Audio Parameters



- There is no loss in capacity when using complex/low bitrate codecs – For the best user experience we recommend G722 for the best quality audio. Other codecs include G711 and G729
- Can set QoS for SIP Audio – Outbound Call-back
- Unified Communications Sizing Tool – CWMS is now available
<http://tools.cisco.com/cucst/faces/newSol.jsp>
- The most commonly purchased edition of CWMS has TLS/SRTP audio encryption available
 - Turkish and Russian customers may only purchase the "-AU" edition which lacks TLS/SRTP and is thus compliant with Russian / Turkish import laws

End User Management/SSO



Managing User Profiles in WebEx

There are three options:

- Manually define individual using administrative GUI
- Bulk import based upon .CSV
- Federated SSO (Automated)
 - SAML 2.0 SSO End User Authentication
 - Auto-Create Profile (Optional)

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:

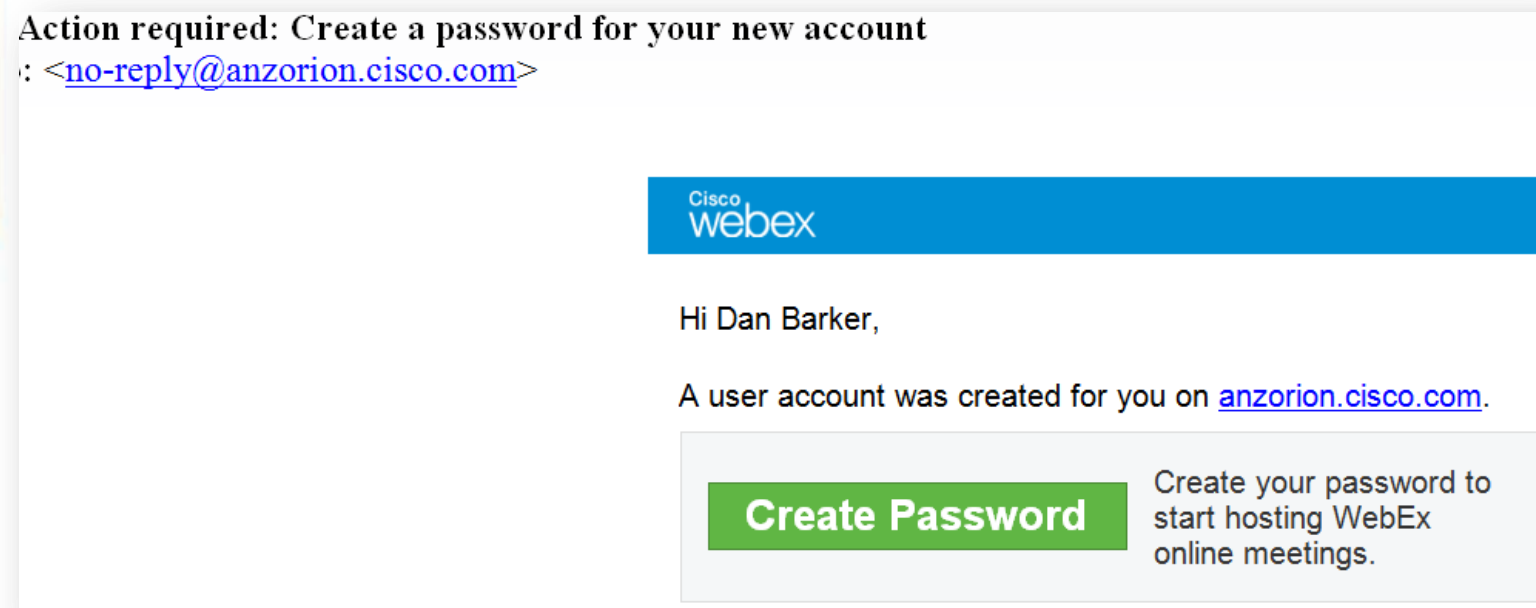
Delimiter:
 Tab
 Comma

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

User Profile Parameters

- Required Fields (First Name, Last Name, Email)
- Optional (10) customisable fields available
- User receives email to set password

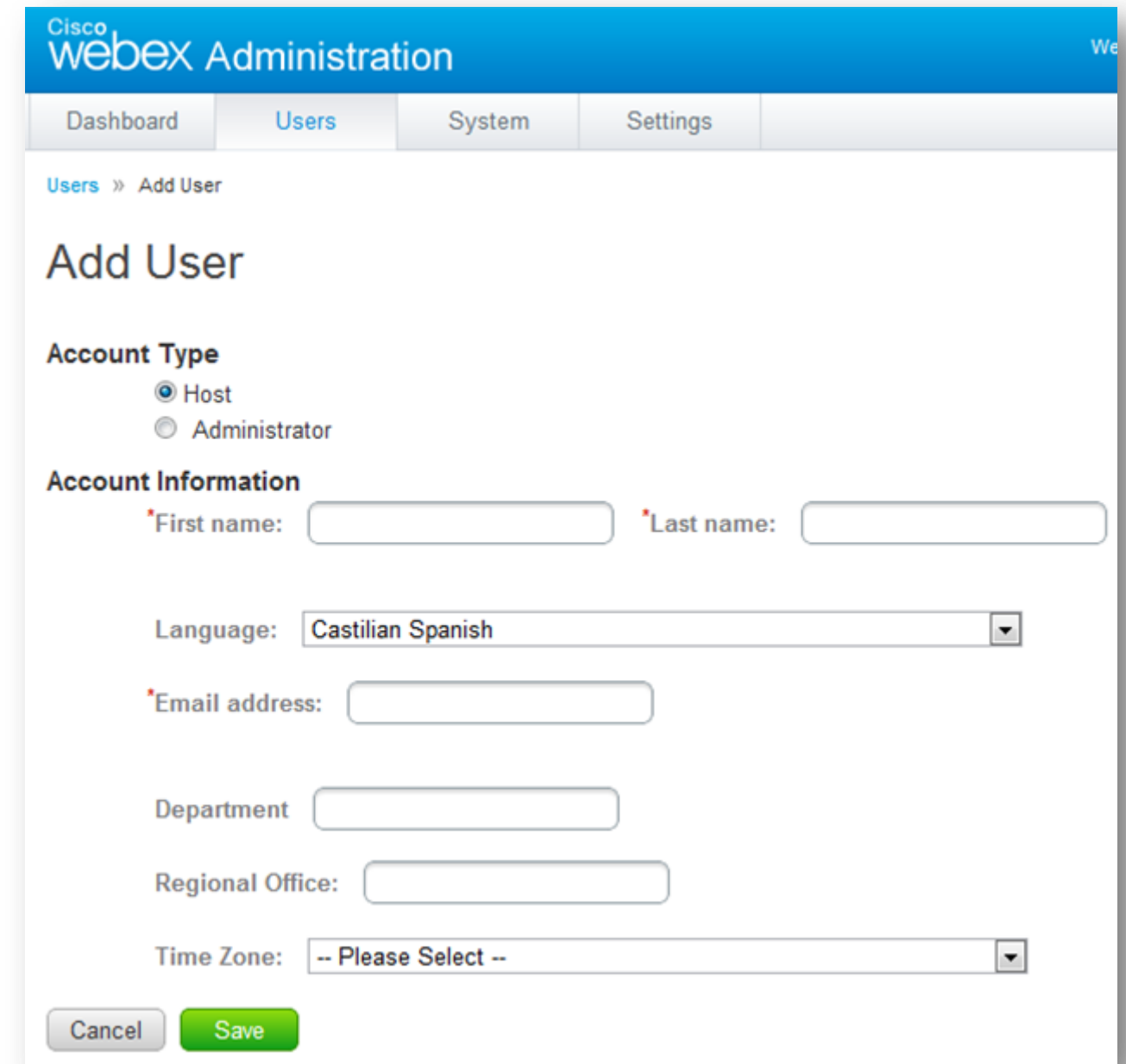
Action required: Create a password for your new account
: <no-reply@anzorion.cisco.com>



Hi Dan Barker,

A user account was created for you on anzorion.cisco.com.

Create Password Create your password to start hosting WebEx online meetings.



Cisco WebEx Administration

Dashboard Users System Settings

Users » Add User

Add User

Account Type

Host
 Administrator

Account Information

*First name: *Last name:

Language:

*Email address:

Department:

Regional Office:

Time Zone:

Cancel Save

User Authentication

- Administrators can manage accounts and password requirements, as well as deactivate accounts.

Require strong passwords for user accounts

Minimum character length

Minimum number of alphabetic characters

Minimum number of numeric characters

Minimum number of special characters

Must include mixed case

Do not allow any character to be repeated more than 3 times

List of unacceptable passwords

List of unacceptable passwords

Company name, site name, user email address, and host name

Must not include previous passwords

CWMS Single Sign On

- Enabled by Administrator if needed
- 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 as well from outside firewall.
- X.509 Security Certificate uploaded into WebEx Server

WebEx SSO Customer Requirements

- SAML 2.0 Compliant Identity & Access Management System (IAM)
 - Microsoft Windows Server AD Federated Services(ADFS) and Geneva
 - CA SiteMinder
 - Ping Identity PingFederate
 - Sun Microsystems OpenSSO Enterprise
 - Others SAML 2.0 compliant
- X.509 Digital Certificate & SSL TLS Encryption
 - Granted by Certificate Authority Or Customer generated

Integrated Windows Authentication (IWA)

- Customer AD Federated Services (ADFS) needs to be configured for IWA
- After logging into Windows PC, no need to enter UserID/Password for WebEx meetings/scheduling
- Windows generates Kerberos/NTLMSSP token which IDMS validates and WebEx Federated SSO does not prompt for any userID /Password.



Windows
Server

Federated SSO Types

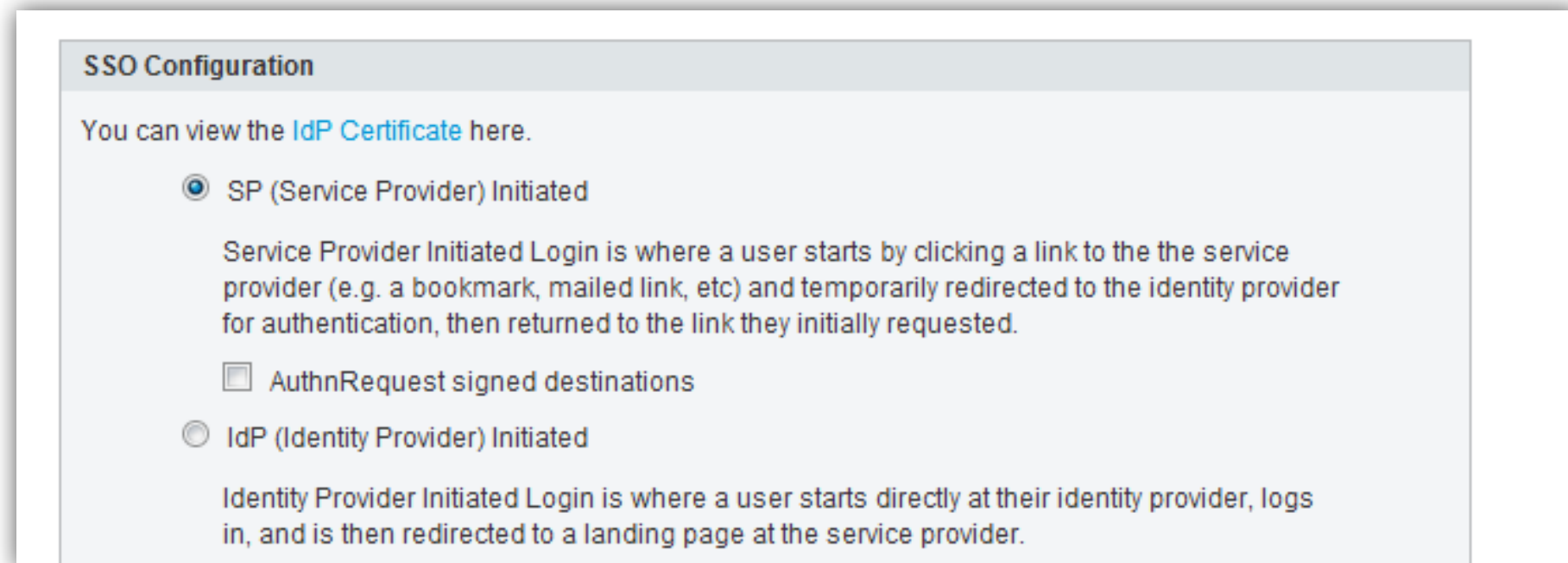
- IdP Initiated

- Identity Provider Initiated
- SAML 2.0

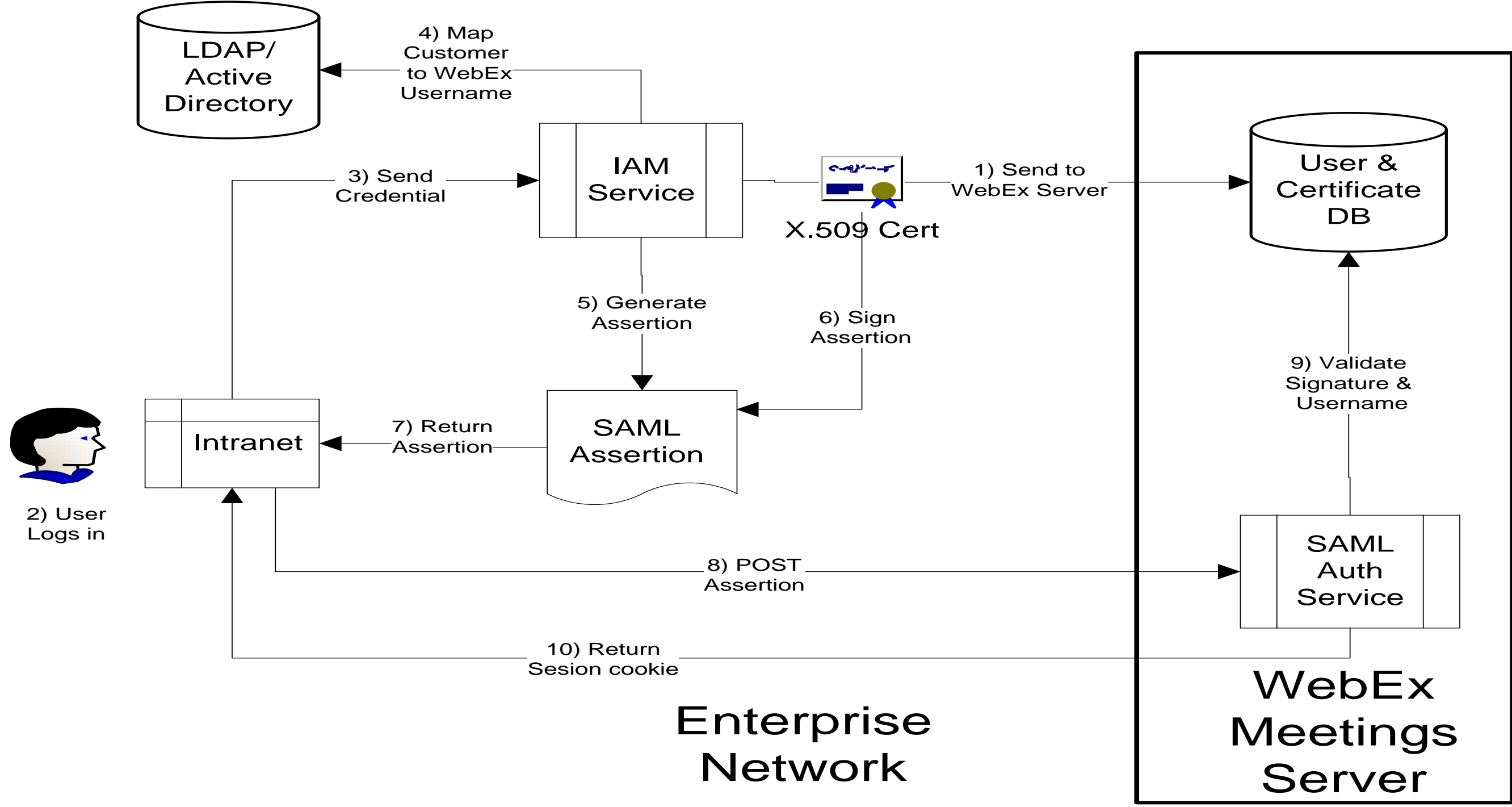
- SP Initiated

- Service Provider Initiated
- (WebEx Server)
- SAML 2.0

- PingFederation 6.5.2, ADFS V.2, OpenAM 9.5.4



SSO Authentication Process flow SP Initiated



Auto-Account Creation & Update

- Admin Settings for SAML 2.0
- Mandatory creation fields
 - lastname, firstname, email
- WebEx Server User Profiles receive all default permissions

