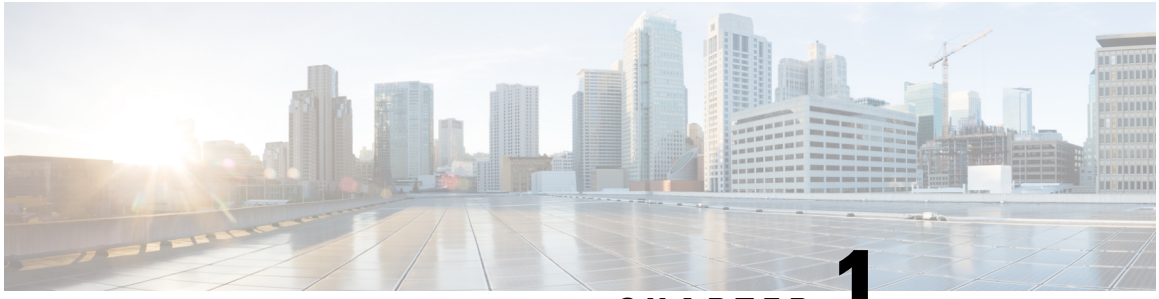
Planning Guide and System Requirements for Cisco Webex Meetings Server Release 4.0

First Published: 2019-04-29

Last Modified: 2021-06-10

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

CONTENTS



CHAPTER 1

Webex System Requirements

General System Requirements

Cisco Webex Meetings Server (CWMS) is compatible with Cisco UCS servers that meet or exceed the specifications presented in this section.

Important When you perform an *upgrade* to a major release of CWMS, such as to Release 2.0 or Release 2.5 from Release 1.x, the ESXi hosts (Cisco UCS server) where the Admin virtual machine is located require a minimum of 1.5-TB of free disk space. Refer to the section in this document that describes the different size user systems that begin with the 50-user System, on page 10. During an upgrade, there are two sets of virtual machines on your network at the same time; the *original* virtual machines running Release 1.x and the *upgrade* virtual machines to support the new release. For more details, see the "Upgrading the System" section in the CWMS Administration Guide at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Module	Requirements Notes
Host server and processors	• Cisco UCS *C-series* rack server or equivalent *B-series* blade server. • AES-NI instruction set support. • 2.4 GHz or faster processor clock speed. **Note** Third-party hardware is not supported.
Network interfaces The NICs between the ESXi hosts (for the Cisco Webex Meetings Server virtual machines) and the Ethernet switch (not to the external network interface).	• Minimum 1 physical NIC for a non-redundant configuration. See the 50-user System, on page 10 section for special requirements where the Internet Reverse Proxy (IRP) and Admin virtual machine are sharing a host. • Redundant configurations must have all NIC interfaces duplicated (*teamed* or *bonded*) and connected to an independent switching fabric. • An additional NIC for the VMware management network (optional).
[1]Internal (DAS) Storage for ESXi hosts where internal virtual machines are deployed	• Minimum of 4 drives in a RAID-10 or RAID-5 configuration • Minimum of 2.5 TB usable storage for new system deployments or upgrades. • When you upgrade CWMS, the ESXi hosts each require from 300 to 1759 GB free disk space. The requirement depends on the size of your system and the virtual machines. For more information, see Minimum Hardware Requirements, on page 7. • Optional second array for ESXi **Note** The virtual machines must use thick provisioning for storage.
Internal (DAS) storage for ESXi hosts where IRP virtual machines are deployed	• Minimum of 2 drives in a RAID-1 configuration • Minimum of 600-GB usable storage • Can use the same configurations as for the internal virtual machines **Note** The virtual machines must use thick provisioning for storage.

Module	Requirements Notes
SAN storage	• Can be used as a substitute for DAS. (We recommend allocating of the same amount of storage space.) • B-series blade servers have only two hard disk drives. If you are using Cisco UCS B-series blade servers, upgrading requires the use of SAN storage. SAN storage meets the requirement to have 4 hard disk drives in either a RAID 5 or RAID 10 configuration. • Recommended only for deployments where the support staff has experience monitoring and tuning SAN performance. **Note** You take responsibility for adding storage for new VMware requirements and future growth of the system. • Fiber Channel (FC) or Fiber Channel over 10-GB Ethernet (FCoE) only. • Performance requirements are the same as for DAS.
Hypervisor	ESXi versions and vSphere licenses are described in the Minimum Hardware Requirements, on page 7 section. VMware Vsphere is required and the only product supported; other hypervisor products are not supported. One VMware license per processor socket. For more information about vSphere licenses, see Minimum Hardware Requirements. VMware vCenter Server or vCenter Server appliance versions: 6.0, 6.5, 6.7 and 7.0. Coresidency: • vCenter can be coresident with CWMS, providing the processor and memory requirements are added to the system requirements. • vCenter coresident configurations are supported only for 50-user and 250-user systems. • Coresidency with Cisco Unified Communications products on the same physical ESXi host is not supported. • Coresidency with non-CWMS virtual machines on the same physical ESXi host is not supported. Advanced VMware vSphere features such as Distributed Resource Scheduler (DRS), Cloning, Fault Tolerance (FT), and vMotion or Storage vMotion are not supported.

Module	Requirements Notes
Email server	• Fully qualified domain name (FQDN) of the mail server that the system uses to send emails. • Port number—default value of the SMTP port number is 25 or 465 (secure SMTP port number). • To use a TLS-enabled email server with third-party certificates, you must import the certificates into your system. For more information, See "Managing Certificates" in the administration guide at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.
Licenses	MDC licenses—An MDC license is required for each data center in a multi-data center system. A MDC license is not required for a system with a single data center. Host license—Each user that shall host a meeting must have a Host license to start a Webex Web, Webex Audio, Blast Dial meeting, or Personal Conferencing. For more information about Host licenses, see About Host Licenses, on page 162.

[1] If your organization has expertise in managing a storage area network (SAN), we recommend SAN over direct attached storage (DAS). SANs can be more reliable than local disk arrays.

Cisco Unified Communications Manager Requirements

Cisco Unified Communications Manager (CUCM) supports TLS 1.1 and later; TLS 1.0 is not supported, with one exception. Client connections from Cisco Webex Meetings Server (CWMS) to an SMTP server using TLS 1.0 are supported.

This release supports CUCM 8.6 or 9.0 without TLS/SRTP. For secure teleconferencing, this release supports the following CUCM releases:

- 9.1
- 10.0 and 10.5
- 11.0(1a), 11.5(1)SU1, 11.5(1)SU3, 11.5SU5, 11.5SU6, 11.5SU7, and 11.5SU8.
- 12.0, 12.0SU2, 12.5, 12.5SU2, and 12.5(1)SU1

Cisco Webex Meetings Server Best Practices

The following is a list of best practices that you should refer to when configuring and maintaining your Cisco Webex Meetings Server system:

- Use an uninterruptible power source (UPS) to minimize power interruptions to your virtual machine hosts. Repeated power failures can damage host systems and virtual machines.
- Always put your system into maintenance mode before shutting down a guest operating system.

- For scheduled events and other situations that require a system shutdown, gracefully shut down your virtual machines by shutting down the guest operating system.
- The system is designed to repair itself when necessary and rebooting can interrupt this process. We do not recommend that you reboot your system to fix it. If your system is in an unhealthy state, contact the Cisco TAC. Power off your system only when instructed to do so or during scheduled events such as data center maintenance.
- Configure network redundancy to minimize network failures. Refer to "Adding a High Availability System" in the *Cisco Webex Meetings Server Administration Guide* for more information.
- Using snapshots on your virtual machines can impair system performance in ways that affect user experience even when the system is otherwise lightly loaded.
- If your system is having problems, make sure that you check your VMware VCenter environment to determine if conditions in VCenter or the network are causing the problem.
- Configure high availability to increase the probability that your system can continue to operate if a failure occurs.
- If you have a high-availability system and your secondary system fails, you can repair it by removing the existing secondary system (refer to "Removing a High Availability System" in your *Cisco Webex Meetings Server Administration Guide*) and adding a new secondary system (refer to "Adding a High Availability System" in your *Cisco Webex Meetings Server Administration Guide*). If the primary system on a high-availability system fails, you cannot repair it using this procedure. We recommend that you restore your primary system using the disaster recovery procedure and then add a new secondary system. Until you add a new secondary system your deployment is operating without full redundancy. This procedure helps prevent unplanned outages if any of your secondary virtual machines fails. Refer to "Using the Disaster Recovery Feature" in the *Cisco Webex Meetings Server Administration Guide* for more information.
- Since your system only keeps the latest system backup on the NFS and removes previous instances every day, we recommend that you keep several recent backups on other media.

Restriction Do not manually create files or directories in the NFS share used by Cisco Webex Meetings Server, as it runs various scripts on NFS files and directories. The NFS storage server must be for the exclusive use of Cisco Webex Meetings Server.

- Use your dashboard to monitor the health status of the NFS, CPU, and storage. We recommend enabling dashboard alarms for storage and CPU.
- If you plan to use directory integration, refer to the Configuring Directory Integration section in the "Managing Users" chapter of the *Cisco Webex Meetings Server Administration Guide* for more information.
- When using Cisco Webex Meetings Server, the related SIP trunk on CUCM in the CallManager service interface should have the **Media Termination Point Required** check box unchecked on the **Trunk Configuration** page. See Configuring a SIP Trunk on a Load Balance Point, on page 102 and Configuring a SIP Trunk for an Application Point, on page 103 for more details.
- If you are running Cisco Webex Meetings Server Release 2.0 or higher and using B-series blade servers, you are required to use SAN storage to fulfill the hard drive requirements. See General System Requirements, on page 1 for more information about SAN requirements.

Webex Meetings Desktop Application

With the Cisco Webex Meetings Desktop Application, users can schedule, start, and join meetings without going to the Webex site. The latest version is available from Webex Administration, **Settings** > **Downloads**.

Users

The system supports a lifetime maximum of 400,000 user accounts. This number represents the total of both active and deactivated user accounts. This lifetime maximum number is large enough to accommodate expected growth in the user database.

Administrators cannot delete users from the system. Instead, users are deactivated. This design enables administrators to reactivate previously deactivated user accounts, even after long periods of user inactivity. The user's meetings and other content (including recordings) are restored.

Deployment Sizes For Your System

When determining the size for your system, consider how many users you expect to be using the system at any given time. For example, in a 50-user system the maximum number of users concurrently attending meetings is 50. If more than 50 users attempt to join a meeting, an error messages displays for all users who attempt to join a meeting after the maximum number of users is exceeded, and the system prevents these users from joining the meeting.

- 50-user System, on page 10
- 250-user System, on page 12
- 800-user System, on page 14
- 2000-user System, on page 17

Here are some things to consider when determining the size for you system:

- Determine the largest number of users you anticipate will join a meeting at any given time, including rare or unusual occasions.
- You can expand the system size to a larger size at any time as long as your hardware meets or exceeds the minimum requirements for the larger size system; otherwise, you must purchase additional hardware.
- If you plan to add High Availability (HA) or a Multi-data Center (MDC) to your system, include the additional virtual machines necessary to support the HA or MDC system, when you purchase your hardware.

Requirements for vCenter Co-residency

VMware vCenter Server or vCenter Server Appliance can reside with other virtual machines or with Cisco WebexLar Meetings Server (CWMS) virtual machines in some instances.

On a 50– or a 250–user system, VMware vCenter can reside on the same host with CWMS. However additional RAM must be installed with the Cisco UCS server. For the exact amount of RAM required, see the requirements for that system size in Minimum Hardware Requirements.

Virtual Machines In Your System

These are the virtual machines created for your system. Some functions are combined into one virtual machine for the smaller system sizes.

- Admin—*Heart node* of the system. Includes the system database and provides administrative functions.
- Media—Provides media services (audio-video function, telephony and meetings services).

  Included in the Admin virtual machine in a 50 concurrent users system.
- Web—Provides web services (meeting list and recordings). Enables the user to schedule future meetings.

  Included in the Admin virtual machine in a 50, 250 or 800 concurrent users system.

  End users sign in to the Webex web site. Administrators sign in to the Administration web site.
- Internet Reverse Proxy (IRP)—Provides public access, enabling users to host or attend meetings from the Internet and mobile devices. The Internet Reverse Proxy is required for your mobile workforce to attend meetings.

Note Only the IRP provided with this product may be used in this system. Internet Reverse Proxies or web load balancers, supplied by other vendors, are not supported. The IRP provided with this product is optimized for handling real-time web, audio, and data-sharing traffic from external users joining meetings from the Internet.

Note In this documentation, we use the term *internal virtual machines* to refer to the Admin virtual machine, and if applicable, to the Media and Web virtual machines.

The IRP is situated in the DMZ network (non-split-horizon and split-horizon network topologies) or in the internal network (all internal network toplogy).

- Non-Split-Horizon Network Topology, on page 39
- Split-Horizon Network Topology, on page 42
- Internal Internet Reverse Proxy (IRP) Network Topology, on page 38

Minimum Hardware Requirements

This section lists some of the Cisco UCS servers you can use for each size system. For specific requirements for each system, see the following topics:

- 50-user System
- 250-user System
- 800-user System
- 2000-user System

Table 1: ESXi Versions and License Types

System Size	ESXi Version	vSphere License Type
50 or 250	5.5, 6.0, 6.5, and 6.7	Standard Edition, Enterprise Edition, Enterprise Plus Edition
800 or 2000	5.5, 6.0, 6.5, and 6.7	Standard Edition, Enterprise Edition, Enterprise Plus Edition

Table 2: Host Models

Deployment Size	Example of UCS Model
50 Users	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
250 Users	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
800 Users	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 (2.0 and higher)
2000 Users	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 (2.0 and higher)

Co-residency with vCenter is supported with 50- and 250-user system deployments only. Co-residency with Cisco Unified Communications products on the same physical host is not supported.

You can use older models of the UCS hardware with your system, but for a better user experience use the hardware listed in the table. For example, you can use the UCS C220 M3 for a 250-user system if you already have that hardware available.

When upgrading Cisco Webex Meetings Server, you can use Cisco UCS B200 M3 blade servers with 2x local hard drives, as long as the upgraded system uses SAN storage for its virtual machines. Using SAN storage with B-series blade servers allows your system to meet the 4 hard disk drives in a RAID 5 or RAID 10 configuration requirement for Cisco Webex Meetings Server.

Note For 800-user and 2000-user systems, we do not recommend deploying additional virtual machines on a DMZ host. This can result in increased packet loss and noticeable latency on media connections.

Resources Consumed by CWMS and the ESXi Host

Cisco Webex Meetings Server is deployed on one or more virtual machines on ESXi hosts. Both Cisco Webex Meetings Server (CWMS) and ESXi (VMware component that enables virtualization on the physical Cisco UCS Server) use CPU and memory resources, and storage space. Depending on your system size, vCenter and multiple virtual machines might run on the same Cisco UCS server.

Important Disable hyperthreading for all CWMS virtual machines. Some services and applications are not designed to work with multithreading capabilities. This incompatibility can cause issues, such as high CPU or memory usage. We do not include hyperthreading in the CPU calculations for any size CWMS system.

CWMS uses *resource reservation* for its virtual machines to guarantee system scalability. Other VMware workloads do not take CPU and other resources away from the virtual machines. The minimum requirements for each system size includes enough resources to support:

- Continued quality of service for CWMS at peak system usage (maximum capacity).
- VMware ESXi.
- VMware vCenter (when co-resident).

  For the requirements for vCenter Server, see Knowledge Base and search for "Installing vCenter Server <version> best practices," where <version> is your vCenter Server version.
- VMware snapshots of the virtual machine (delete these as soon as possible otherwise you may experience severe performance degradation).

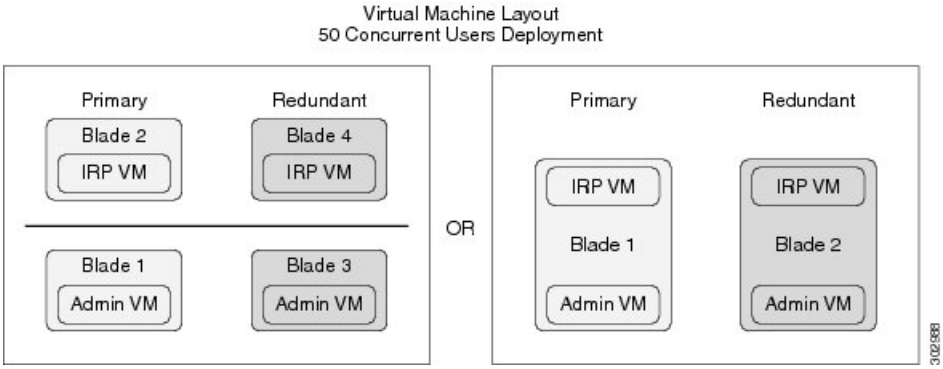
  Extra disk space is required for snapshots, as some snapshots may be as large as the original virtual machine. In some cases, vSphere may delete snapshots to create storage space, compromising the ability to roll back to previous snapshots.
- Use of the Cisco UCS Server over the typical life cycle of the server.

The hardware requirements specified in the OVA file are the minimum requirements to deploy Cisco Webex Meetings Server. These requirements *do not include* any CPU, memory, or storage requirements for VMware vCenter or ESXi.

Caution Co-residency, other than the configurations listed in the tables in this document, is not supported. If you disregard our system requirements, your virtual machines might not boot. The deployment of the virtual machines can stall from within the earliest product screens during the vCenter OVA deployment.

50-user System

A 50-user system is also called a *micro* system. (Multi-data Center (MDC) is not available for micro systems.) The diagram illustrates two versions of a 50-user deployment. (The "Redundant" virtual machines demonstrate support for High Availability (HA).)



The table lists the minimum hardware requirements for the ESXi hosts (Cisco UCS servers) in your system. The last two columns show the amount of free disk space needed for new installations of Cisco Webex Meetings Server, and for an Automatic Upgrade, using your existing Cisco UCS servers. For more information, see General System Requirements.

For information about the bandwidth requirements, see the Network Bandwidth Requirements, on page 47.

Note For IOPS information, see Advantages of Deploying a System on VMware vSphere, on page 30.

Co-residency with vCenter is supported with a 50-user system deployment as configured in the following table.

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Admin	4	24	2 for the Admin virtual machine, including 1 if NIC teaming is used for redundancy 1 recommended for ESXi management network	2.5 TB; minimum of 7,200 RPM

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Stora Requirement fo New Installs
Admin and vCenter (co-resident)	6	36	2 for the Admin virtual machine, including 1 if NIC teaming is used for redundancy 1 for vCenter 1 recommended for ESXi management network	2.5 TB; minimu of 7,200 RPM
Internet Reverse Proxy (IRP)	6	12	2 for the IRP virtual machine, including 1 if NIC teaming is used for redundancy 1 recommended for ESXi management network	600 GB; minim of 7,200 RPM
Admin and IRP (co-resident)	8	36	2 for the Admin virtual machine, including 1 if NIC teaming is used for redundancy 2 for IRP virtual machine, including 1 if NIC teaming is used for redundancy 1 recommended for ESXi management network	2.5 TB; minimu of 7,200 RPM
Admin and IRP and vCenter (all co-resident)	12	40	2 for the Admin virtual machine, including 1 if NIC teaming is used for redundancy 2 for IRP virtual machine, including 1 if NIC teaming is used for redundancy 1 for vCenter 1 recommended for ESXi management network	2.5 TB; minimu of 7,200 RPM

Note If you plan to use a High Availability (HA) system, double the hardware requirements and quantities of the primary system to support both systems.

Resources Reserved by the Virtual Machines in a 50-user System

This section describes how much media the virtual machines use and is intended for those with expert knowledge of VMware. CPU resources are specified as vCPUs (cores) and MHz (CPU cycles). The VMware VMkernel uses MHz cycles to control CPU scheduling.

Memory resources are specified by maximum memory and reserved memory. Reserved memory is not shared with other virtual machines on the same physical Cisco UCS Server.

Disk resources (storage) are controlled in two separate areas. During the OVA build, the CentOS file system partition sizes determine the minimum disk size. Secondly, vCenter controls the maximum disk space available.

If you attempt to deploy a virtual machine without the minimum number of vCPUs, the OVA deployment of the virtual machine will fail. If you attempt to deploy a virtual machine without the minimum total MHz processor speed, then the virtual machine will not power on.

Important The numbers in this table do not include resources for VMware ESXi.

Virtual Machine Type	Virtual CPU (vCPU)	CPU[2] (MHz)	Reserved Memory/Total Memory[3] (GB)	Disks (GB)
Admin	4	8000	12/14	836
Internet Reverse Proxy	4	8000	4/4	276

[2] Number obtained by multiplying the number of physical CPUs with the speed of the CPU chip (MHz). Hyperthreading is not included in this calculation. (The physical CPU must have a clock speed of 2.4 GHz or faster.)