- Single logout
- Auto account creation
- Auto account update
- Remove UID domain suffix for Active Directory UPN

High Availability



CWMS Redundancy Models – 3 options

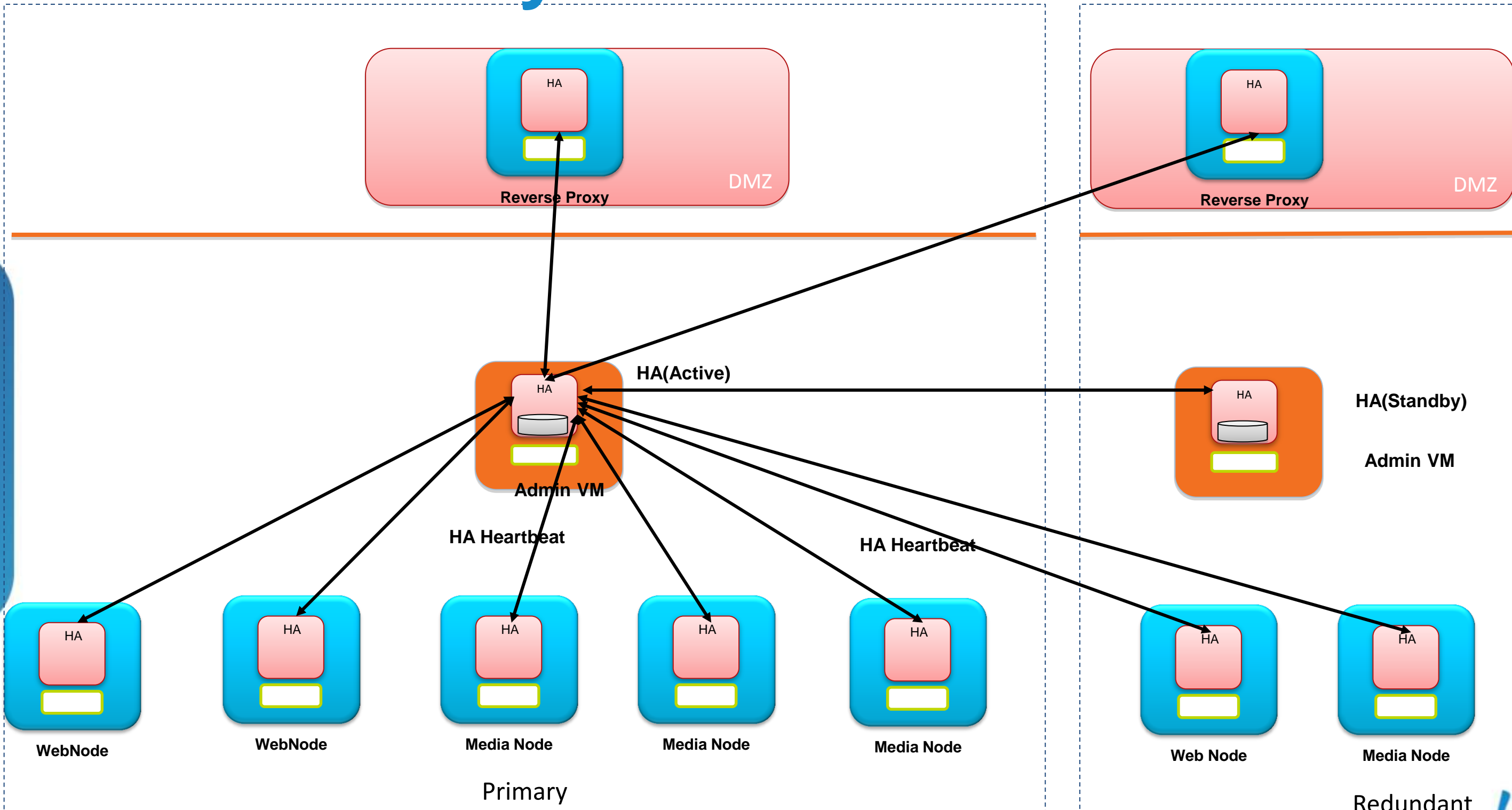
- Non-redundant Centralised (Recommended for initial deployment)
 - No redundant components
 - Single Data Centre only
 - With Internet Reverse Proxy (IRP) for External Access or without IRP
- Level 1: High Availability (HA) (Can be added on after initial deployment)
 - Centralised Single Data Centre – multiple servers/blades (N+1)
 - Active/Active resiliency – load sharing between all like VM's
 - <1ms latency between VMs
 - With Internet Reverse Proxy (IRP) or without IRP (no external web access)
- Level 2: Disaster Recovery (DR) – (Can be added on after initial deployment)
 - Dual Data Centre model – “cold standby” mode
 - Multiple ways to “enable” this site
 - Requires IT manual intervention to use DR Site system
 - Restore DB, change DNS routing, change CUCM SIP Routing



High Availability

- The goal of adding a redundant system is to provide “no single point of failure”.
- The redundant systems for Micro, Small and Medium are exactly same as the primary systems in terms of VMs/nodes.
- The Large redundant system has one each of the Admin, Media, Web and DMZ on the redundant side.
- In case of failure of the ‘Active HA’ on the primary Admin VM, the ‘Active HA’ can failover to the redundant Admin VM.
- There is no failback of HA to the Primary Admin VM unless there is a failure on the redundant Admin VM.

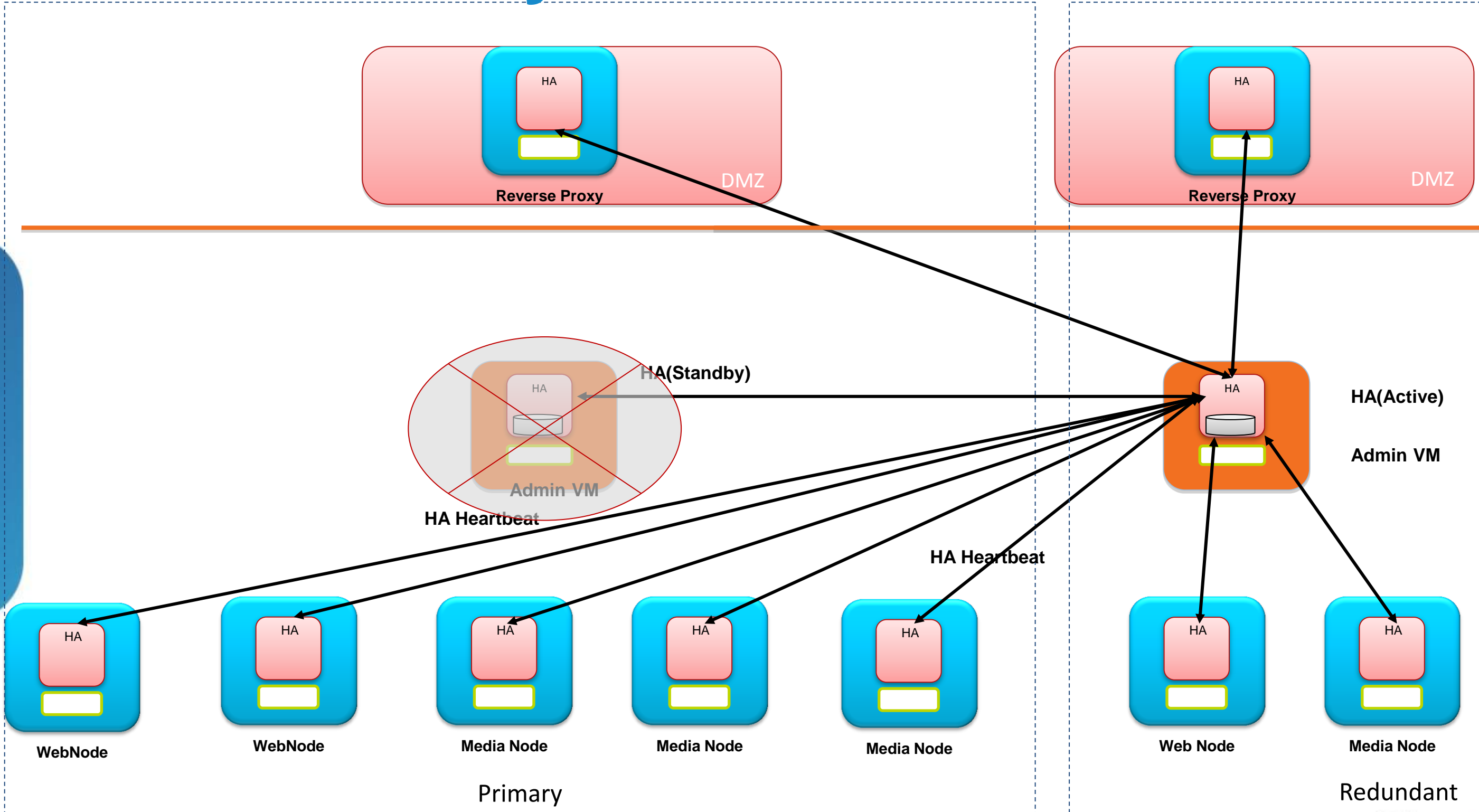
Redundant System



Large System

Redundant *Cisco live!*

Redundant System










Large System







System Status

System » Properties

Properties

Primary System					
Virtual Machines	Hostname	IPv4	IPv6	Status	
2000_Users_Admin	orion-webadmin-vm30.cisco.com	172.27.224.120		 Good	
2000_Users_Internet_Reverse_Proxy	orion-webadmin-vm3.cisco.com	10.194.133.157		 Good	
2000_Users_Media	orion-webadmin-vm33.cisco.com	172.27.224.123		 Good	
2000_Users_Media	orion-webadmin-vm34.cisco.com	172.27.224.124		 Good	
2000_Users_Media	orion-webadmin-vm35.cisco.com	172.27.224.125		 Down	
2000_Users_Web	orion-webadmin-vm31.cisco.com	172.27.224.121		 Good	
2000_Users_Web	orion-webadmin-vm32.cisco.com	172.27.224.122		 Good	

High Availability System					
Virtual Machines	Hostname	IPv4	IPv6	Status	
2000_Users_Internet_Reverse_Proxy	orion-webadmin-vm4.cisco.com	10.194.133.158		 Good	
2000_Users_Web	orion-webadmin-vm45.cisco.com	172.27.224.135		 Good	
2000_Users_Admin	orion-webadmin-vm44.cisco.com	172.27.224.134		 Good	
2000_Users_Media	orion-webadmin-vm46.cisco.com	172.27.224.136		 Good	

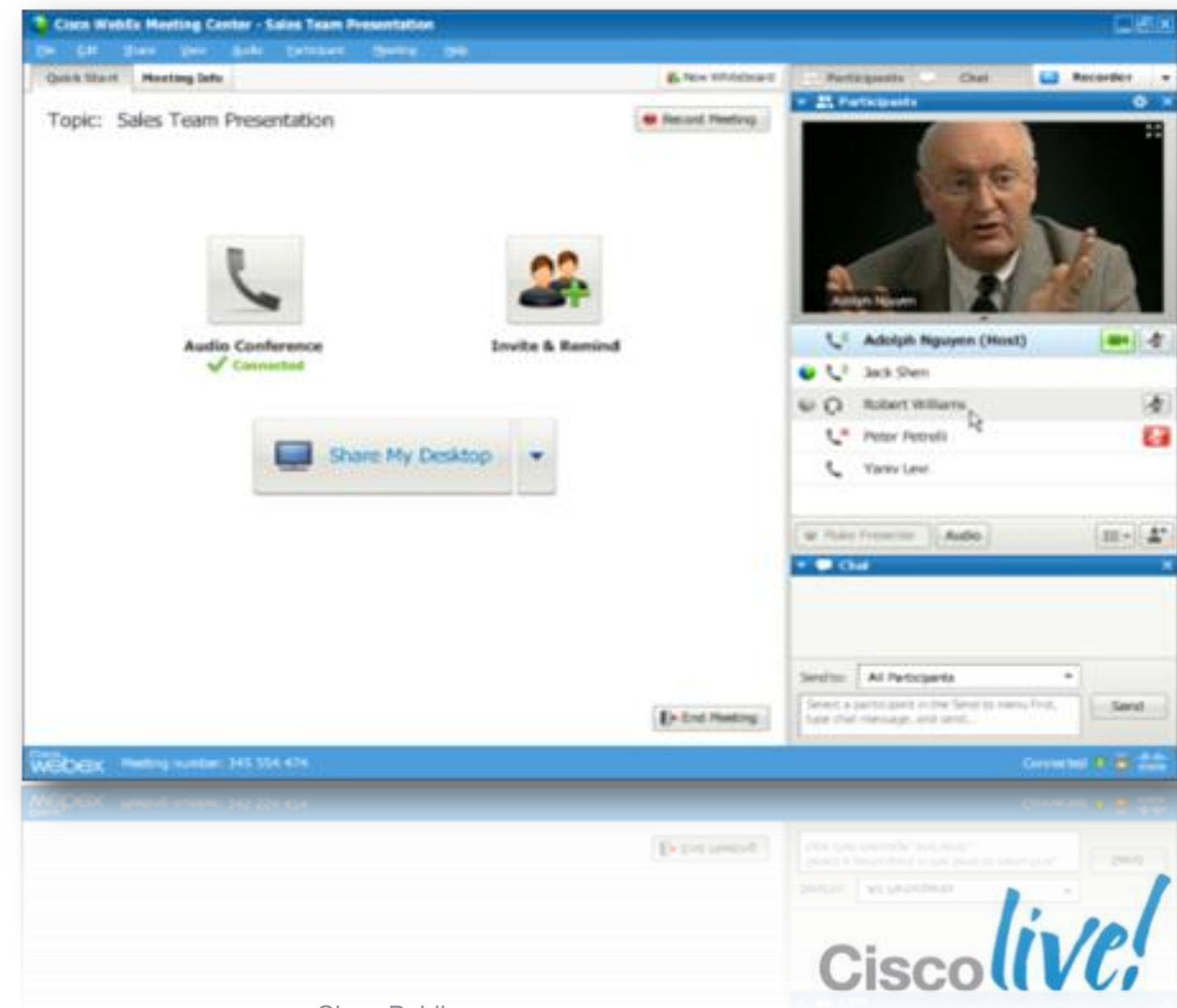
Recordings



CWMS Recording Elements

Combined files include any of these functions used in meetings

- Application Share, Desktop Share
- Document View, Presentation, Whiteboard
- Participant List – who's speaking/sharing
- HQ Video (view from Presenter)
- Chats
- Polls
- File Share(s)



Recordings

- Recordings are streaming only (no download or conversion supported)
- WebEx “.arf” formats (proprietary)
- A unique URL link to the current recording is associated so that a user can look up at the meeting later.
- Available to both internal and external users via URL Link
 - External users via Internet Reverse Proxy (IRP)
- Recordings Saved period is End User controlled – no automated expiration
- Administrator can Enable or Disable Recordings system wide
- Requires Customer provided NFS Server on network for Recording storage

CWMS Recording Setup

The screenshot shows the Cisco Webex Administration interface. At the top, the header includes the Cisco Webex Administration logo and navigation links: Welcome, Darren Henwood | Sign Out | Reports | Support | Help. Below the header is a navigation bar with tabs for Dashboard, Users, System, and Settings. A 'Turn Off Maintenance Mode' button is visible in the top right corner. The main content area shows a breadcrumb trail: System » Servers » Add Storage Server. The title of the page is 'Add Storage Server'. A modal dialog box is open, titled 'Add Storage Server' with a 'Cancel' button. The dialog contains the following text: 'The NFS server is the storage server where all the meeting recordings will be stored.' Below this is a field labeled '*NFS Mount Point:' with the value '10.66.120.226:/Recording' entered. A green 'Save' button is located below the input field. At the bottom of the page, there is a copyright notice: '© 2013 Cisco and/or its affiliates. All rights reserved.' and the Cisco logo.