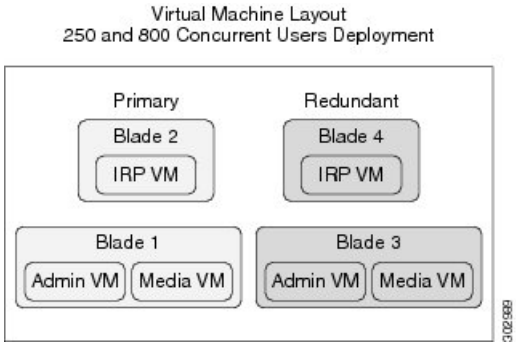
[3] Virtual machines with media functionality have additional, non-reserved memory; Memory = Reserved/Total

Related Topics

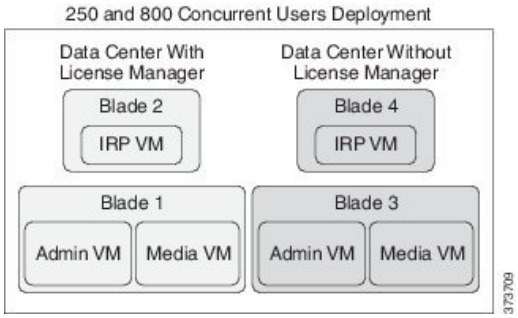
Resources Consumed by CWMS and the ESXi Host, on page 9

250-user System

A 250-user system is also called a *small* system. This diagram illustrates two versions of a 250-user deployment. The "Redundant" virtual machines demonstrate support for High Availability (HA). If your system does not include HA support, only deploy the **Primary** system.



This diagram shows the layout of a 250-user system with two data centers that form a Multi-data Center (MDC) system with Internet Reverse Proxy (IRP) support.. The License Manager runs on only one data center.



The table lists the minimum hardware requirements for the ESXi hosts (Cisco UCS servers) in your system. The last two columns show the amount of free disk space needed for new installations of Cisco Webex Meetings Server, and for an Automatic Upgrade, using your existing Cisco UCS servers. For more information, see General System Requirements.

For information about the bandwidth requirements, see Network Bandwidth Requirements, on page 47.

For IOPS information, see Advantages of Deploying a System on VMware vSphere, on page 30.

Co-residency with vCenter is supported with a 250 user system deployment as configured in the following table.

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Admin and Media	12	52	• 2 for Admin and Media, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	2.5 TB; minimum of 7200 RPM
(Admin and Media) and vCenter (co-resident)	16	56	• 2 for Admin and Media, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network • 1 for vCenter	2.5 TB; minimum of 7200 RPM
Internet Reverse Proxy (IRP)	12	36	• 2 for IRP, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	600 GB; minimum of 7200 RPM

Note If you plan to use a HA system, purchase the same hardware and quantities for the HA system as you did for the primary system.

Resources Reserved by the Virtual Machines in a 250-user System

This section describes how much media the virtual machines use and is intended for those with expert knowledge of VMware. CPU resources are specified as vCPUs (cores) and MHz (CPU cycles). The VMware VMkernel uses MHz cycles to control CPU scheduling.

Memory resources are specified by maximum memory and reserved memory. Reserved memory is not shared with other virtual machines on the same physical Cisco UCS Server.

Disk resources (storage) are controlled in two separate areas. During the OVA build, the CentOS file system partition sizes determine the minimum disk size. Secondly, vCenter controls the maximum disk space available.

If you attempt to deploy a virtual machine without the minimum number of vCPUs, the OVA deployment of the virtual machine will fail. If you attempt to deploy a virtual machine without the minimum total MHz processor speed, then the virtual machine will not power on.

Important The numbers in this table do not include resources for VMware ESXi.

Virtual Machine Type	Virtual CPU (vCPU)	CPU[4] (MHz)	Reserved Memory/Total Memory[5] (GB)	Disks (GB)
Admin	4	8000	16/16	876
Media	8	16,480	13/23	276
Internet Reverse Proxy	8	16,480	6/6	276

[4] Number obtained by multiplying the number of physical CPUs with the speed of the CPU chip (MHz). Hyperthreading is not included in this calculation. (The physical CPU must have a clock speed of 2.4 GHz or faster.)

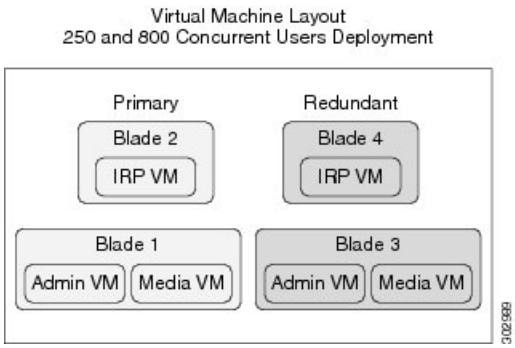
[5] Virtual machines with media functionality have additional, non-reserved memory; Memory = Reserved/Total

Related Topics

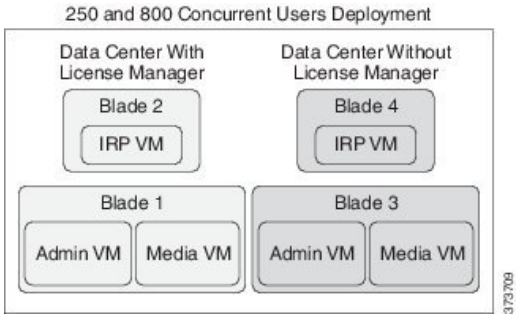
Resources Consumed by CWMS and the ESXi Host, on page 9

800-user System

An 800-user system is also called a *medium* system. This diagram illustrates two versions of an 800-user deployment. The "Redundant" virtual machines demonstrate support for High Availability (HA).



This diagram shows the layout of an 800-user system with two data centers that form a Multi-data Center (MDC) system with Internet Reverse Proxy (IRP) support. The License Manager runs on only one data center.



The table lists the minimum hardware requirements for the ESXi hosts (Cisco UCS servers) in your system. The last two columns show the amount of free disk space needed for new installations of Cisco Webex Meetings Server, and for an Automatic Upgrade, using your existing Cisco UCS servers. For more information, see General System Requirements.

For more information about the bandwidth requirements, see Bandwidth on Cisco Webex Meetings Server Network Interfaces.

For information about the bandwidth requirements, see the Network Bandwidth Requirements, on page 47.

Note Co-residency with vCenter is not supported with an 800-user system deployment.

For IOPS information, see Advantages of Deploying a System on VMware vSphere, on page 30.

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Admin and Media (combined)	40	80	• 2 for Admin and Media, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	2.5 TB; minimum of 10,000 RPM

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs	Fre Sto Au
Internet Reverse Proxy (IRP)	20	18	• 2 for IRP, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	600 GB; minimum of 10,000 RPM	30

Note If you plan to use an HA system, purchase the same hardware requirements and quantities as the primary system.

For 800 user systems, we do not recommend deploying additional virtual machines on a DMZ host. This might result in increased packet loss and noticeable latency on media connections.

Resources Reserved by the Virtual Machines in an 800-user System

This section illustrates how much media the virtual machines use and is intended for those with expert knowledge of VMware. CPU resources are specified as vCPUs (cores) and MHz (CPU cycles). The VMware VMkernel uses MHz cycles to control CPU scheduling.

Memory resources are specified by maximum memory and reserved memory. Reserved memory is not shared with other virtual machines on the same physical Cisco UCS Server.

Disk resources (storage) are controlled in two separate areas. During the OVA build, the CentOS filesystem partition sizes determine the minimum disk size. Secondly, vCenter controls the maximum disk space available.

If you attempt to deploy a virtual machine without the minimum number of vCPUs, the OVA deployment of the virtual machine will fail. If you attempt to deploy a virtual machine without the minimum total MHz processor speed, then the virtual machine will not power on.

Important The numbers in this table do not include resources for VMware ESXi.

Virtual Machine Type	Virtual CPU (vCPU)	CPU[6] (MHz)	Reserved Memory/Total Memory[7] (GB)	Disks (GB)
Admin	10	20,600	16/16	876
Media	30	60,800	14/44	276
Internet Reverse Proxy	20	41,200	10/10	276

[6] Number obtained by multiplying the number of physical CPUs with the speed of the CPU chip (MHz). Hyperthreading is not included in this calculation. (The physical CPU must have a clock speed of 2.4 GHz or faster.)

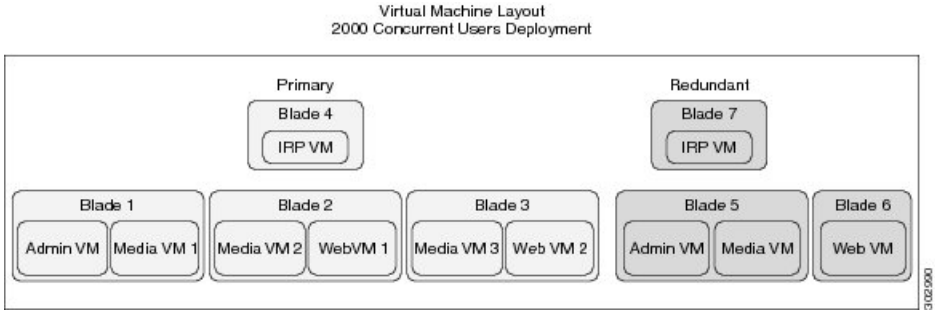
[7] Virtual machines with media functionality have additional, non-reserved memory; Memory = Reserved/Total

Related Topics

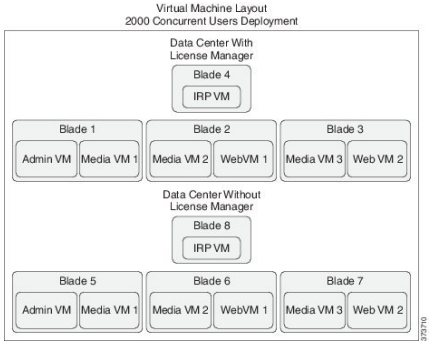
Resources Consumed by CWMS and the ESXi Host, on page 9

2000-user System

A 2000-user system is also described as a *large* system. This diagram shows a 2000-user system with High Availability (HA) and Internet Reverse Proxy (IRP) support. The HA virtual machines are shown as the **Redundant** virtual machines. If your system does not include HA support, only deploy the **Primary** system.



This diagram shows a 2000-user system deployment with two data centers that form a Multi-data Center (MDC) system with Internet Reverse Proxy (IRP) support. The License Manager runs on only one data center.



Important We recommend that you deploy the all virtual machines shown in the diagram. By deploying different types of virtual machines on a physical server, you can better avoid a system shutdown in the event of a hardware failure. For example, placing a Media and a Web virtual machines on a single physical server is more resilient than if you place both Web virtual machines on the same physical server.

On a large system there is an exclusion from the equal load balance rule (see Load Balancing, on page 52 for more information), where there are SIP trunk load balancers on Media 1 and Media 2, and where Media 3 and optionally Media HA do not have load balancing. If there is a failure of both Media 1 and 2 on the primary system, all telephony service on CWMS is lost. If the system is a HA deployment, the redundancy mitigates the failure of a single virtual machine.

The table lists the minimum hardware requirements for the ESXi hosts (Cisco UCS servers) in your system. The last two columns show the amount of free disk space needed for new installations of Cisco Webex

Meetings Server, and for an Automatic Upgrade, using your existing Cisco UCS servers. For more information, see General System Requirements.

For more information about the bandwidth requirements, see Network Bandwidth Requirements, on page 47.

If you plan to add a HA system, those virtual machines are shown as the "redundant" virtual machines. If you do not want HA, deploy only the primary system.

Note Co-residency with vCenter is not supported with a 2000-user system deployment.

Note For IOPS information, see Advantages of Deploying a System on VMware vSphere, on page 30.

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Media1 and Admin (combined)	40	80	• 2 for Media1 and Admin, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	3 TB; minimum of 10,000 RPM
Media2 and Web1 (combined)	40	80	• 2 for Media2 and Web1, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	1.5 TB; minimum of 10,000 RPM
Media3 and Web2 (combined)	40	80	• 2 for Media3 and Web2, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	1.5 TB; minimum of 10,000 RPM

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Internet Reverse Proxy (IRP)	20	18	• 2 for IRP, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	600 GB; minimum of 10,000 RPM
Media and Admin (combined) for HA	40	80	• 2 for Media and Admin, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	3 TB; minimum of 10,0 RPM
Web for HA	20	40	• 2 for Web, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	1.5 TB; minimum of 10, RPM
IRP for HA	20	18	• 2 for IRP, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	600 GB; minimum of 10,000 RPM

Table 3: Requirements for Extended Capacity Systems

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
IRP1 and IRP3 (combined) IRP2 and IRP4 (combined)	40	36	• 2 for IRP, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	1.5 TB; minimum of 10, RPM

Virtual Machines on ESXi Host (Cisco UCS Server)	CPU Cores	Memory (GB)	Ethernet Ports	Hard Drive Storage Requirement for New Installs
Media 4 and Web3 (combined) Media 5 and Web4 (combined) Media 6 and Web5 (combined)	40	80	• 2 for Web, including 1 if NIC teaming is used for redundancy • 1 recommended for ESXi management network	1.5 TB; minimum of 10,000 RPM

Note For 2000 user systems, we do not recommend deploying additional virtual machines on a DMZ host. This might result in increased packet loss and noticeable latency on media connections.

Resources Reserved by the Virtual Machines in a 2000-user System

This section illustrates how much media the virtual machines use and is intended for those with expert knowledge of VMware. CPU resources are specified as vCPUs (cores) and MHz (CPU cycles). The VMware VMkernel uses MHz cycles to control CPU scheduling.

Memory resources are specified by maximum memory and reserved memory. Reserved memory is not shared with other virtual machines on the same physical Cisco UCS Server.

Disk resources (storage) are controlled in two separate areas. During the OVA build, the CentOS file system partition sizes determine the minimum disk size. Secondly, vCenter controls the maximum disk space available.

If you attempt to deploy a virtual machine without the minimum number of vCPUs, the OVA deployment of the virtual machine will fail. If you attempt to deploy a virtual machine without the minimum total MHz processor speed, then the virtual machine will not power on.

The numbers in the following table apply to Extended Capacity systems.

Important The numbers in this table do not include resources for VMware ESXi.

Virtual Machine Type	Virtual CPU (vCPU)	CPU[8] (MHz)	Reserved Memory/Total Memory[9] (GB)	Disks (GB)
Admin	10	20,600	16/16	1134
Media	30	60,800	14/44	276
Web	10	20,600	16/16	276
Internet Reverse Proxy	20	41,200	10/10	276

[8] Number obtained by multiplying the number of physical CPUs with the speed of the CPU chip (MHz). Hyperthreading is not included in this calculation. (The physical CPU must have a clock speed of 2.4 GHz or faster.)

[9] Virtual machines with media functionality have additional, non-reserved memory; Memory = Reserved/Total

Related Topics

Resources Consumed by CWMS and the ESXi Host, on page 9

System Capacity Matrix

Key Points:

- One of the basic assumptions for the information presented in this section is that there are at least two people participating in a meeting.
- Concurrent meeting connections is defined as the number of people participating in a meeting at any given time. For example, for a 50 user system, the maximum concurrent meeting connections can be comprised of five concurrent meetings that each have a total of 10 people in the meeting (for example, one host and nine participants).
- After the maximum number of meeting participants is reached for any point in time, the system does not allow other users to start or join meetings. Of those maximum number of meeting participants (2000, 800, 250 or 50 people), only half of the participants can use video. Video is defined as sending or receiving, meaning users might be using their Webex webcam video or the video file share option which allows users to share a video.
- Desktop sharing is not considered video. This means with a 250 user system, 250 people can be sharing their desktops during meetings at any given time.
- The addition of High Availability or Multi-data Center does not increase the capacity of the system to hold meetings; an 800-user system is still an 800-user system.

The numbers in the table below represent the design capacity for the Cisco Webex Meetings Server system. Operating the system at a capacity higher than these specifications can result in a degraded user experience and may result in system instability. Cisco reserves the right to enforce capacity limits at these levels.

Note These values in the following table remain the same regardless of whether your system is a single data center or a multi-data center system.

Table 4: System Capacity Matrix

System Capacity	4000 user system	2000 user system	800 user system	250 user system	50 user system	Notes
Maximum Concurrent Meeting Connections (Audio, Video, and Web users)	4000	2000	800	250	50	The number of people participating in concurrent meetings at any given time.

System Capacity	4000 user system	2000 user system	800 user system	250 user system	50 user system	Notes
Maximum Simultaneous Audio Connections (Teleconference Phone Calls and Voice Connection Using Computer From Meeting Clients)	4000	2000	800	250	50	The system capacity remains the same as shown on the left, regardless of what combination of the following features are used: • G.711, G.722, G.729 audio codecs • IPv4 or IPv6 teleconferencing • TLS/SRTP audio encryption
Maximum Concurrent Video and Video File Sharing Users	2000 (180p, 360p) / 1000 (720p in 4.0)	1000 [10]	400	125	25	These numbers show the maximum number of concurrent meeting connections (or participants) allowed to use video sharing at the same time. When the number of users with video sharing in concurrent meetings reaches this limit, then the remaining users invited to the concurrent meetings can join the meetings, but their video windows are dimmed. **Note** If one participant in a meeting uses video, then all other users in the same meeting are counted as video users, even if they are not using video themselves. **Note** Desktop sharing is not considered video.
Maximum Participants in One Meeting	500	500	500	250	50	These numbers show the maximum number of participants who can attend a meeting.
Maximum Meetings That Can be Recorded Simultaneously	200	100	40	13	3	This is the total number of meetings that can use the Recording feature at one time.

System Capacity	4000 user system	2000 user system	800 user system	250 user system	50 user system	Notes
Maximum Concurrent Recording Playback Sessions	1000	500	200	63	12	This is the total number of recording playback sessions that can occur simultaneously. This refers to recordings that are saved on your storage system and does not include recordings that are downloaded to users' desktops. **Note** These playback sessions are not included in the concurrent meeting connections on the system.
Maximum Number of User Profiles	400,000	400,000	400,000	400,000	400,000	This number includes active and deactivated users.
Maximum Concurrent Meetings	2000	1000	400	125	25	The number of separate meetings that can be active concurrently.
Maximum Call Rate (calls/per second)	40	20	8	3	1	This is the average number of users who can dial into a meeting during a one second time period. After the system reaches this number, the next few users to dial into the meeting might experience an additional few seconds wait before connecting to the meeting.
Maximum Concurrent Sign-in	40 people per second	20 people per second	8 people per second	3 people per second	1 person per second	This is the average number of users who can simultaneously sign in to your Webex site during a one second time period. After the system reaches this number, the next few users to sign in to the Webex site might experience an additional few seconds wait before they can join a meeting.
Maximum Aggregate Bandwidth Utilization	10 Gbps	5 Gbps	2 Gbps	625 Mbps	125 Mbps	Using our test system at its maximum bandwidth, this is the maximum bandwidth the test system could handle. For more information about bandwidth utilization see the Network Bandwidth Requirements section in the *Networking Topology for Your System* chapter of the Planning Guide. You can also refer to the Webex Network Bandwidth White Paper.

[10] 800 in Federal Information Processing Standards (FIPS environments)

Tip The maximum length of a meeting is 24 hours for all size user system deployments.

Note When considering an upgrade, plan for the increased size of the data stores, as the original system and the upgraded system share data stores until testing of the upgraded system is complete and the original system is removed.

For information about network bandwidth requirements for the various size user systems, see the "Network Bandwidth Requirements" section in the Network Topology For Your System chapter in this book.

Supported Upgrade Paths

This release of Cisco Webex Meetings Server supports upgrades from release 1.5 to 3.0. The following points apply:

- An upgrade is a replacement of the system to deploy major modifications that we made to the system.
- An update is an incremental modification of the system. Updates deploy fixes and minor improvements.
- An update retains all data from the original system. An upgrade retains all data from the original system, except for the logs.
- You can't change the audio encryption type (Audio Encrypted -AE/Audio Unencrypted -AU) for the system, during an upgrade or during an update. After deployment, the only way to change a system from one type of audio encryption to the other is to deploy a new system.
- When upgrading, you can't skip a major version of the software and go directly to a companion maintenance release (MR). For more information, see the following table.

Use the following table to determine your upgrade path to Cisco Webex Meetings Server Release 4.0.

Installed Release	Path to Release 4.0[11]
2.8 [12]	**1.** Update to the latest available 2.8MR3 patch. **2.** Install Webex Productivity Tools, or push it to the desktops. **3.** Upgrade to 4.0 FCS. **4.** Update to the latest available 4.0MR release and patch. **5.** Uninstall Webex Productivity Tools. **6.** Install the Webex Meetings desktop app, or push it to the desktops.

Installed Release	Path to Release 4.0[11]
3.0[13]	**1.** Update to the latest available 4.0MR and patch. **2.** Uninstall Webex Productivity Tools. **3.** Install the Webex Meetings desktop app, or push it to the desktops. **Important** You can't start instant meeting from Webex Productivity Tools versions earlier than 2.82.7000.1229.
4.0	**1.** Update to the latest available 4.0MR and patch. **2.** Update Webex Meetings Desktop app if required.