General



Cisco Jabber Integration

- Cisco Jabber integration

 - Requires CWMS 1.1

 - Windows XP, Vista and Windows 7 only

 - Currently, no SSO (Single Sign On) support

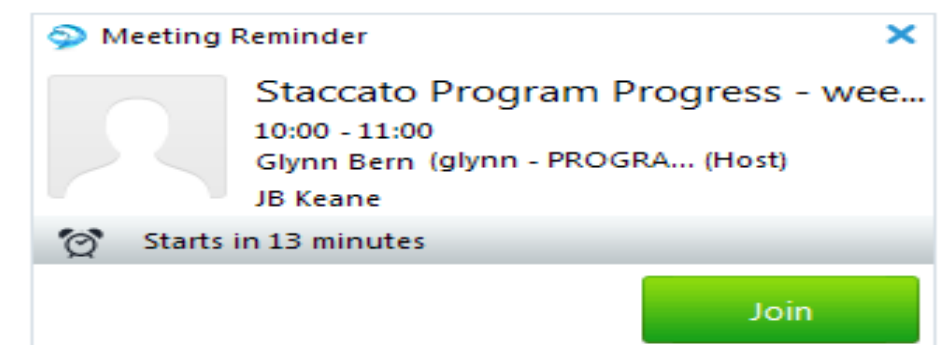
 - Launch WebEx meeting from daily calendar

 - Launch an instant WebEx meeting

 - Remind me of my upcoming meetings

- Jabber for Mac, iPad and iPhone

 - Road-map for CWMS Phase II



Productivity Tools Distribution

The screenshot shows the Cisco WebEx interface. At the top, there is a blue header with the 'Cisco webex' logo. Below the header are two tabs: 'Meetings' and 'Recordings'. The main content area is titled 'Downloads' and features a section for 'Productivity Tools' with a wrench and screwdriver icon. The text below the icon reads: 'WebEx Productivity Tools include the WebEx Meet Now and... meetings quickly without having to go to your WebEx service...'. A 'Download' button is located at the bottom of this section.

The screenshot shows the Systems Management Server (SMS) console. The left pane displays a tree view of the 'Systems Management Server' hierarchy, including 'Site Database (SMS - webex)', 'Collections', 'Packages', 'WebEx Communications Inc.', 'Access Accounts', 'Distribution Points', 'Programs', 'Advertisements', 'Software Metering Rules', 'Reporting', 'Product Compliance', 'Queries', 'Software Updates', 'System Status', 'Advertisement Status', 'WebEx Productivity Tools', 'Package Status', 'Site Status', 'Status Message Queries', 'Security Rights', 'Tools', and 'Online Library'. The right pane shows a table of software packages with columns for 'Name', 'Run Time (hh:mm)', 'Disk Space', and 'Comment'. A context menu is open over the 'Per-system unattended' package, showing options: 'All Tasks', 'Distribute Software', 'Distribute Software Updates', 'Delete', 'Properties', and 'Help'. The 'Distribute Software' option is highlighted.

Name	Run Time (hh:mm)	Disk Space	Comment
Per-system attended	Unknown	9 MB	
Per-system unattended	Unknown	9 MB	
Per-system uninstall			
Per-user attended			
Per-user unattended	nknown	9 MB	
Per-user uninstall	nknown	Unknown	

Upgrade Procedure



Version format: 1.0.1.157.A *[Major.Minor.Maintenance.BuildNumber.Line]*

- **Fresh installation**

In the form of OVA:

cisco-webex-meetings-servers-1.0.1.6.A.ova

- **Update**

In the form of ISO:

cisco-webex-meetings-servers-1.0.1.101.A.ISO

ISO package for an official release is available if an update to this release from prior release is supported

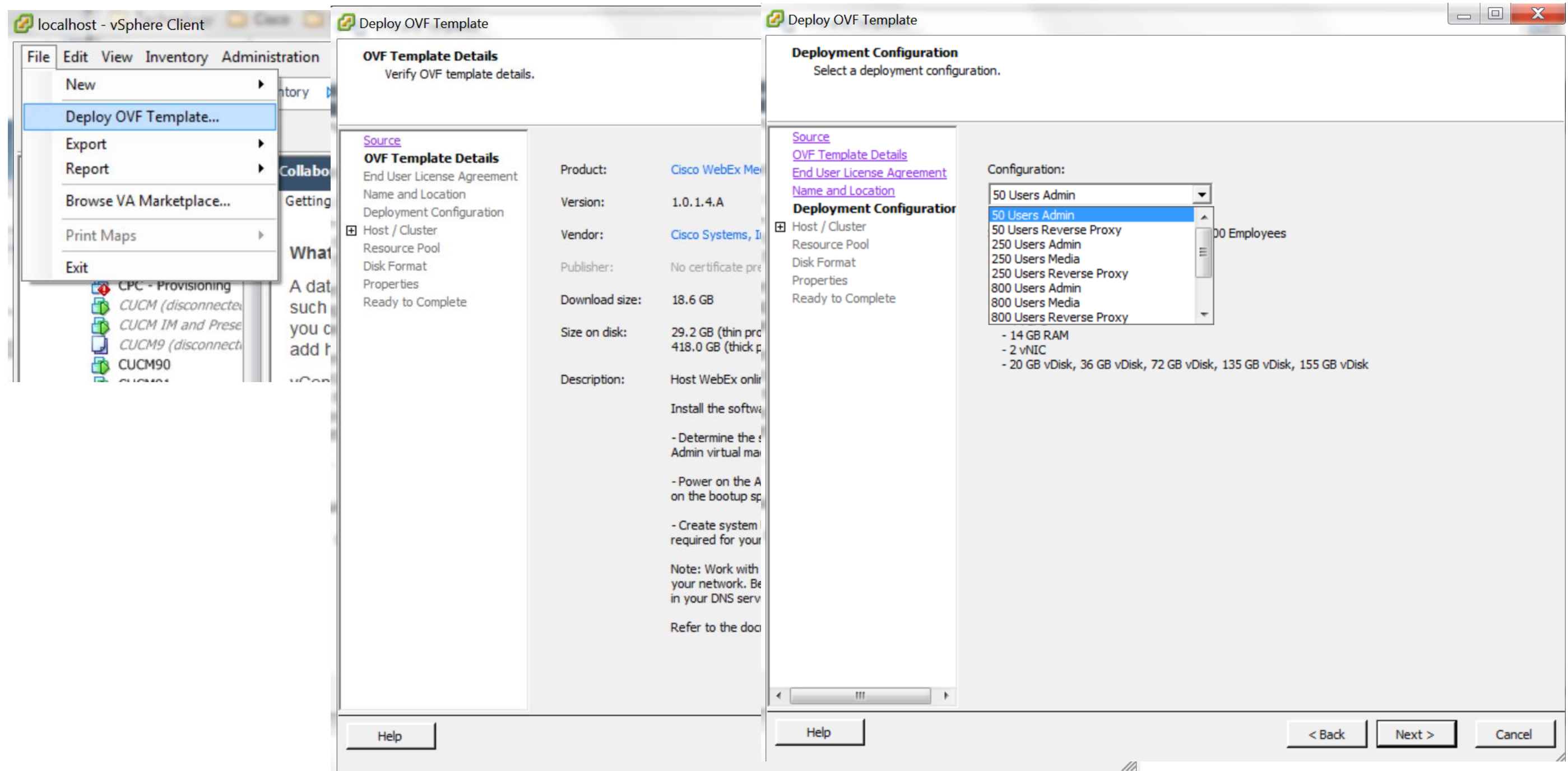
- **Patch**

Always in the form of ISO package

- **Upgrade, Expand**

Use OVA install new System

vCenter – Creating OVA



Troubleshooting – Logs

Cisco **Webex Administration** Welcome, Darren Henwood | Sign Out | Reports | **Support**

Dashboard | Users | System | Settings | Turn On Maintenance M

Support

Open/View Support Cases

Looking for technical support? Open a case with Cisco Technical Assistance Center (TAC). To open a case, you must have a service contract.

Cisco Technical Assistance Center (TAC): <http://www.cisco.com/cisco/web/support/index.html>

Debugging

Generate and examine logs to help debug your system. If you need additional assistance, contact the TAC.

A customer support representative might request that you create a Remote Support Account that the TAC can use to access your system.

[Logs](#)

[Remote Support Account](#)

Type	Log File
Audio (SIP Signalling)	\logs\ccapi
Core	\logs\core

Resources



Resources

CWMS Planning Guide

http://www.cisco.com/en/US/docs/collaboration/CWMS/b_planningGuide.pdf

CWMS System Requirements

http://www.cisco.com/en/US/docs/collaboration/CWMS/b_System_Requirements.html

CWMS Administration Guide

http://www.cisco.com/en/US/docs/collaboration/CWMS/b_administrationGuide.pdf

CWMS Release Notes

http://www.cisco.com/en/US/docs/collaboration/CWMS/b_Release_Notes.pdf

Single Sign On Material

<https://developer.cisco.com/web/webex-developer/sso-reference>

Q & A



Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 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 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.www

Cisco *live!*



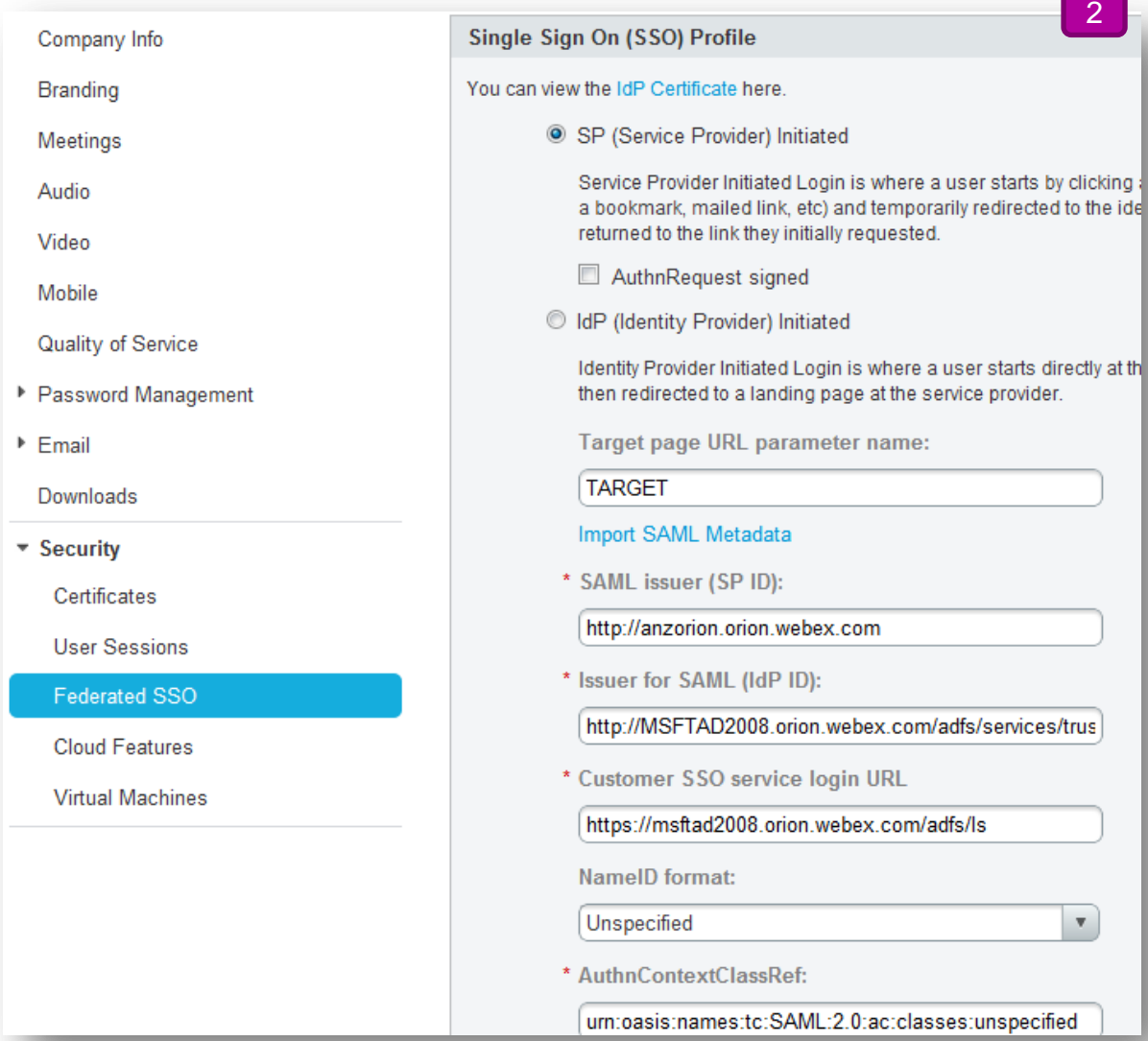
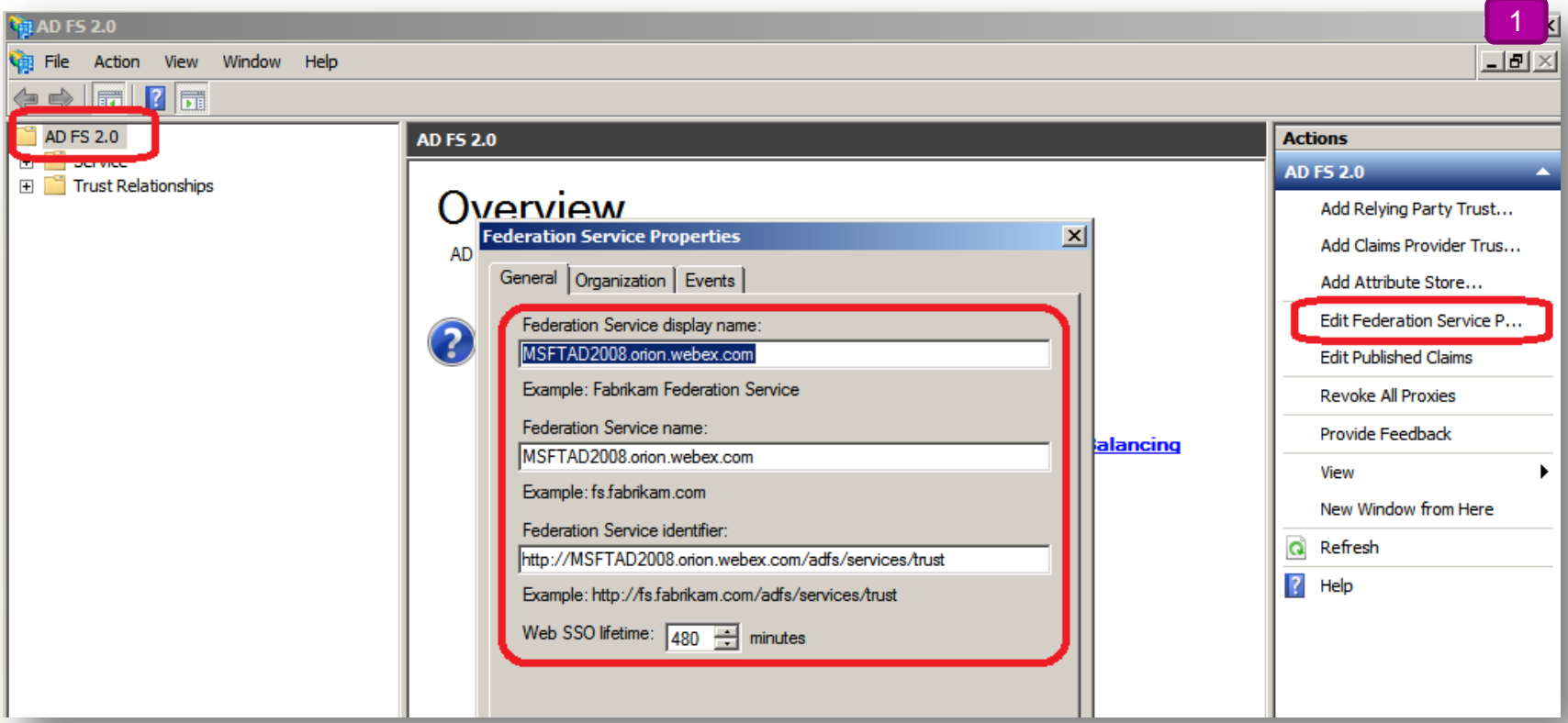
Appendix



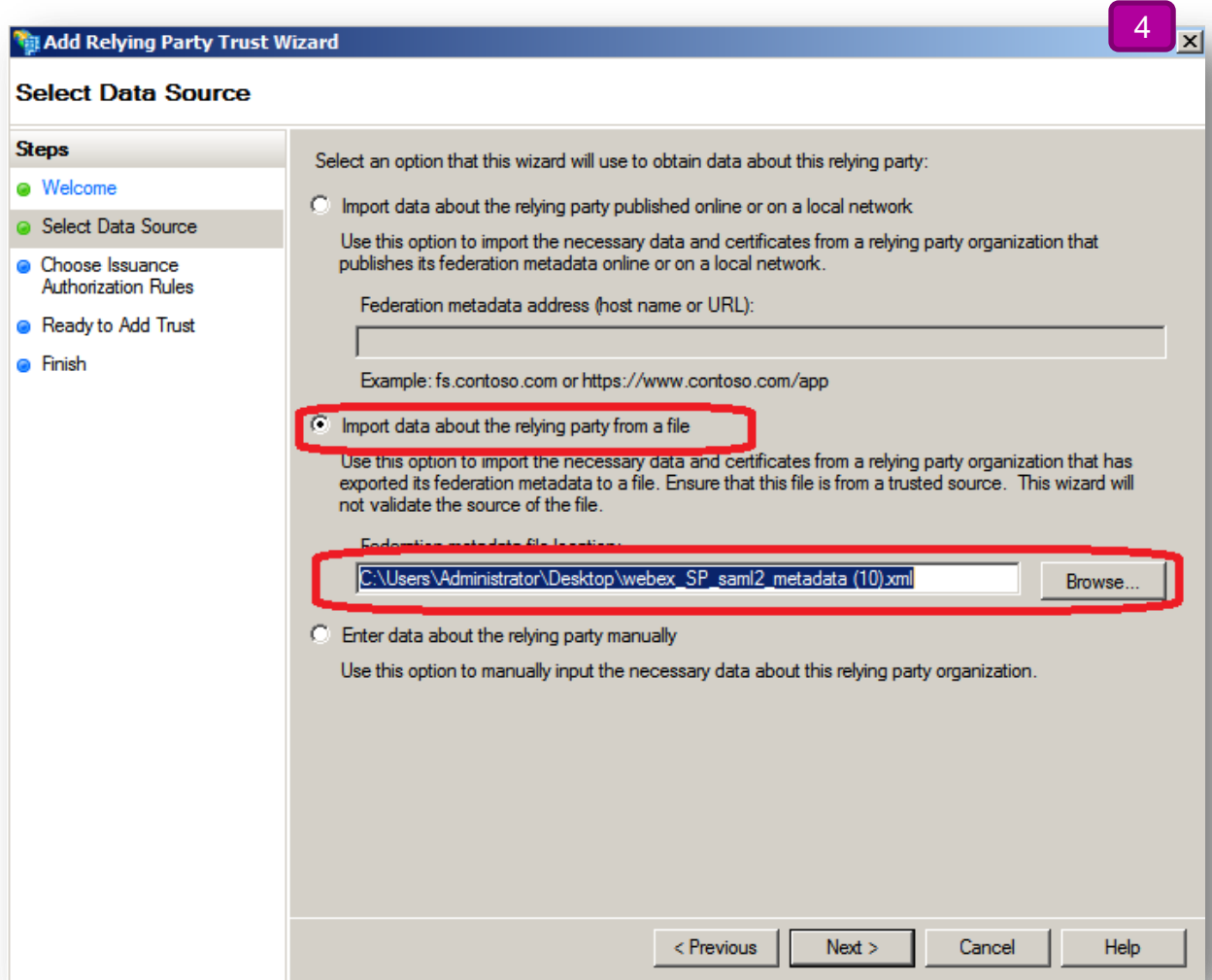
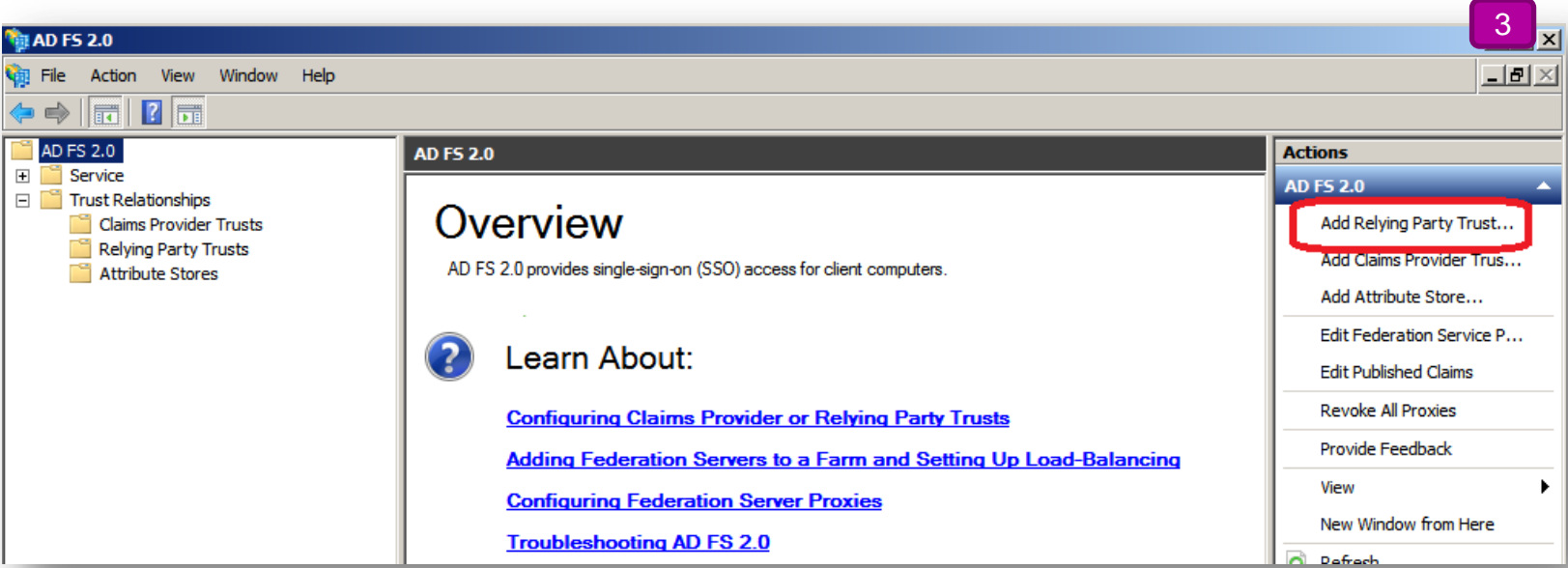
Single Sign On Details



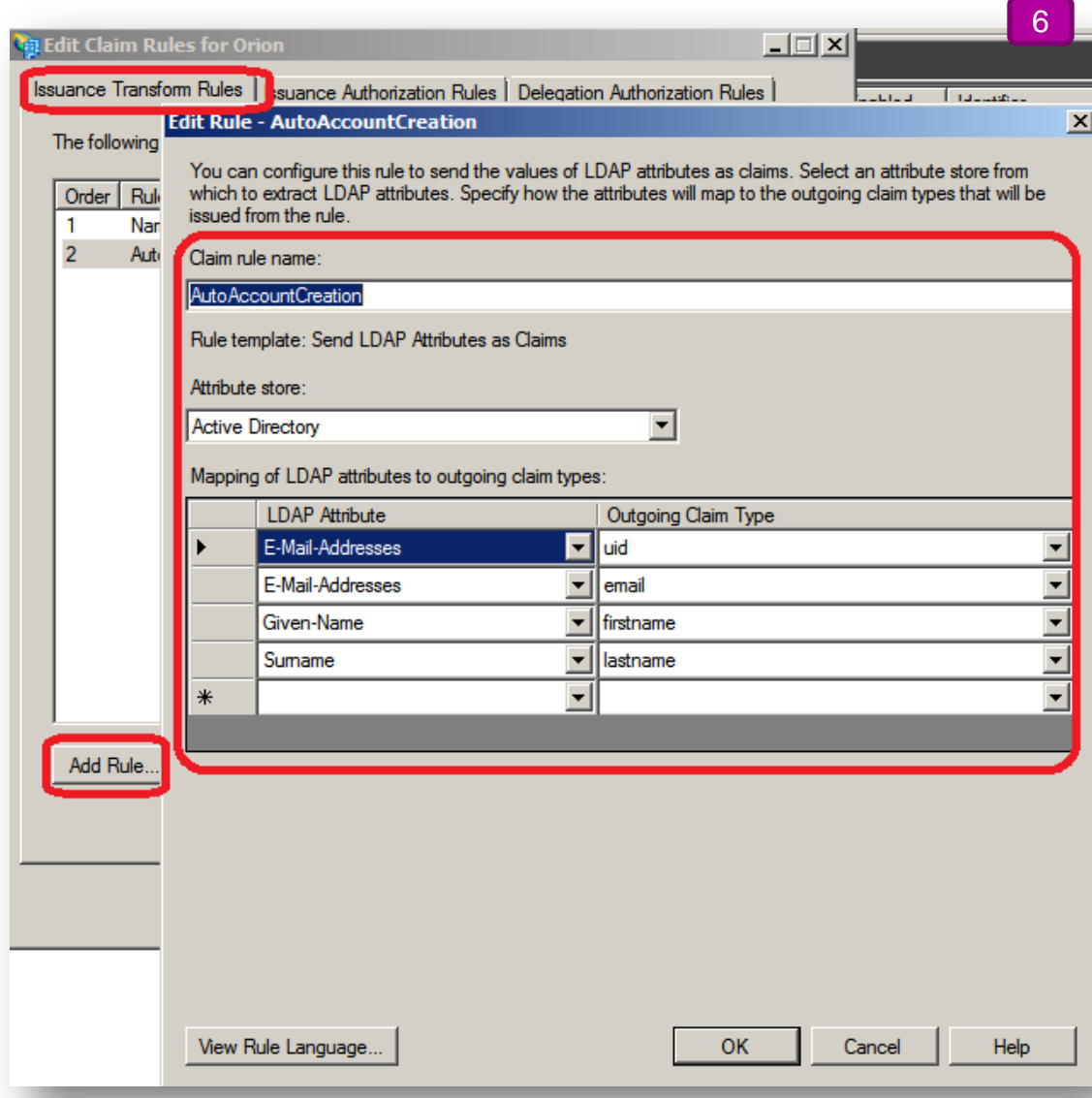
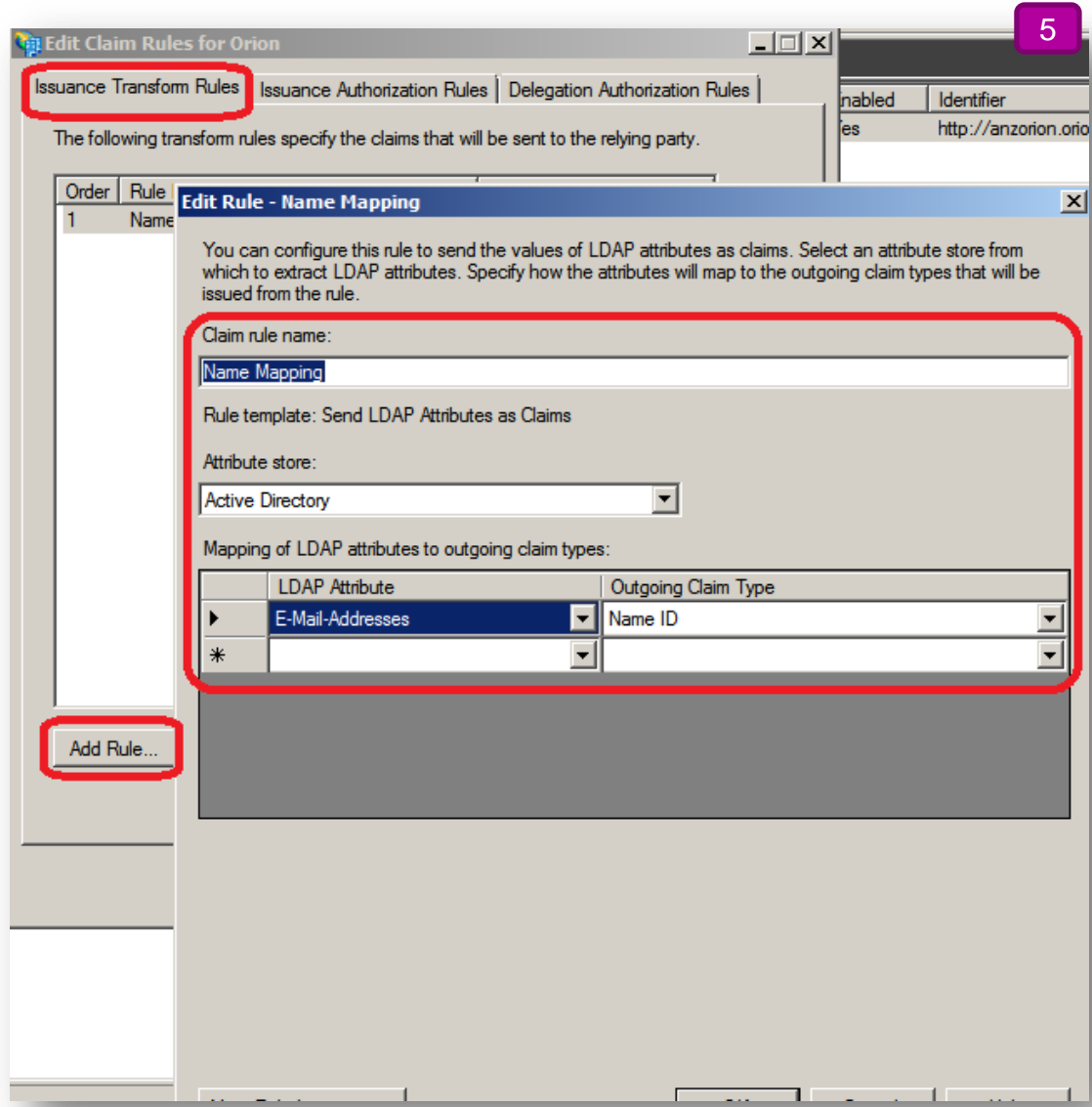
Enabling SSO for CWMS



Enabling SSO for CWMS



Enabling SSO for CWMS



Other – Details on SSO Outlook Plugin Authentication

- SSO Authentication
- WebEx productivity tools (Outlook Integration, One Click, etc) share a common Client Authentication Module (CAM)
- CAM opens a browser window to a customer-hosted authentication web page
- Customer's IDMS generates a SAML assertion and posts to WebEx Server
- WebEx Server authenticates and optionally provisions the user and returns a session ticket
- Productivity tools then collectively utilise the session ticket for subsequent XML API requests
- SAML 2.0 Assertion formats supported

Administration Portal

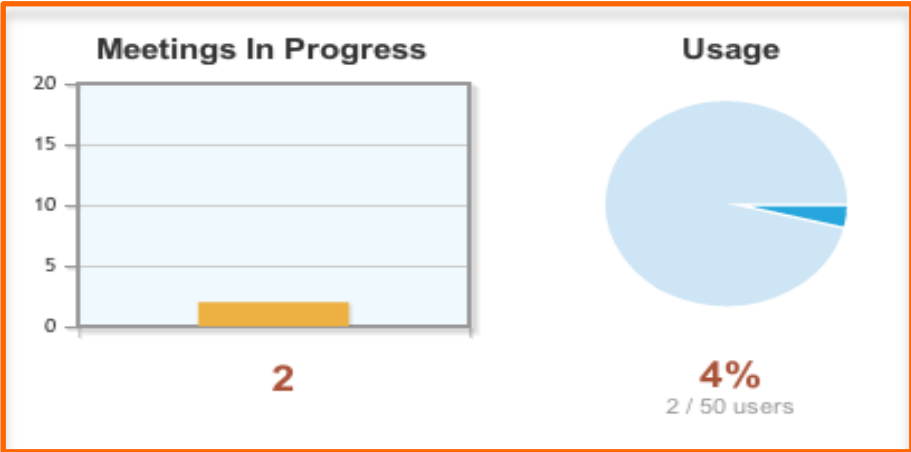


Administration Dashboard

System Monitor

Status: ● Good | Fri, Jun 22, 1:54:49 pm

Alarms



Displayed data reflects a delay of up to 5 minutes.