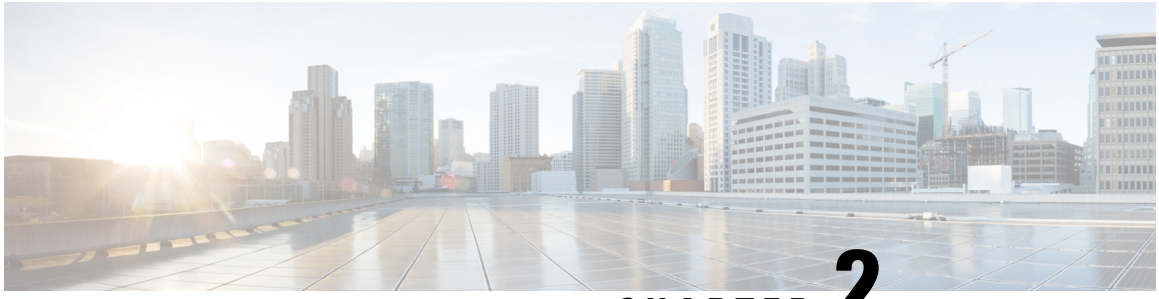
[11] The Webex Meetings desktop app replaced Webex Productivity Tools for Cisco Webex Meetings Server 4.0. If you require Productivity Tools as part of your upgrade strategy, only version 2.82.7000.1229 or later is compatible.

[12] If your system is running an earlier version, see the *Release Notes for Cisco Webex Meetings Server Release 2.8*.

[13] The Webex Productivity Tools version must be 2.82.7000.1229 or later, to start the 4.0 and later meeting clients. Upgrade Productivity Tools, before you update Cisco Webex Meetings Server to 4.0MR2.

Note All updates require downtime. For Multi-data centers, you update both data centers simultaneously.

Caution Don't click **Restart** for one data center until the update for the other is complete, and both display the **Restart** button.



CHAPTER 2

Introduction and Data Center Topology For Your System

This chapter provides an introduction, a data center overview, and VMware vCenter requirements for your system.

Introducing Cisco Webex Meetings Server

Cisco Webex Meetings Server (CWMS) is a secure, fully virtualized, private cloud (on-premises) conferencing solution that combines audio, video, and internet to reduce conferencing costs and extend your investments in Cisco Unified Communications.

Like other Cisco Webex products, it offers real-time collaboration tools, including document, application, and desktop sharing, annotation tools, full host control for effective meeting management, an integrated participant list with active talker, and video switching, recording, and playback. This product utilizes high quality video, so the video sharing experience is crisp and clear.

You can deploy and manage this conferencing solution in your private cloud, behind the firewall in your data center. It is designed for Cisco UCS servers and VMware vSphere. (For specific requirements, see Minimum Hardware Requirements, on page 7.) It features a rapid virtual deployment and powerful tools for administrators to configure and manage the system and see key system metrics.

In addition, mobile users can attend and participate in meetings. For supported devices, see Operating Systems Requirements for Mobile Devices, on page 161.

Important Considerations For Your System

Note the following:

- Forward proxies—not recommended, though you may use forward proxies with restrictions. For complete details, refer to the *Cisco Webex Meetings Server Troubleshooting Guide*.
- Reverse proxies—only the Internet Reverse Proxy server included with this product is supported.
- NAT—supported when it meets the requirements for this system. For complete details, see Using NAT With Your System.
- Single data centers—deployments within a single data center are supported for all releases of Cisco Webex Meetings Server. For complete details, see Deploying a Single Data Center.
- Multi-data centers—data centers running Cisco Webex Meetings Server Release 2.5 or higher can be joined to create a system comprised of multiple data centers. For complete details, see the *About Multi-data Center* in the Cisco Webex Meetings Server Administration Guide.
- Storage Server—Each data center in a multi-data center system must have a separate storage server. The same storage server cannot support more than one data center.
- High-availability system—defined as a system with redundant virtual machines running the same version of Cisco Webex Meetings Server. If the primary system (in a single data center system) fails, the high-availability system continues service. The redundant high-availability virtual machines must be co-located in the same data center with the primary virtual machines. The primary and high-availability system virtual machines must be on the same VLAN or subnet.

  You cannot join high-availability systems to create a multi-data center environment.
- Internet Reverse Proxy (IRP) Server—is defined as a virtual machine placed as a proxy between the external Internet and a company's internal network to provide public access to CWMS. An Internet Reverse Proxy server is required to allow users to schedule and attend meetings from mobile devices or to provide secured access to your Webex Site from the Internet. An Internet Reverse Proxy server is not required if you are going to limit access to Cisco Webex Meetings Server to your internal network. (Deploy an IRP virtual machine by using the same OVA file you use to deploy your administration virtual machine. The IRP virtual machine must be on the same subnet as the Public Virtual IP address.)
- Virtual IP (VIP) Address—used to communicate with the Admin, Media, and Web virtual machines within a data center.
- Private Virtual IP (VIP) address—configured on the Admin virtual machine and is associated to the Administration Site URL. The private VIP can also be associated with the Webex Site URL if the address is configured in the internal DNS server in a Split-Horizon DNS deployment or deployments without an Internet Reverse Proxy server.
- Public Virtual IP (VIP) address—configured on the Internet Reverse Proxy virtual machine and is associated with the Webex Site URL only. The Webex Site URL on the external DNS servers must be resolvable to the Public Virtual IP address to provide users access to the Webex Site from the Internet. A public virtual IP address is not configured on the system if there is no Internet Reverse Proxy server.

Caution If you disregard our recommendations and requirements when deploying a system, you will not receive support from Cisco. Cisco is not responsible for any problems you might encounter as a result of not following our guidance.

New and Changed Features for Cisco Webex Meetings Server

For a list of new and changed features, see the "New and Changed Features for Cisco Webex Meetings Server" in the *Release Notes for Cisco Webex Meetings Server* at Release Notes.

Information for Cisco Unified MeetingPlace Customers

Because of architectural differences, there is no migration path (for existing user accounts, customizations, and meetings) from Cisco Unified MeetingPlace to Cisco Webex Meetings Server. These are two distinct products.

You can ease the transition for your users by continuing to support both Cisco Unified MeetingPlace and Cisco Webex Meetings Server while encouraging your users to switch to the new system.

Deploying a Single Data Center

Cisco Webex Meeting Server (CWMS) can be deployed as a Single-data Center (SDC) system and optionally as a High Availability (HA) system or a Multi-data Center (MDC) system (see Redundancy in HA or MDC Deployments, on page 43). A SDC system (including a system with HA support) requires only Host licenses after a trial period. A MDC system requires a minimum of two MDC feature licenses, Host licenses, and there is no MDC trial period.

Joining Single Data Centers to Create a Multi-data Center (MDC) System

You can join two data centers that are running Cisco Webex Meeting Server Release 2.5 or higher to form a single Multi-data Center (MDC) system. A maximum of two data centers can be joined. The difference between a Multi-data Center and a High Availability system is that a High Availability system must be co-located and functions as a backup system. In an MDC system, the data centers can be located in different geographic locations and both data centers contribute to system processing. See Redundancy in HA or MDC Deployments, on page 43. One license must be purchased for each CWMS data center in an MDC system. MDC licenses should be purchased before you attempt to deploy an MDC system. (A system with a single data center does not need a feature license.) For details on how to prepare your data centers to be joined, the Join process, and how to carry over data from one data center to another when the Join process is complete, refer to the "Joining Data Centers to Create a Multi-data Center (MDC) System" chapter in the *Cisco Webex Administration Guide* (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html).

Using VMware vSphere with Your System

Important This product only installs on a VMWare vSphere virtualization platform. VMWare Tools for CWMS are automatically installed during system deployment and should not be upgraded manually. See docwiki.cisco.com/wiki/VMWare_Tools for more information on VMWare Tools.

- Cisco Webex Meetings Server is designed to work on any equivalent Cisco UCS Server that meets or exceeds the system requirements. However, to save you time, we recommend using standard Cisco UCS servers. For complete details on the hardware and VMWare requirements, see Minimum Hardware Requirements, on page 7.
- Purchase VMWare vSphere 5.5 or 6.0 for use as the hypervisor platform for Cisco Webex Meetings Server.

  Complete one of the following:

  - Buy vSphere directly from Cisco on the GPL (Global Price List). Cisco is an approved VMWare partner and distributor.
  - Purchase vSphere directly from VMWare through enterprise agreements you have with VMWare.

Advantages of Deploying a System on VMware vSphere

This section explains why VMware vSphere and vCenter are integral to using this Cisco Webex product and lists some considerations.

Deployment of the System

- This product is packaged as a VMware vSphere compatible OVA virtual appliance and not as a collection of software packages on a DVD. You must have vCenter to deploy the OVA or the product will not install.
- By packaging it as a virtual appliance we enable rapid deployment; in some cases in under an hour.
- To facilitate rapid installations with the OVA virtual appliance, you can select automatic system deployment for most system sizes. Simply provide vCenter credentials and we will deploy all the virtual machines for your system without manual intervention. This innovation will minimize your labor costs and time.

Note The OVA template creates two virtual NICs for each virtual machine. However, only the Admin virtual machines uses both virtual NICs. For all other Cisco Webex Meetings Server (CWMS) virtual machines, only one virtual NIC is used and the other one is disconnected.

- CWMS requires you to run VMware ESXi or the corresponding VMware ESXi installable Cisco ISO Image. Both these editions contain the necessary drivers required to support the Cisco UCS Servers that are required by CWMS. For more information, see http://www.cisco.com/en/us/docs/unified_computing/ucs/release/notes/ol_26617.pdf.

Easy Recovery From System Errors

If the change does not meet your expectations, by using VMware Data Recovery you can revert system-impacting changes rapidly and without a system redeployment.

vSphere Considerations

Note the following considerations:

- You can move your virtual machine to another ESXi host. However, you must retain the layout of the virtual machines on the new ESXi host. In other words, if you plan to move a Media virtual machine that is co-resident with a Web virtual machine, then you must either move it to a separate ESXi host (where it is the only virtual machine) or move it to an ESXi host that already has a Web virtual machine.

Note Your destination ESXi host must conform to the same system requirements as the source ESXi host.

The following VMware features are not supported with CWMS:

- VMotion and Storage VMotion (Although you can move your virtual machines, you may not do so by using these tools.)
- VMware Distributed Resource Schedule (DRS)
- vSphere High Availability (HA)
- vSphere clustering and resource sharing
- Cloning a virtual machine

vSphere Best Practices

- We recommend that you do not use virtual machine snapshots. If you decide to use snapshots, then after confirming your system changes, either commit the snapshots or remove them as soon as possible. Keeping a snapshot for any period of time will result in severe performance degradation.
- For SAN environments, deploy disk images to a SAN with high IOPS numbers.

  For an 800-user system, the average IOPS for an OVA deployment is 506 (max IOPS is 855) for the Admin virtual machine and 475 (max IOPS is 652) for a Media virtual machine. Once these virtual machines are created and powered on, then you can enter the case-sensitive URL and continue the system deployment in a web browser. The average IOPS for a primary system is 108 (max IOPS is 1558) and 163 (max IOPS is 1736) for a secondary system.
- Verify that there is enough free space on your SAN. Snapshots are stored on the same SAN.
- Deploy a 10GB network for the quickest deployment and bandwidth for future growth.
- We recommend that you manage all virtual machines by using the same vCenter. This allows for an easier restoration should you need to recover your system.