Processes	Status
Video	● Good
Audio	● Good
Web Sharing	● Good
Recording	● Good
Start/Join Meetings	● Good

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

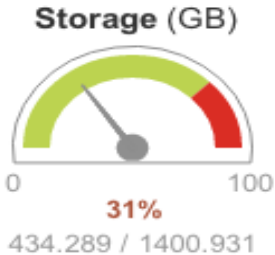
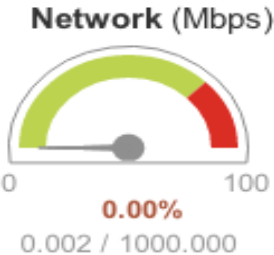
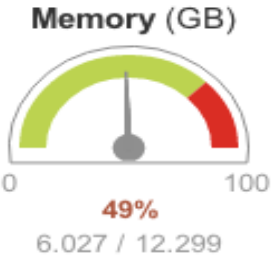
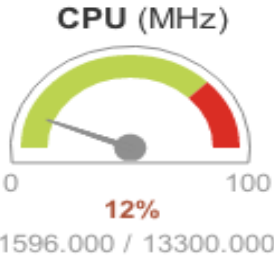
Next Backup: Jun 22, 2012 9:17 PM
[View More](#)

System

Size: 50 simultaneous users
Version: 1.0.0.1478.A
WebEx Site URL: orion-dev-vm43.cisco.com
User Licenses: Using 0 of 0
[View More](#)

Settings

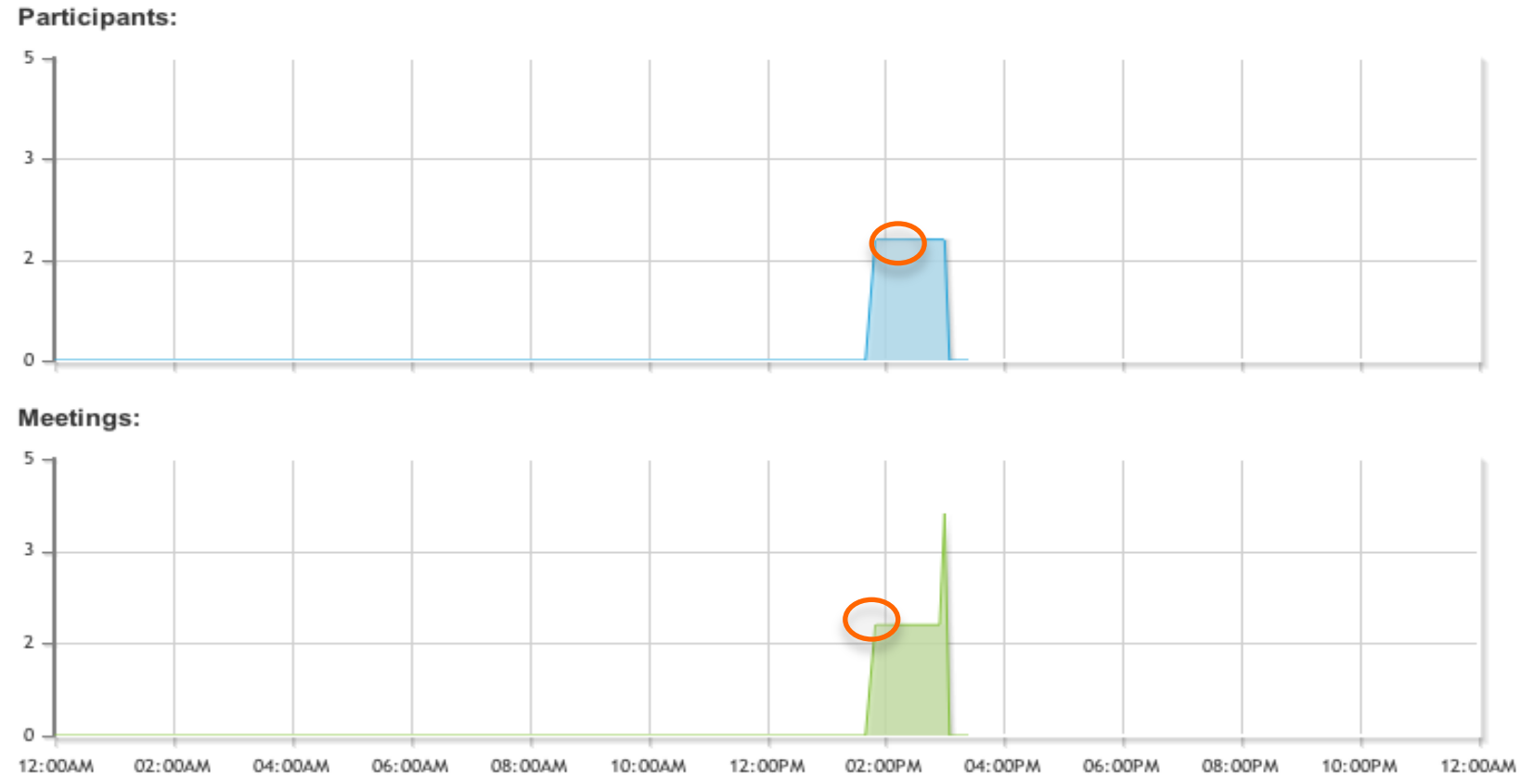
Maximum Participants per Meeting: 50
Audio: VoIP
WebEx HQ Video: Enabled
Mobile: Off
SSO: Disabled
[View More](#)



Meeting Trend

Dashboard » Meeting Trend

Meeting Trend



Current System Status:
● Good

CPU (MHz)
10%
1330.000 / 13300.000

Memory (GB)
43%
5.289 / 12.299

Network (Mbps)
0.00%
0.001 / 1000.000

Storage (GB)
31%
434.289 / 1400.931

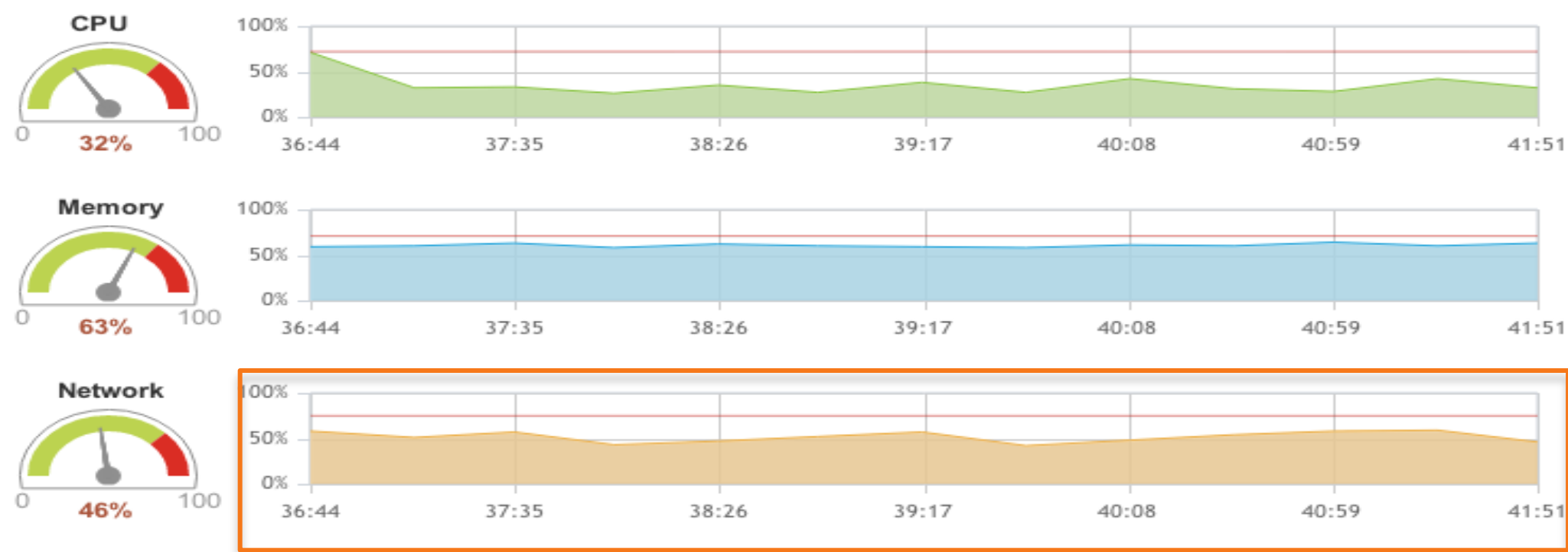
View: 1 day 1 week 1 month 6 months Fri, Jun 22 Show future scheduled meeting



Resource History

Dashboard » Resource History

Resource History



Current System Status:
● Good

Meetings In Progress
37
Usage (Meeting Participants)
96%
48 / 50 users

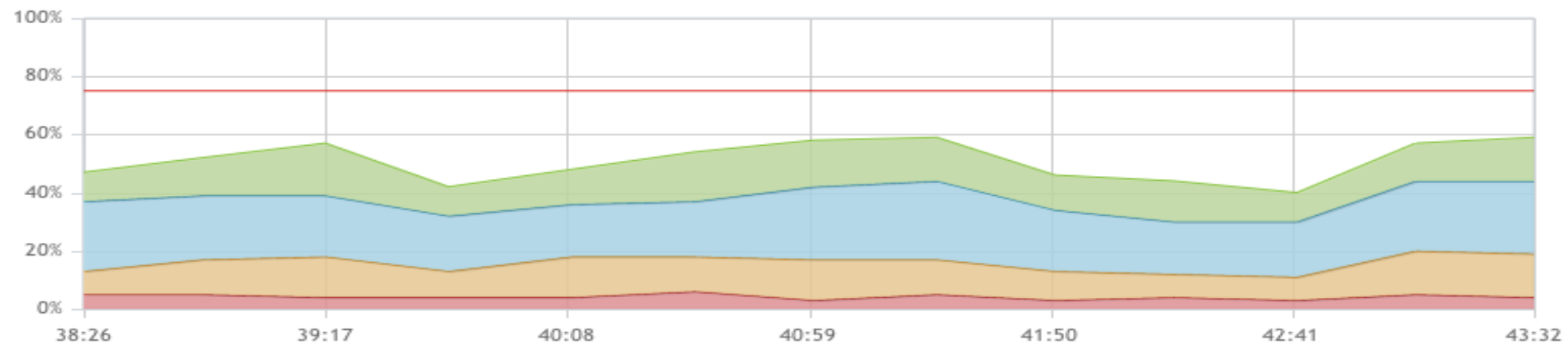
Storage (GB)
31%
434.289 / 1400.931



Network History

Dashboard » Resource History » Network History

Network History



VoIP: 4% Phone: 15% Web Sharing: 25% Video: 15%

Current System Status:
● Good

Meetings In Progress
37
Usage
(Meeting Participants)
96%
48 / 50 users

CPU (MHz)
36%
5984.998 / 16624.994
Memory (GB)
63%
8.400 / 13.333
Network (Mbps)
59%
590.000 / 1000.000

Storage (GB)
31%
434.289 / 1400.931



Storage History

Dashboard » Storage History

Storage History

Current Usage: 434.289 / 1400.931 GB (31%)

Mon, Jun 25, 9:53:08 pm



Refresh

Current System Status:
● Good

Meetings In Progress
0
Usage (Meeting Participants)
0%
0 / 50 users

CPU (MHz)
11%
1463.000 / 13300.000
Memory (GB)
60%
7.379 / 12.299
Network (Mbps)
0.00%
0.001 / 1000.000

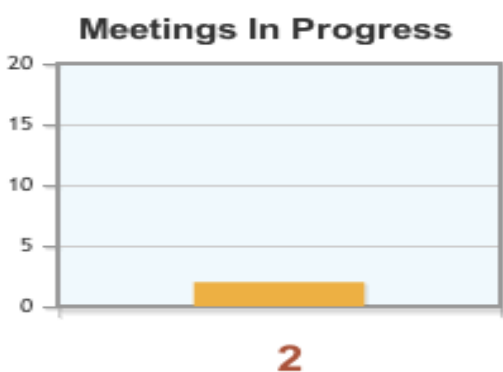


Administration Dashboard

System Monitor

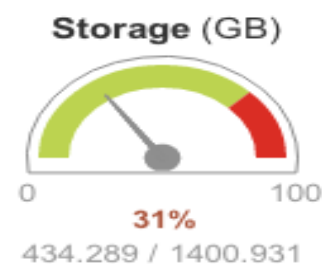
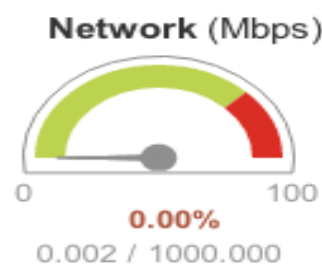
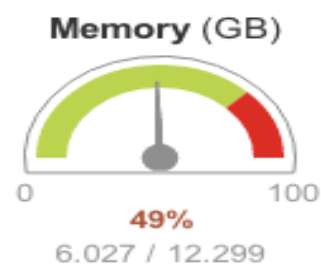
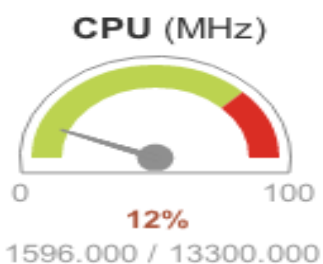
Status: ● Good | Fri, Jun 22, 1:54:49 pm

 [Alarms](#)



Processes	Status
Video	● Good
Audio	● Good
Web Sharing	● Good
Recording	● Good
Start/Join Meetings	● Good

 Displayed data reflects a delay of up to 5 minutes.



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](#)

System

Size: 50 simultaneous users
Version: 1.0.0.1478.A
WebEx Site URL: orion-dev-vm43.cisco.com
User Licenses: Using 0 of 0

[View More](#)

Settings

Maximum Participants per Meeting: 50
Audio: VoIP
WebEx HQ Video: Enabled
Mobile: Off
SSO: Disabled

[View More](#)

Alarm Thresholds

Cisco **webex** Administration Welcome, wgu@cisco.com | Sign Out | Reports | Support | Help

Dashboard Users System Settings Maintenance Mode

Dashboard » Alarms

Alarms

System status alarms are emailed to all administrators. You can enable or disable alarms, or change the settings.

Important: To keep the number of emails to a minimum, the system emails you the first time an issue is detected within the selected interval. [Learn More.](#)

	Edit
75% of meetings in progress are experiencing issues Interval: one hour	
Online meeting participants reach 75% of 50 users Interval: one hour	

Edit Alarm Thresholds in Percentage

Dashboard » Alarms » Edit

Edit Alarms

System status alarms are emailed to all administrators. You can enable or disable alarms, or change the settings. **Important:** To keep the number of emails to a minimum, the system emails you the first time an issue is detected within the selected interval. [Learn More.](#)

	Percentage %	Number #
<input checked="" type="checkbox"/> Meetings In Progress When meetings experiencing issues reach: Interval: <input type="text" value="one hour"/>	75% of meetings in progress	
<input checked="" type="checkbox"/> Usage When online meeting participants reach: Interval: <input type="text" value="one hour"/>	75% of 50 users	
<input checked="" type="checkbox"/> CPU When CPU usage reaches: Interval: <input type="text" value="one hour"/>	75% of 13300 MHz	
<input checked="" type="checkbox"/> Memory When memory usage reaches: Interval: <input type="text" value="one hour"/>	75% of 12 GB	
<input checked="" type="checkbox"/> Network When network bandwidth usage reaches: Interval: <input type="text" value="one hour"/>	75% of 1000 Mbps	
<input checked="" type="checkbox"/> Storage When storage usage reaches: Interval: <input type="text" value="one hour"/>	74% of 1400.931 GB	99%



Edit Alarm Thresholds in Number

Cisco **webex** Administration Welcome, wgu@cisco.com | Sign Out | Reports | Support | Help

Dashboard | Users | System | Settings | Maintenance Mode

Dashboard » Alarms » Edit

Edit Alarms

System status alarms are emailed to all administrators. You can enable or disable alarms, or change the settings.
Important: To keep the number of emails to a minimum, the system emails you the first time an issue is detected within the selected interval. [Learn More.](#)

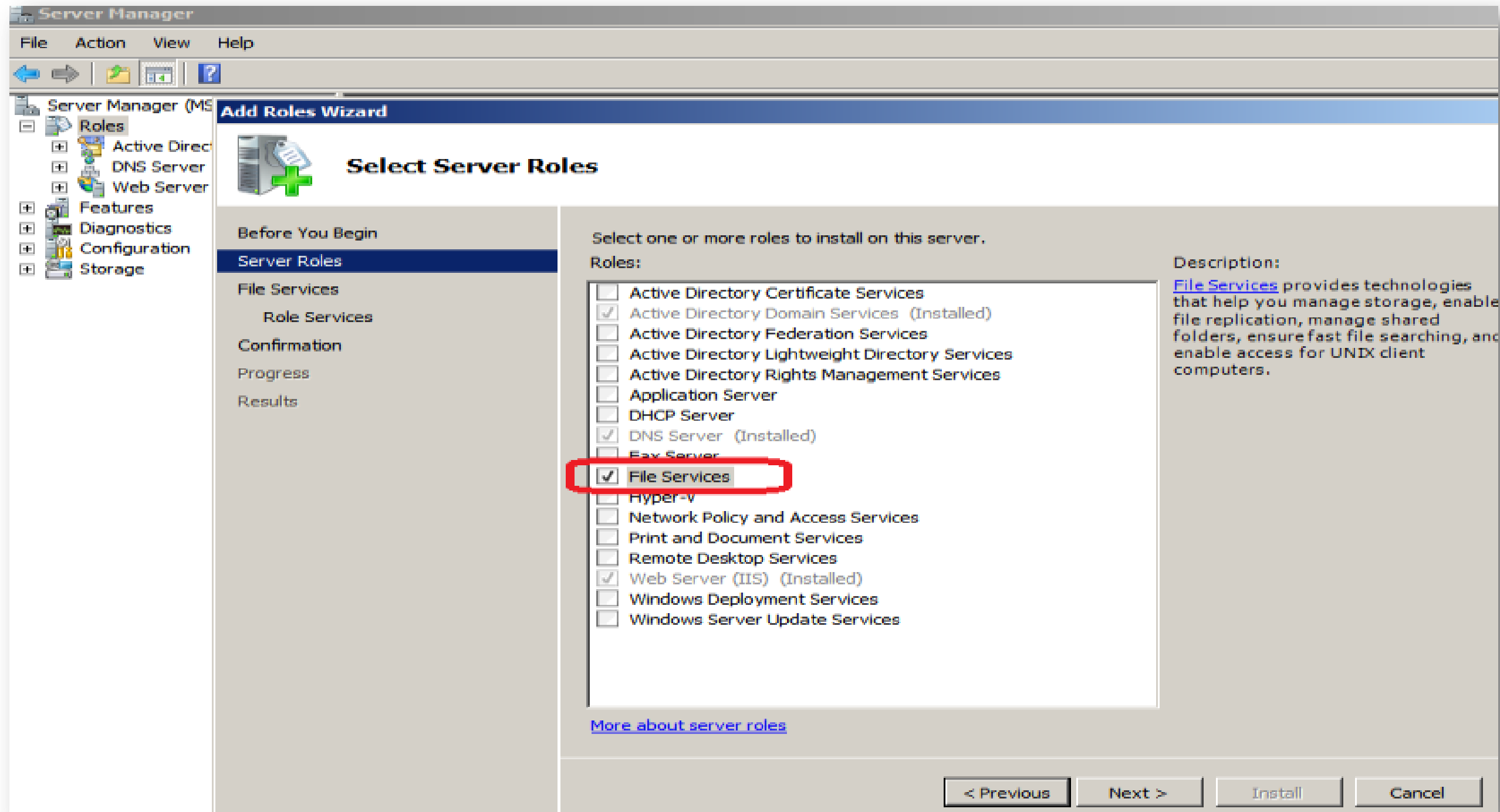
	Percentage %	Number #
<input checked="" type="checkbox"/> Meetings In Progress When meetings experiencing issues reach: Interval: one hour	75 % of meetings in progress	
<input checked="" type="checkbox"/> Usage When online meeting participants reach: Interval: one hour	37 users of 50 users	
<input checked="" type="checkbox"/> CPU When CPU usage reaches: Interval: one hour	9576 MHz of 13300 MHz	
<input checked="" type="checkbox"/> Memory When memory usage reaches: Interval: one hour	8 GB of 12 GB	
<input checked="" type="checkbox"/> Network When network bandwidth usage reaches: Interval: one hour	750 Mbps of 1000 Mbps	
<input checked="" type="checkbox"/> Storage When storage usage reaches: Interval: one hour	1036 GB of 1400.931 GB	