For more information on network bandwidth, see Network Bandwidth Requirements, on page 47.

vCenter Server Requirements

In addition to vSphere, vCenter Server is also required.

- To deploy this virtual appliance, you must also use vCenter to deploy and manage the virtual machines in your system. This product will not work without vCenter Server.

- Cisco recommends backups and snapshots of the system ahead of important system-impacting operations. Creating backups permits you to roll back the changes in case the update does not meet your expectation. You may automate backups and snapshots using vCenter.
- CWMS supports vSphere Standard Edition.

vSphere Edition For the 800 and 2000 User Systems

- The 800 and 2000 user systems comprise virtual machines that require between 30 and 40 vCPUs. These virtual machines use these vCPUs to perform very compute intensive tasks such as SSL encoding or decoding, mixing audio streams, and so on.

  For complete information on vCPU requirements, see Resources Consumed by CWMS and the ESXi Host, on page 9.
- At minimum, you must purchase the vSphere 5.0 Enterprise Plus edition or the vSphere 5.1 Enterprise edition, as the lower-end vSphere editions do not support the number of required vCPUs.

IOPS and Storage System Performance

Expected Maximum IOPS and Throughput

The following table shows the expected maximum Input/Output Operation Per Second (IOPS) and throughput values for maximum load on the system.

System Size	Virtual Machine	Maximum Input/Output Operations (IOPS)	Maximum Read Megabytes per Second	Maximum Write Megabytes per Second
50 user system	Admin	450	1	15
	DMZ	70	0.3	0.3
250 user system	Admin	1400	1	25
	Media	150	1	10
	DMZ	110	0.4	0.6
800 user system	Admin	1400	3	50
	Media	300	1	30
	DMZ	150	1	1.5
2000 user system	Admin	1600	2.5	60
	Media	300	1	25
	Web	200	3	1.5
	DMZ	200	1.5	3

IOPS for System Reboot for a 2000 User System

The following table shows IOPS information for a 2000 user system for the boot (reboot) process.

Virtual Machines in a 2000 User System	IOPS for System Boot (Reboot)	IOPS for Minor Update
Admin	2300	3000
Media	2000	2000
Web	1500	2000
Web	1000	2000

IOPS for Backup for a 2000 User System

The following table shows IOPS information for a 2000 user system for a backup done during the off hours.

Admin Virtual Machine for a 2000 User System	IOPS for Backup	Maximum Read Megabytes per Second	Maximum Write Megabytes per Second
1 GB Backup	2000	220	300
12 GB Backup	5000	320	600

Installing VMware vSphere ESXi and Configuring Storage

Cisco Webex Meetings Server is a software-based solution. It is not a combination hardware and software package. You can choose what to purchase and how to provision your hardware platforms, as long as the hardware meets or exceeds CPU, memory, and storage requirements.

You can deploy Cisco Webex Meetings Server on Cisco UCS Servers that meet our minimum specifications. Or you can choose to deploy this product on newer and higher-end UCS Servers that exceed our minimum specifications.

Multiple RAID controller and network options are available. You can choose to use SAN storage instead of local RAID. We do not provide details about every storage configuration that you may choose.

For more information, see the *Cisco UCS Servers RAID Guide*: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.html.

Setting the Write Cache on a RAID Controller

For optimal system performance, configure the Default Write setting on your RAID controller. You can set Default Write to three settings: *Write Back with BBU*, *Write Through*, or *Always Write Back*. Some guidelines for selecting the appropriate setting for Default Write on your Cisco UCS Servers are:

- **Write Back with BBU**—Use this setting if you have installed a battery backup unit on your RAID controller. If the system experiences a power loss, the battery backup unit preserves the content of the controller cache memory.

  If the battery backup unit fails or goes offline to a re-learn cycle, the Write Back with BBU setting automatically fails back to **Write Through** cache. Without a working battery backup unit, the Write

Through setting is safer although you may notice performance degradation on the I/O subsystem of the host machine.

- **Write Through**—Use this setting and enable the cache explicitly (using the Disk Cache option) if you must remove the battery backup unit for repairs. This setting gives you better, but not optimal performance. After you replace the faulty battery, you can safely return the Default Write setting to Write Back with BBU mode.
- **Always Write Back**—Use this setting if the host that houses your RAID controller is connected to an uninterruptible power supply unit.

Note When you create a RAID array using SSD drives, you can set **Disk Cache Policy** to the default: **Unchanged**.

Joining Meetings

End users sign in to the Webex site, where they can schedule, start, and join meetings. This website includes real-time conferencing elements that facilitate online meetings. Users can join meetings through a browser or through a client on their desktops.

For more information about the end user experience, sign in to your Webex site and click **Help**.

Windows Users

This document assumes that users have Windows Administrator privileges on their PCs, sufficient to allow them to join Webex meetings. If this is not true, you can push Webex applications to users by using desktop management software such as IBM Tivoli. See Configure Your Application Download Settings, on page 114.

- Microsoft Internet Explorer users can install an ActiveX control or Java plug-in, download the Webex Meetings application installer, or run the application in a temporary system folder (such as TFS). The first time the user joins a meeting, the client software is downloaded and automatically installed.
- Google Chrome and Mozilla Firefox users can install a Java plug-in, download the Webex Meetings application, or run the application in a temporary system folder. The client software is downloaded and automatically installed the first time the user joins a meeting.

It is not necessary to change any of the ActiveX, Java plug-in, Webex Meetings application installer, or TFS settings.

Mac Users

- If Java is enabled, the client software is downloaded and automatically installed the first time the user joins a meeting. (Java is turned off by default in Mac OS X Lion version 10.7 and OS X Mountain Lion version 10.8.)
- If Java is disabled, the user can download and install the Webex Meetings application.

Multi-data Center System Users

Your Webex site can use self-signed certificates instead of certificates from a well-known Certificate Authority. After you join your data center to another data center, users must install a certificate for each data center in the Trusted Root Certification Authorities store before they start or join a meeting.

Using Chrome and FireFox Browsers

If you use Chrome 32 and later or Firefox 27[14] and later, you might see a prompt to install a Cisco Webex plug-in. Select **Download** and follow the instructions to install the required plug-in.

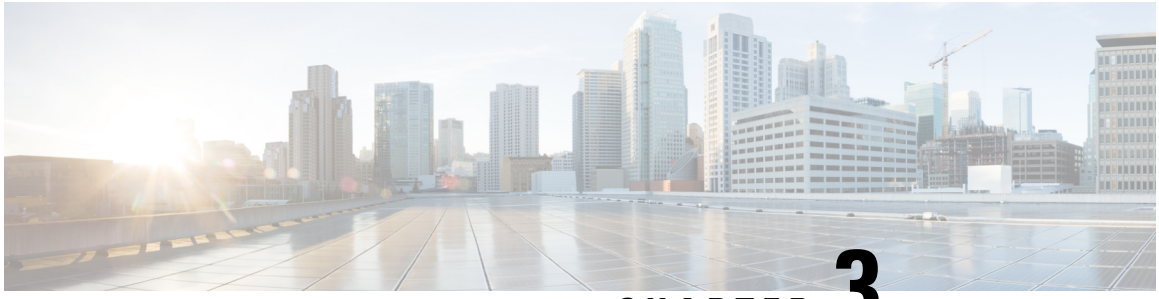
Note After installing the plug-in, some browsers require that you enable it.

- If you use Chrome, click the plug-in icon that appears on the top right of your page. Select the **Always allow plug-ins...** option and then click **Done**.
- If you use Firefox, click the plug-in icon that appears at the beginning of your URL (before https:) and then click **Allow and Remember**.

If the meeting does not start automatically, refresh the page.

If you use the Chrome browser to start a Webex meeting or to play a Webex recording, you might need to add the Cisco Webex extension to Chrome. This is a one-time installation.

[14] The exact versions of Chrome and Firefox that are affected by this policy have not been finalized as of the publishing of this document.



CHAPTER 3

Networking Topology

Virtual Machine Layout in Your Network

Cisco Webex Meetings Server (CWMS) comprises two groups of virtual machines: the internal virtual machines and the optional Internet Reverse Proxy (IRP) virtual machines. IRP is required for systems where external users are allowed to host or attend meetings through the Internet without using VPN or by using CDMA mobile devices. Without IRP, only internal and VPN users can host or join meetings. For more information about IRP, see Network Considerations for the Internet Reverse Proxy, on page 45.

Internal Virtual Machines

Internal virtual machines refer to the Admin virtual machine, and if applicable, the Media and Web virtual machines.

- The internal virtual machines *must* be on a single, common VLAN or subnet. During the system deployment, you will see error messages if your IP address assignments violate this rule. The system design assumes that all the internal virtual machines, including any High Availability (HA) virtual machines, are connected through a LAN that offers high bandwidth, negligible packet loss, and a latency of under 4 ms.

  Voice, data, video and the SAN all rely on the network bandwidth. It is critical to deploy a network that is capable of handling the required load.

- Cisco recommends placing all the internal virtual machines on the same Ethernet switch. However, when provisioning a HA system we recommend that you deploy two Ethernet switches to ensure network redundancy.

- If you decide instead to place the virtual machines on different Ethernet switches within the same data center, then your network *must meet* the specific bandwidth and network latency requirements as described in Network Bandwidth Requirements, on page 47. In this situation, the switch-to-switch trunk must meet the same networking characteristics as the L3 latency and throughput for a single physical switch.

For additional information on systems with HA, see Redundancy in HA or MDC Deployments, on page 43.

Different Types of Network Topology for Your System

Cisco Webex Meetings Server supports the following network topologies:

- Internal Internet Reverse Proxy (IRP) Network Topology, on page 38
- Non-Split-Horizon Network Topology, on page 39
- All Internal Network Topology, on page 41
- Split-Horizon Network Topology, on page 42

Important If you want mobile users to attend meetings, select a network topology that includes the Internet Reverse Proxy virtual machine. Deploy the Internet Reverse Proxy regardless of how mobile users attend meetings.

When using a cellular data network, mobile users join the meeting through the Internet to the Internet Reverse Proxy. When using a local Wi-Fi connection, mobile users join the meeting using one of the following methods:

- Internet Reverse Proxy (non-split-horizon network topology)
- Directly through the internal virtual machines (split-horizon network topology)

Note If your network topology includes forward proxies, they must meet specific requirements for the Internet Reverse Proxy to work properly. See the *Cisco Webex Meetings Server Troubleshooting Guide* for complete details.

Internal Internet Reverse Proxy (IRP) Network Topology

This section describes the network topology when all the virtual machines in your system, including the Internet Reverse Proxy (IRP) virtual machine, are in the same internal network.