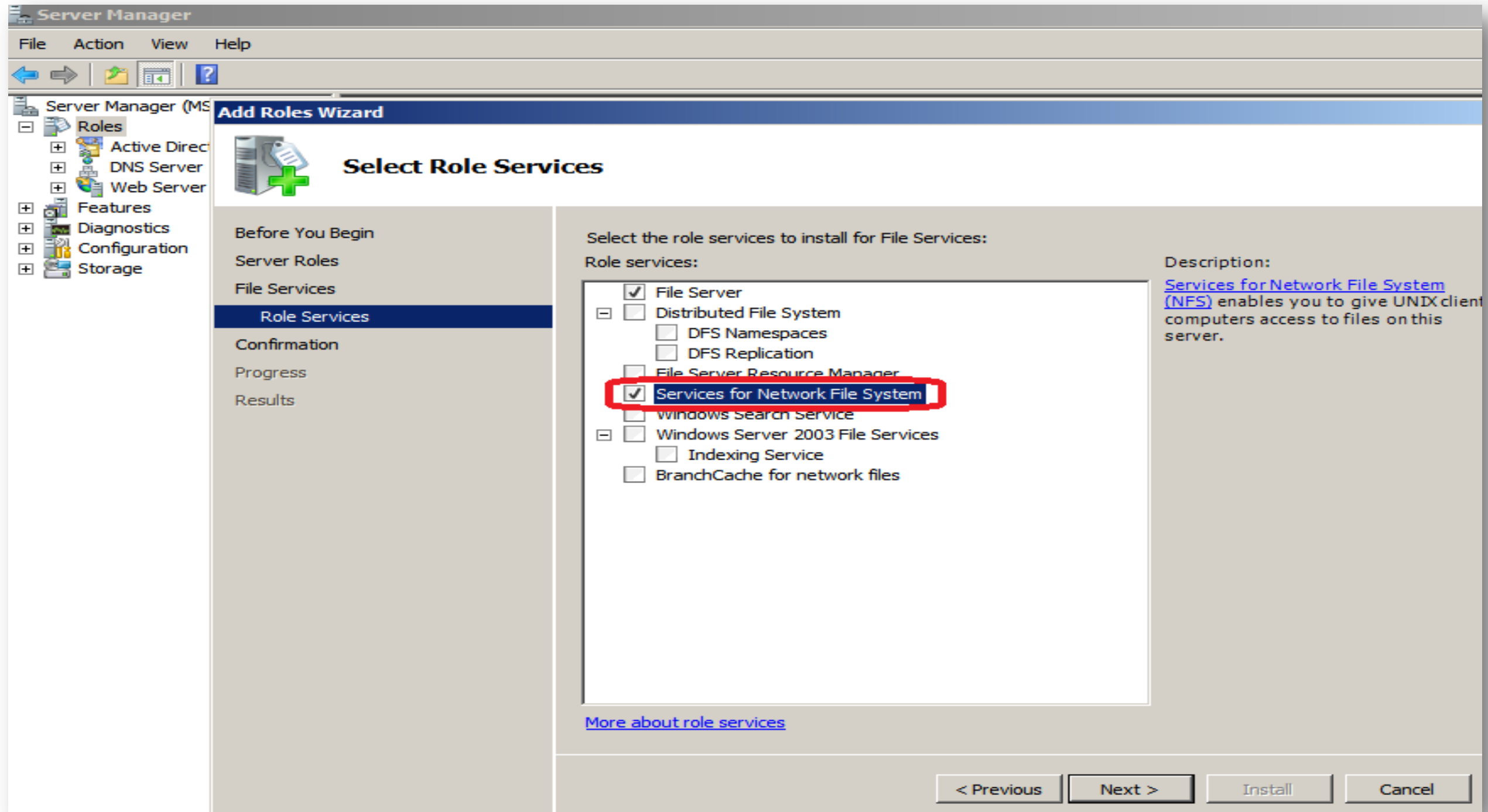
Setup Windows Server 2008 for NFS



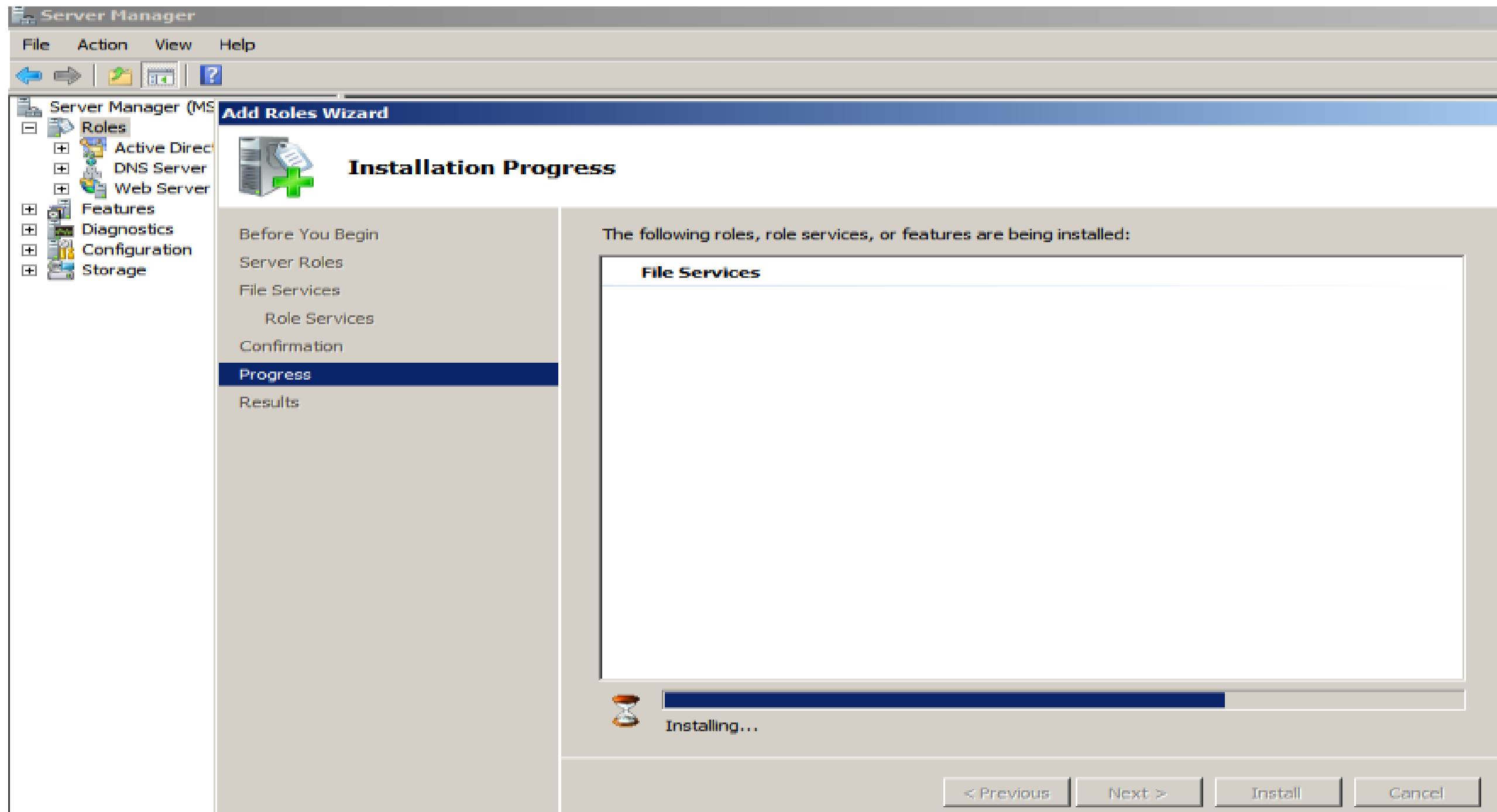
Server Manager Wizard



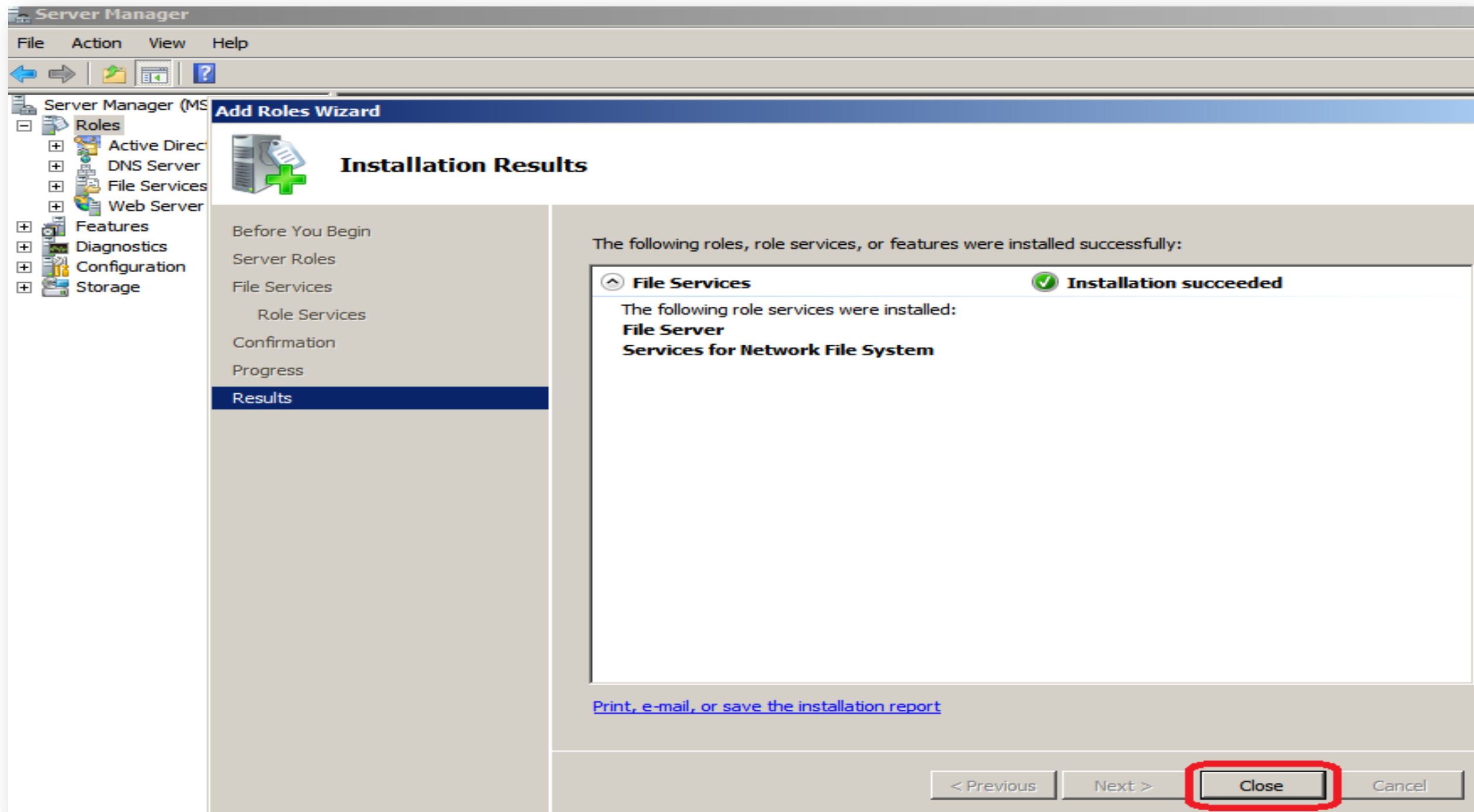
Server Manager Wizard



Server Manager Wizard

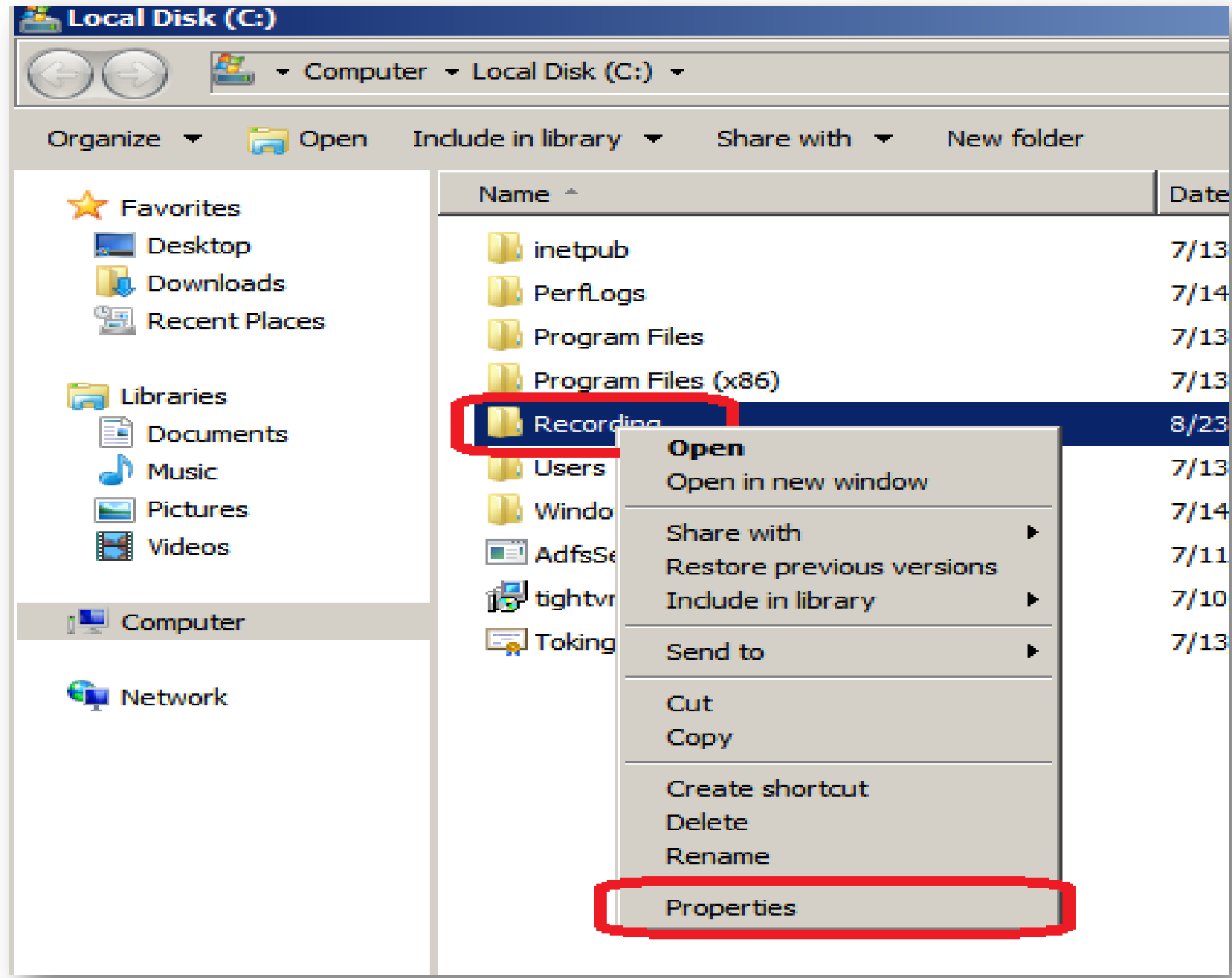


Server Manager Wizard

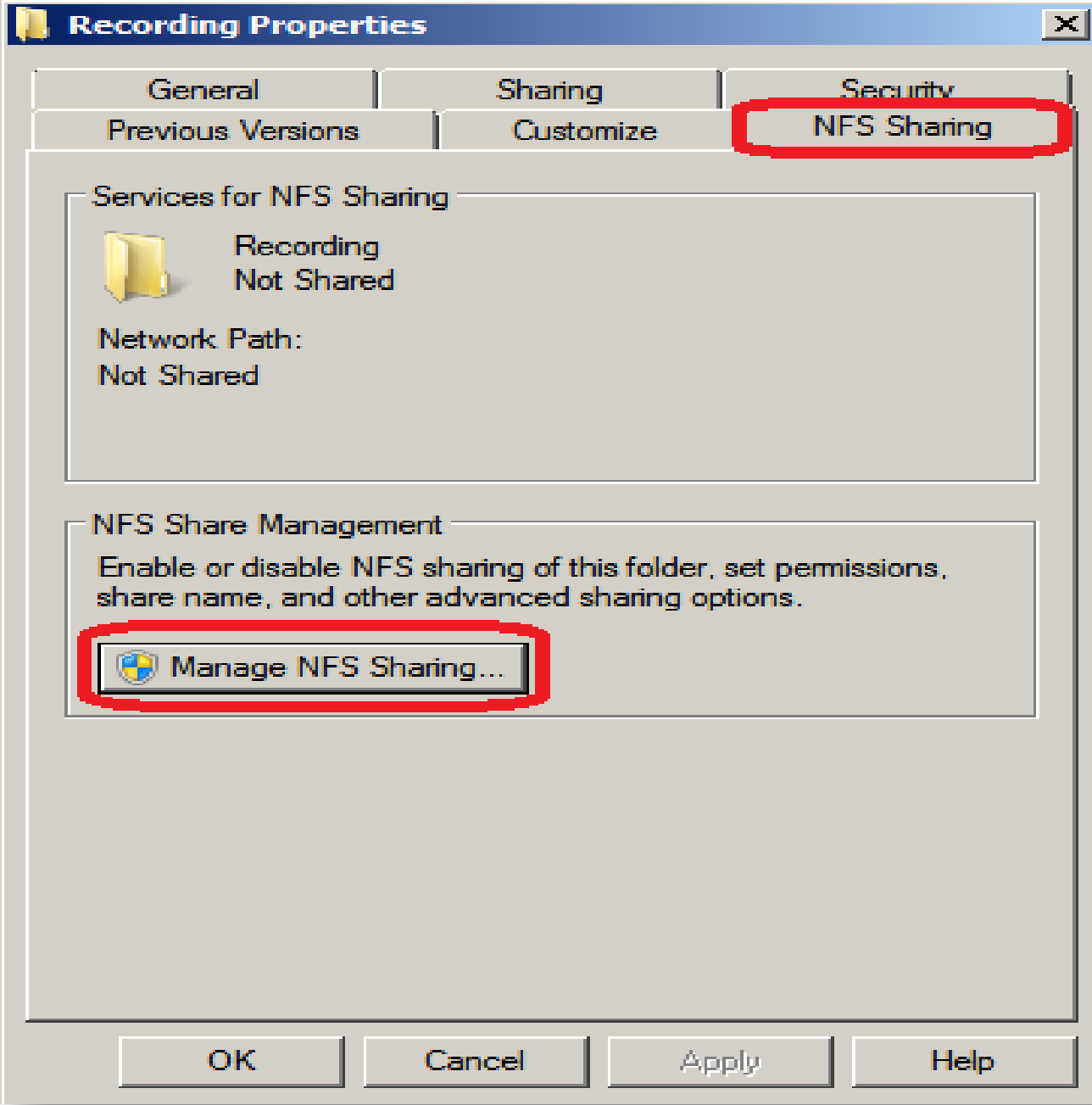
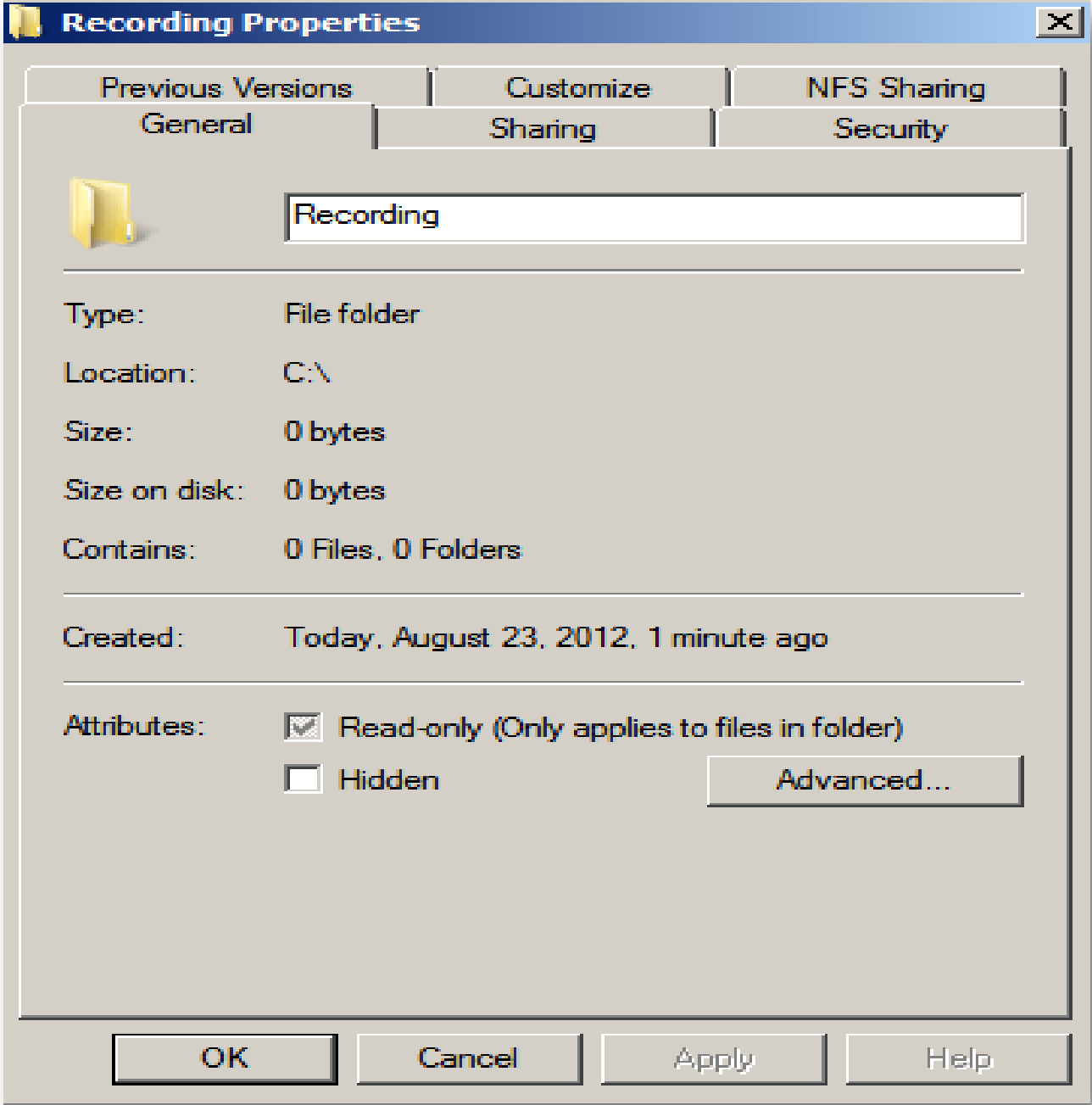


Folder Properties

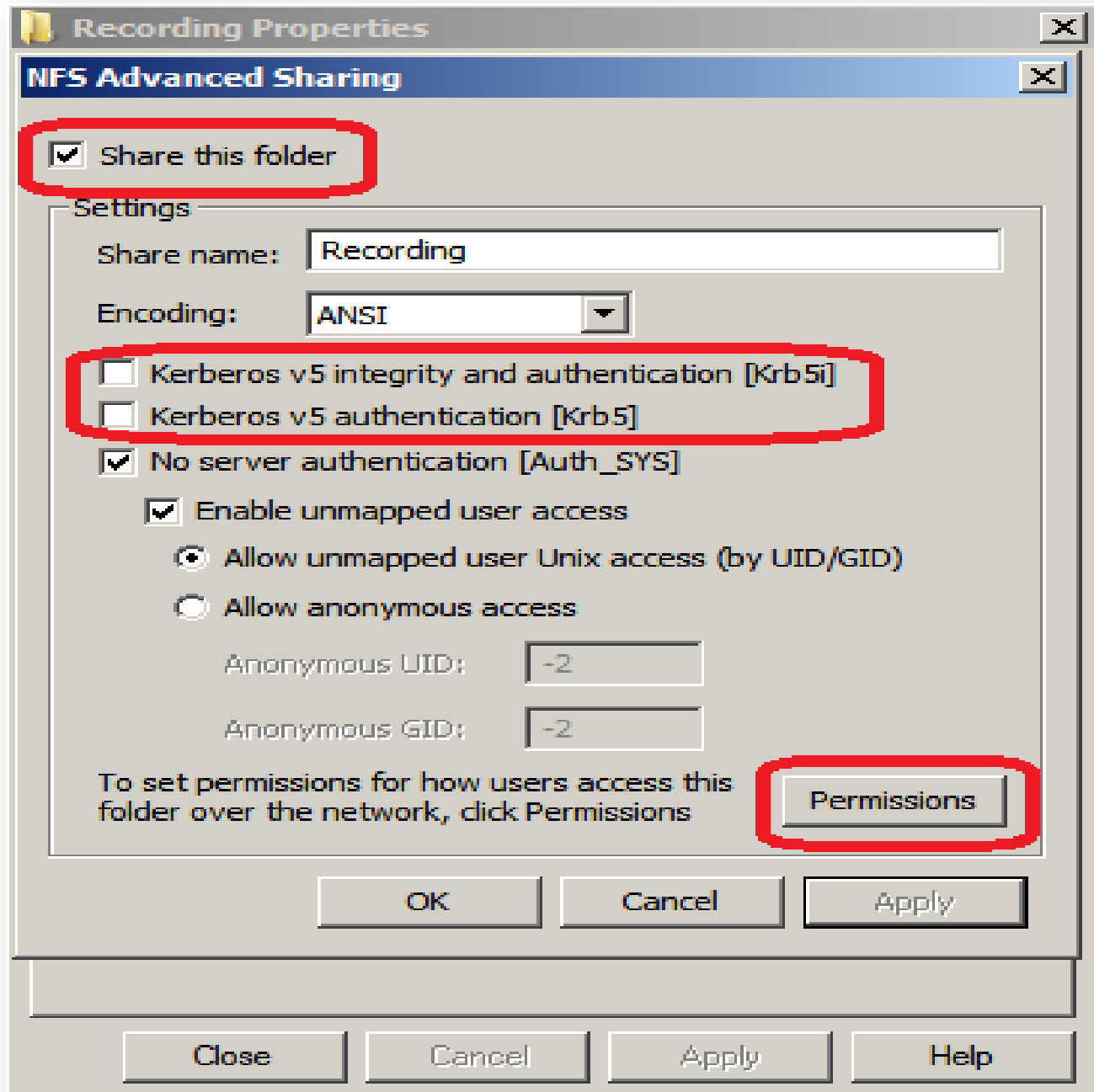
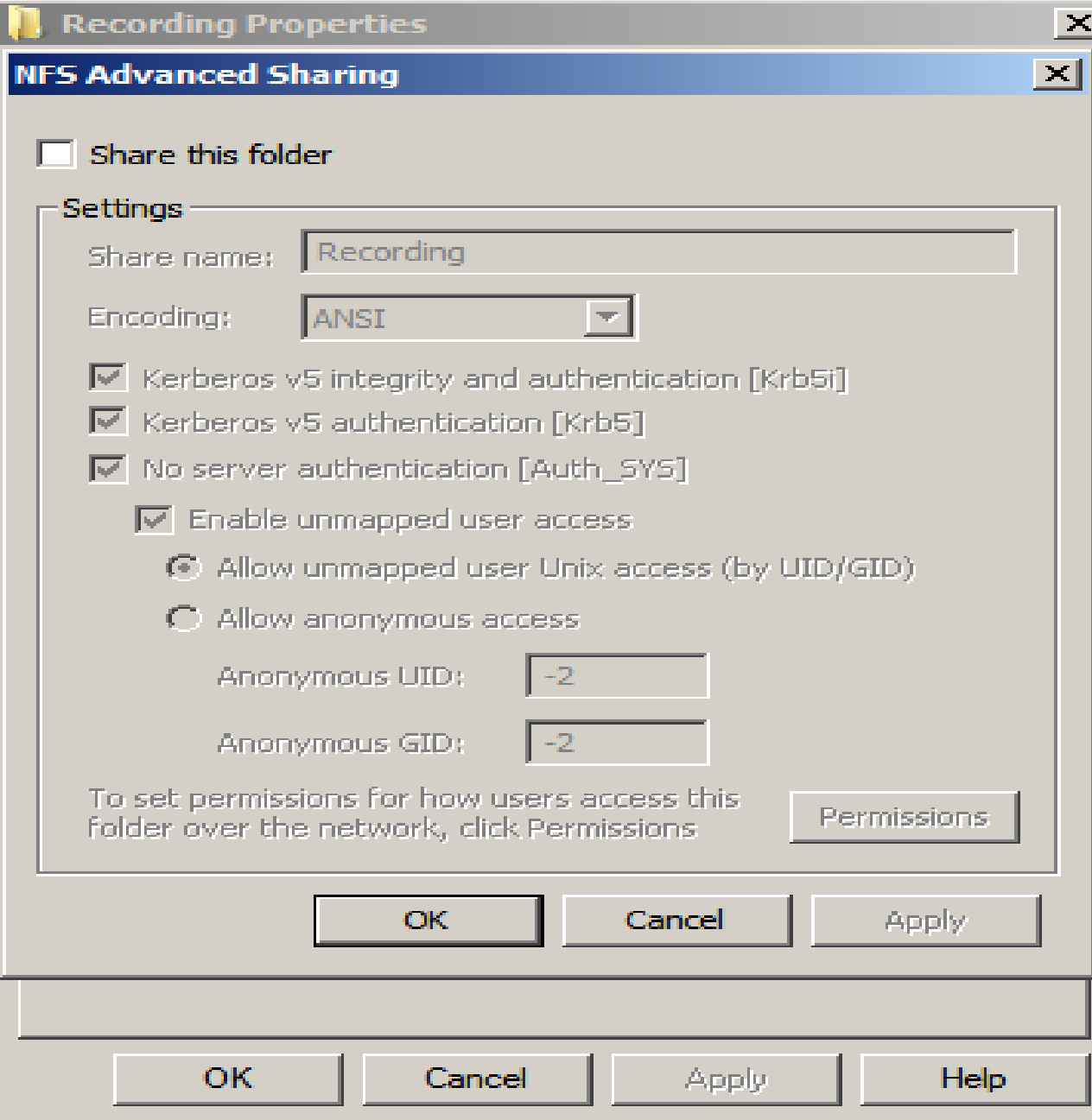
Create folder then right click



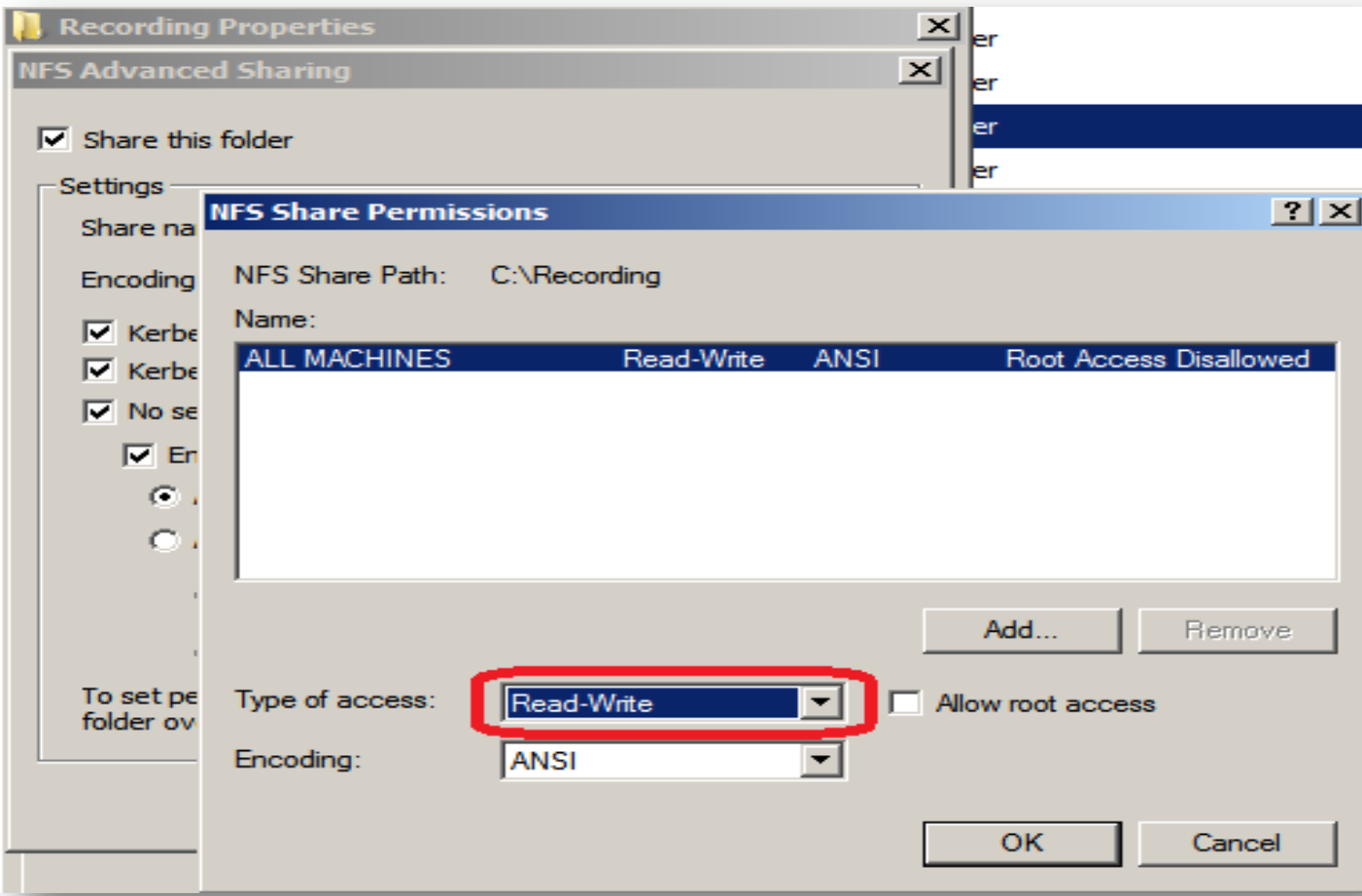
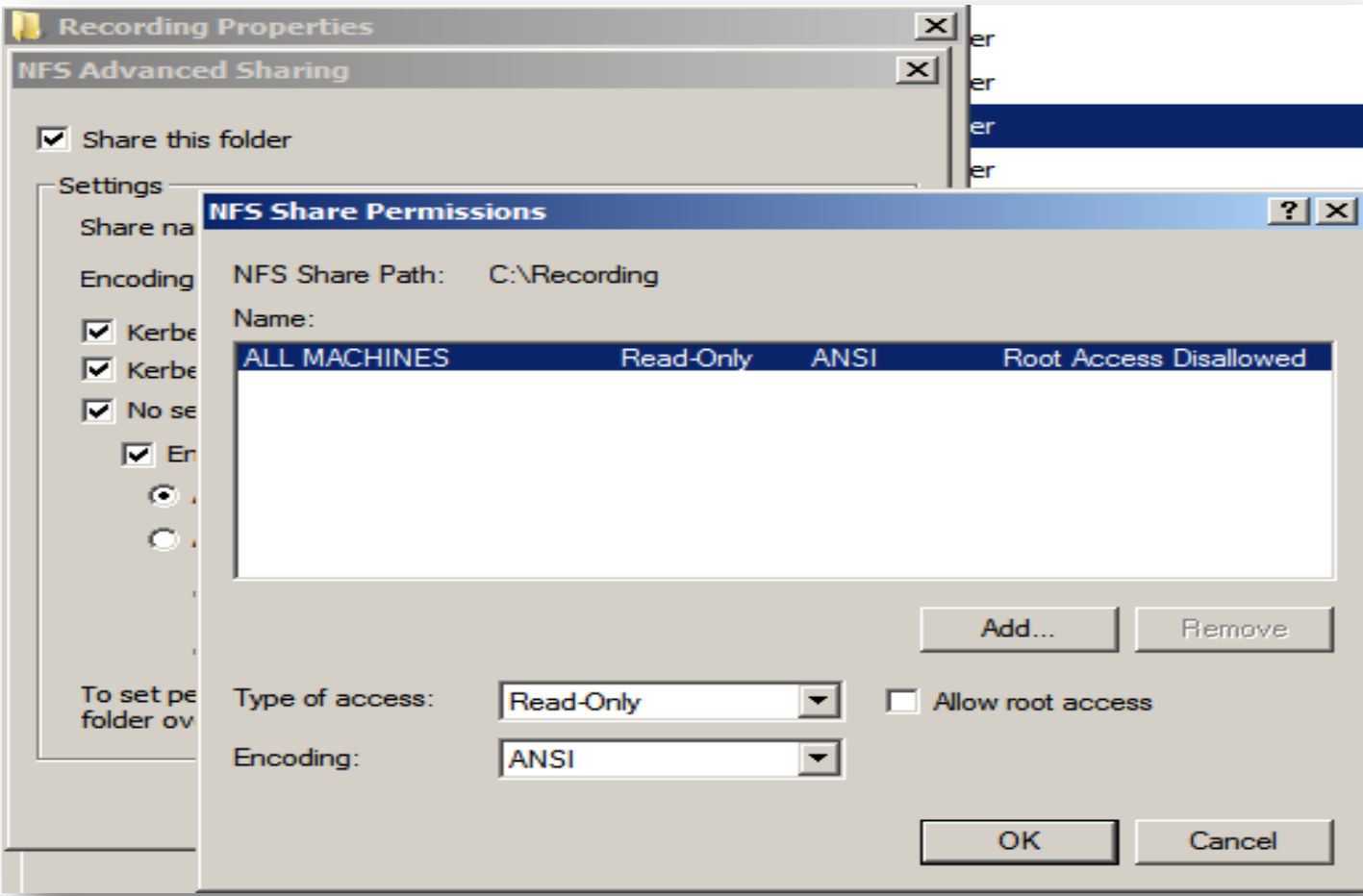
Folder Properties



Folder Properties



Folder Properties



Certificates



Types of Certificates

- Self-signed
 - Generated internally by the system at first launch
 - Recommended only for lab environments
 - Valid for 5 years
- Wildcard
 - Requested by CSR from external CA
 - Valid for all hosts within a single domain
- Subject alternative name (SAN)
 - Requested by CSR from external CA
 - All hosts in the system are listed in the certificate (except IRP hosts)

Wildcard vs. SAN

SAN

- Considered more secure
- Invalidated if system hosts change
- Complete system must be set up (including HA) for CWMS to be able to generate a CSR with all host names
- Can be used for systems with sub domains

Wildcard

- Considered less secure
- Valid if system hosts change
- More flexible
- Cannot be used for systems with multiple sub domains

When are Certificates Invalidated

- If any host names or URLs in the system change, the certificate is not valid for the new hosts
- SSL certificates can become invalid due to the following;
 - The system size expanded
 - The system has been upgraded
 - A high availability system has been added
 - The WebEx site URL changed
 - The Administration site URL changed
 - The FQDN of the Admin virtual machine changed
 - The current SSL certificate expired
- System generates a self signed SAN certificate with all new hosts
- Get new certificate or re-upload previous certificate, if still valid

Request Certificate Interface

The screenshot shows the 'Generate CSR' page in the Cisco Webex Administration console. The page title is 'Generate CSR (Certificate Signing Request)'. It features several input fields: 'Common Name' (with a dropdown menu showing 'vm54-meet.orion-sj.com'), 'Subject Alternative Names' (with a list of four domain names), 'Organization', 'Department', 'City', 'State/Province', 'Country' (set to 'United States'), and 'Key Size' (set to '2048'). At the bottom are 'Cancel' and 'Generate CSR' buttons. Three horizontal lines with circles and arrows point to the 'Common Name' dropdown, the 'Subject Alternative Names' list, and the 'Organization' field. To the right of these lines are the annotations: 'Select SAN or wildcard', 'All SANs currently in the system', and 'Remaining fields are optional'.