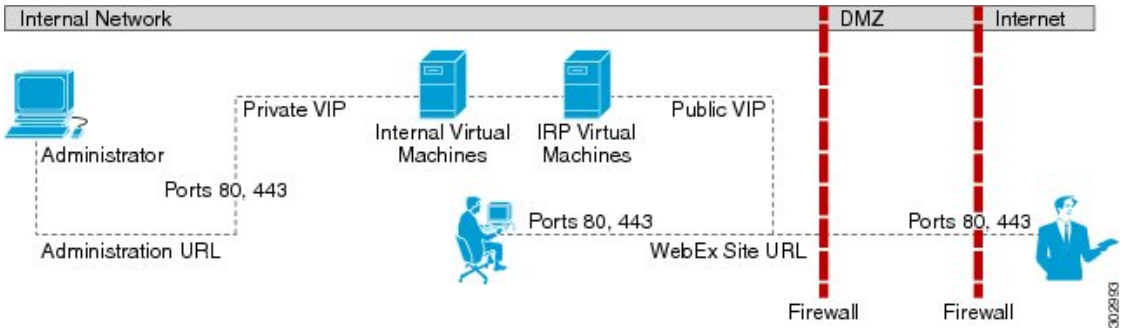
This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

If you are using automatic deployment, then the ESXi hosts for all your virtual machines (including the IRP) must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

Note This configuration supports mobile access.

You will define the Administration URL, the Webex Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco Webex Meetings Server Administration Guide*.

This is a diagram of an all-internal IRP network topology.



For a complete list of the port access required for this deployment, see Port Access When All the Virtual Machines Are in the Internal Network, on page 74.

Advantages of an All Internal IRP Network Topology

Compared with the non-split-horizon network topology, there are no virtual machines in the DMZ, and the network traffic for internal users is not connected through the DMZ to host or attend meetings.

Disadvantages of an All Internal IRP Network Topology

Public access (allowing external users to access the system) requires opening inbound ports (80 and 443) directly from the Internet to the internal network.

For more information about IRP, see Network Considerations for the Internet Reverse Proxy, on page 45.

Non-Split-Horizon Network Topology

This section describes the network topology when you have a non-split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

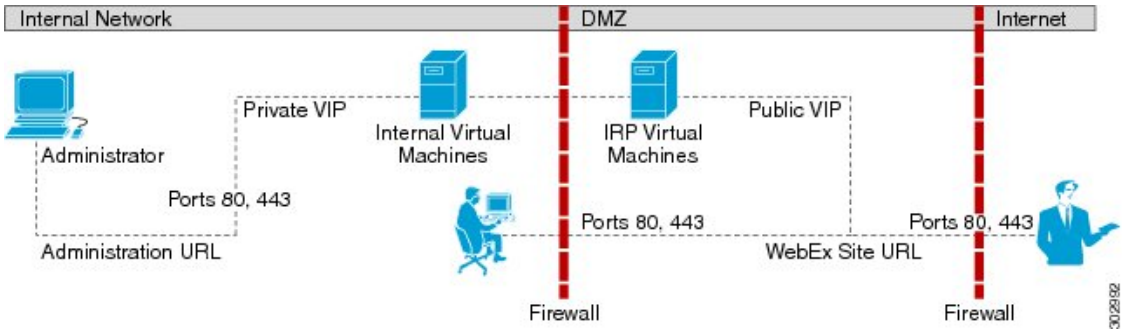
Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

Note This configuration supports mobile access.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the Webex site URL using the private VIP address. External users (outside the firewall) access the Webex site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the Webex site URL using the public VIP address.

You will define the Administration URL, the Webex Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco Webex Meetings Server Administration Guide*.

This is a schematic diagram of a non-split-horizon network topology.



Note For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network, on page 75.

Advantages of a Non-Split-Horizon Network Topology

- Tight control on the traffic that comes in and goes out of a network.
- Addresses more common, simple DNS network requirements.

Disadvantages of a Non-Split-Horizon Topology

- Complex setup, but not as complex as the split-horizon network topology.
- Internal traffic is directed to the DMZ network. All network traffic from the Internet as well as from the internal (private network) goes to the Internet Reverse Proxy in the DMZ network, then comes back to the internal virtual machines.
- Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.
- Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.
- Of the three network topologies, this configuration most affects network performance, since all of the meetings load is through the Internet Reverse Proxy. Because there are multiple hops, network latency is affected as well.

Note Refer to Network Bandwidth Requirements, on page 47 for details about NIC speed requirements for non-split-horizon DNS deployments.

All Internal Network Topology

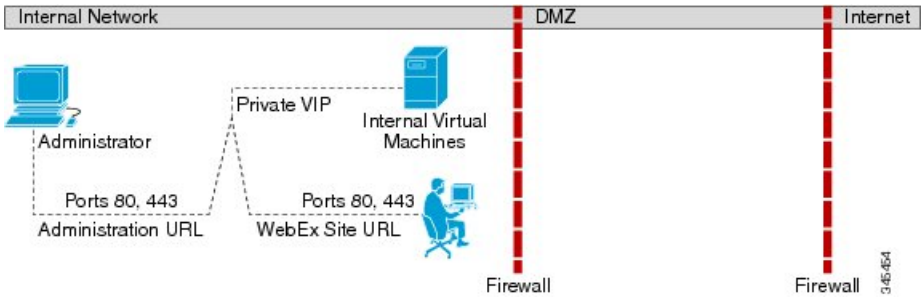
This section describes the network topology when all the virtual machines in your system are in the same internal network. There is no public access; only internal and VPN users can host or join meetings.

Note If you are using automatic deployment, then the ESXi hosts for all your virtual machines must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

Note This configuration does not support mobile access.

You will define the Administration URL, the Webex Site URL and the private VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco Webex Meetings Server Administration Guide*.

This is a schematic diagram of an all internal network topology.



Advantages of an All Internal Network Topology

- Provides lower latency as there are fewer network hops between the virtual machines.

Disadvantages of an All Internal Network Topology

- There is no public access (allowing external users to access the system) and no access for mobile users.

Split-Horizon Network Topology

This section describes the network topology when you have a split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy (IRP) is in the DMZ network.

Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

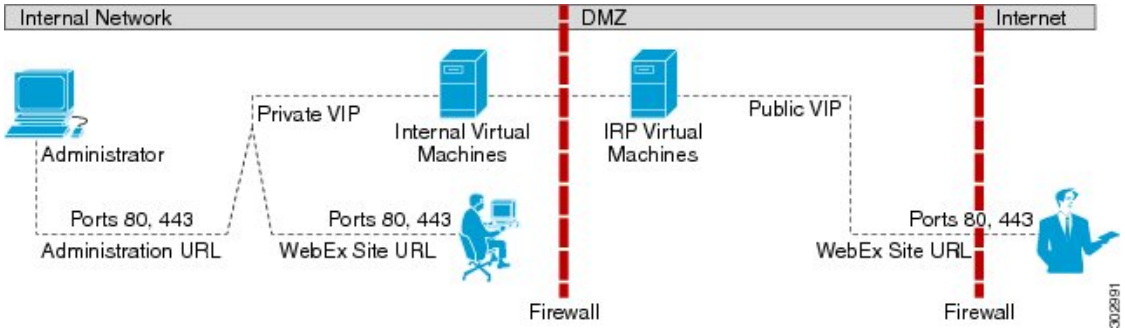
Note This configuration can only support mobile access from a public IP (internet) network. Mobile access is not supported on an internal (intranet) network.

In a split-horizon deployment, Internet-origin traffic (including mobile users employing a cellular data network) goes to the Internet Reverse Proxy. Internal-origin traffic (including mobile users employing local Wi-Fi) goes directly to the internal virtual machines.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the Webex site URL using the private virtual IP (VIP) address. External users (outside the firewall) access the Webex site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the Webex site URL using the public VIP address.

You will define the Administration URL, the Webex Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco Webex Meetings Server Administration Guide*.

This is a schematic diagram of a split-horizon network topology.



Note For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network, on page 75.

Split-horizon DNS with Public VIP NAT on the External Firewall

If you have public virtual IP (VIP) NAT configured on the external firewall, you need three DNS servers to deploy split-horizon DNS:

- Internal DNS: This server resolves the Webex Site URL to the Private VIP IP address on the Admin virtual machine. This server permits internal users to access the Webex site internally with a Private VIP.
- DMZ DNS: This server resolves the IRP VM FQDN to the IRP Eth0 IP address and the Webex Site URL to the Public VIP address. This server is required to successfully deploy the IRP virtual machine and to add Public Access to the topology.
- External DNS: This server resolves the Webex Site URL to the public IP address on the External firewall that is being NATed to the Public VIP on the IRP virtual machine.

Advantages of a Split-Horizon Network Topology

- Tight control on the traffic that comes in and goes out of a network.
- There is a separation of network traffic hitting the system, enabling a more distributed spread of the load.

  The traffic coming in from the Internet goes to the Internet Reverse Proxy. The traffic coming from the internal (private network) goes directly to the internal virtual machines (Admin, and if applicable, Media and Web).
- Performance and network latency is better than a non-split-horizon DNS, but worse than an all internal network topology.

Disadvantages of a Split-Horizon Topology

- Of the three different network topologies, this is the most complex setup.
- Requires sophisticated DNS mapping.
- Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.
- Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.
- Because of web redirection for internal users, the Webex site URL is replaced with the URL exposing the hostname of the virtual machine containing the web services and the Media virtual machines.

For details about NIC speed requirements, see Network Bandwidth Requirements, on page 47.

Redundancy in HA or MDC Deployments

High Availability (HA) provides redundancy through failover from a faulty primary Cisco Webex Meetings Server (CWMS) system to a backup CWMS HA system in the same physical location.

CWMS Multi-data center (MDC) deploys multiple data centers, and then joins them into a single CWMS system. Failover is similar to a HA system, except that MDC system data centers are peers both serving users and they are not geographically limited. Deploying multiple data centers geographically close to users improves network performance. A CWMS system cannot support both HA and MDC.

The conditions for redundancy are:

- The HA virtual machines must be co-located in the same data center as the primary virtual machines. All these virtual machines must be on the same VLAN or subnet. The speed and latency requirements for connectivity between the primary and HA components are the same as defined previously for the primary virtual machines. Splitting the primary and HA components of the system between data centers is not supported.

  The MDC virtual machines are not required to be co-located in the same data center.

- Connectivity between all the internal virtual machines must be fully redundant, so that the failure of a switch or network link does not sever the connectivity between the primary and HA or MDC components. To achieve this redundancy, each host server should have redundant connections to multiple Ethernet switches.

- The primary and HA Internet Reverse Proxy (IRP) virtual machines must be on a common VLAN or subnet (typically not the same subnet as the internal virtual machines). Connectivity between the Internet Reverse Proxy virtual machines should also be redundant, in the same manner as the internal virtual machines.

  After joining data centers in an MDC system, IRP can be enabled or disabled on the data centers. The IRP configuration for all data center in the CWMS MDC system must match; there cannot be a mismatch.

The addition of an HA or a MDC system does not increase the total system capacity. Whether you deploy an 800 user system with or without HA, the total system capacity remains the same; the maximum number of simultaneous audio connections is 800.

The HA or MDC system comprises redundant virtual machines for each virtual machine type in your deployment. (For a description of each type of virtual machine, see Virtual Machines In Your System, on page 7.) For example:

- A 50 user system consists of an Admin virtual machine and optionally an Internet Reverse Proxy (IRP) virtual machine for public access. If you add an HA (MDC is not available) system, the combined 50 user system consists of two Admin virtual machines and two IRP virtual machines.

- A primary 250 or 800 user system consists of an Admin virtual machine, a Media virtual machine, and optionally an IRP virtual machine. If you add an HA or a MDC system, the combined 250 or 800 user system comprises two Admin virtual machines, two Media virtual machines, and two IRP virtual machines.

- A primary 2000 user system consists of an Admin virtual machine, three Media virtual machines, two Web virtual machines, and optionally an IRP virtual machine. If you add a HA or MDC system, the combined 2000 user system comprises two Admin virtual machines, four (three plus one redundant) Media virtual machines, three (two plus one redundant) Web virtual machines, and two IRP virtual machines.

In an HA system, the Public and Private VIP addresses are shared with primary system. When one virtual machine is down, the other virtual machine uses the same VIP addresses. Because of this behavior, a virtual machine failure is transparent to users. Meetings continue without placing unusual demands on the DNS infrastructure. However, a shared VIP address can only be implemented on a single network segment or VLAN. Splitting a VLAN across two data centers is not supported.

We require that connectivity between the primary and HA internal virtual machines be within the same data center. This requirement makes it easier to distinguish between a virtual machine failure and a network failure. A split network can cause split meeting connections and conflicting database updates.

In a MDC system, there are two sets of Public and Private VIP addresses. Data replicates across data centers (except for the License Manager). Therefore if a data center goes down or network connectivity is lost, the surviving data center continues to serve users independent of geographic location.

The best way to build a fault tolerant system is when most system components operate as “all active.” However, certain key components, notably the database service, are “active/standby." (Web servers and media components in the HA system are dependent on the primary system components.) Any latency or interruption on the connections results in delays for users, particularly when joining meetings. Latency between media service components increases audio and video latency for some users during meetings. For Cisco Webex Meetings Server, 4 ms of network latency is acceptable between the internal virtual machines.

Related Topics

Virtual Machine Layout in Your Network, on page 37

Network Considerations for the Internet Reverse Proxy

The Internet Reverse Proxy virtual machines share the same general networking requirements as the internal virtual machines. For the non-split-horizon and split-horizon DNS configuration, the Internet Reverse Proxy virtual machines are deployed in your DMZ network and not the internal network.

Restriction Even if the Cisco UCS Servers are configured with two NICs, Cisco Webex Meetings Server does not support pointing one NIC to the Internet and the other NIC to the Intranet. This restriction applies regardless of the mappings between the physical NICs and virtual NICs used by vSphere (and the Internet Reverse Proxy).

The Internet Reverse Proxy virtual machine always connects to a single external VLAN regardless of the number or NICs you use. If you use multiple physical NICs, and they are connected to different switches or routers, the NICs must still be connected to the same VLAN.

Therefore, you cannot use the Internet Reverse Proxy to bridge traffic between two separate network segments (with one pointing to the Internet and the other pointing to the Intranet). The next section describes how you can accomplish this goal.

Latency Between Internal Virtual Machines and the Internet Reverse Proxy

The maximum acceptable round-trip latency on the path between the NIC on the Internet Reverse Proxy and the NIC on any of the internal virtual machines should be established at less than 4 ms. Excess latency on this path will limit the bandwidth usable by end users for audio, video, and desktop sharing. If the latency increases from 4 ms to 8 ms, for instance, the usable bandwidth will drop by half, with the experience progressively degrading as the latency increases.

Note The 4 ms latency limit does not apply to the path between any of Cisco Webex Meetings Server components and end users endpoints.

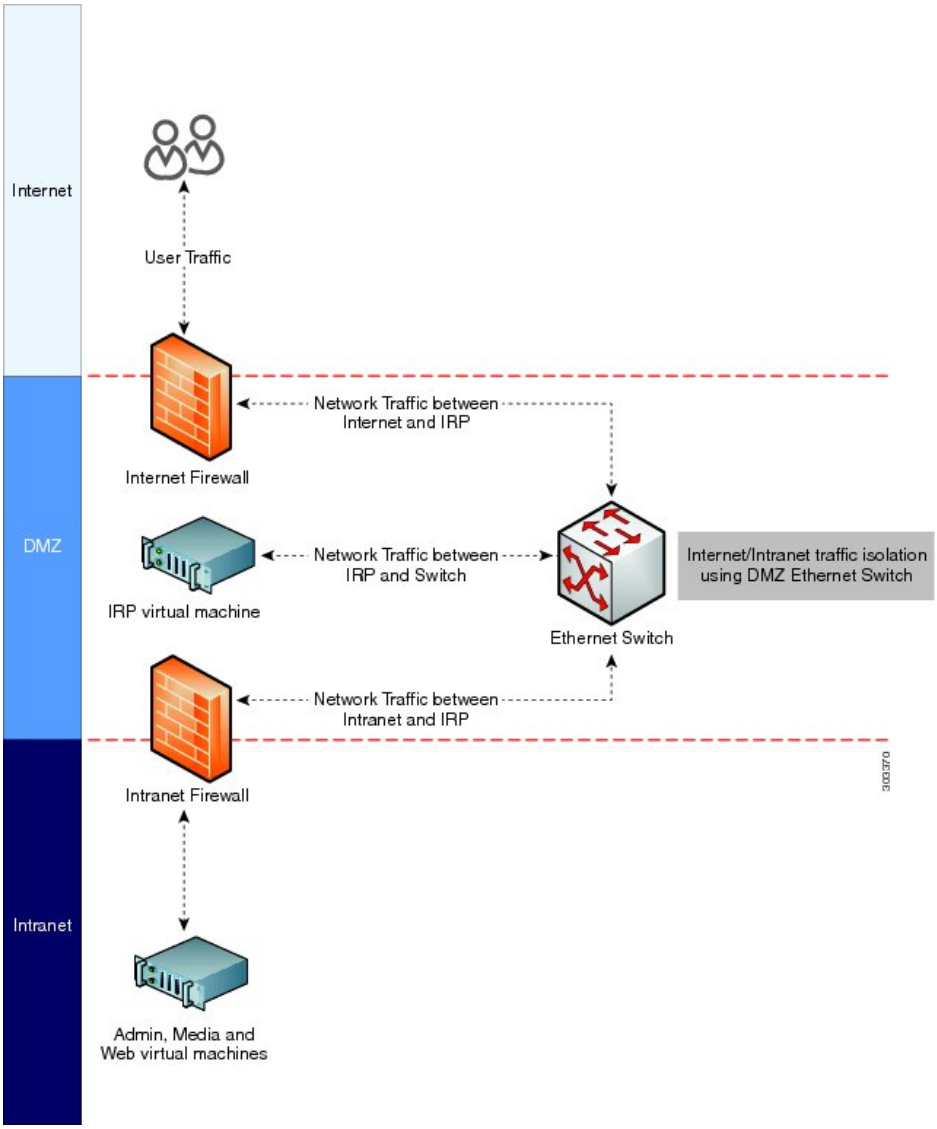
Note Potentially severe delays on end user connections that pass through the Cisco Webex Meetings Server Internet Reverse Proxy can result when latency exceeds 4 ms between the IRP and the internal virtual machines.

Network Traffic Isolation

You may set up network traffic isolation between the Internet and your internal network by using a DMZ Ethernet switch. The following procedure and diagram illustrate one example:

1. Connect the Internet Reverse Proxy to a head-end switch or router and use that switch or router to split the Internet and Intranet traffic.
2. Once the switch or router splits the traffic, then you can pipe those two traffic patterns to two separate physical ports on the switch or router. One port points to the Internet and other port points to the Intranet.

Here is a diagram of a sample network topology:



For information about network bandwidth requirements, see Network Bandwidth Requirements, on page 47.

Network Bandwidth Requirements

This section describes the bandwidth requirements for 50, 250, 800 and 2000 user systems. Meeting the bandwidth requirements outlined in the section will provide a quality end user experience for your users who host and attend Webex meetings, and helps ensure that your network can support the traffic demands from the web sharing, audio, and video.

Estimating Bandwidth for End User Sessions

It is important to estimate the network bandwidth to support the traffic demands of video, audio, and web sharing for the size of your user system. The bandwidth requirements for this product are fundamentally the same as for Cisco Webex cloud services. If you wish to optimize your network provisioning, Cisco Webex cloud services bandwidth usage is presented in the Webex Network Bandwidth White Paper.

The information in the following table shows the expected bandwidth for video, audio and web sharing.

Webex Meeting Component	Aggregate End User Session Bandwidth
Video (360p + 6 thumbnails)	1.5 Mb/s
Audio	0.1 Mb/s
Web sharing (This value assumes you flip a slide every 30 seconds.)	0.6 Mb/s
Total maximum bandwidth	2.2 Mb/s

Although 2.2 Mb/s is the maximum expected bandwidth for a single user connection, Cisco recommends using the maximum expected bandwidth of 1.5 Mb/s when calculating bandwidth requirements. Because only one-half of the maximum number of users can employ video, audio, and web sharing while the remaining users should use only audio and web sharing, this yields an average bandwidth of approximately 1.5 Mb/s per user connection.

If you refer to the *Webex Network Bandwidth White Paper*, you will notice that the bandwidth values in the preceding table are based on worst-case traffic conditions. Average bandwidth utilization is *much* smaller, but Cisco recommends using worst case numbers for the following reasons:

- Using the worst case numbers for your calculation should help you provide the needed bandwidth to prevent a degraded user experience as a result of heavy usage.
- The Cisco Webex Meetings Server sends the same data simultaneously to all the participants in a meeting. When a Webex host flips a page on a presentation, an image of that page (possibly comprising several megabytes) is sent separately to each endpoint, simultaneously, and as quickly as possible.

Bandwidth on Network Paths

Use the following process to determine the necessary bandwidth on various network paths.

1. Determine the averaged bandwidth for a user session using the table provided in the preceding section.
2. Determine the maximum number of users you expect to connect simultaneously over that link.
3. Multiply the total bandwidth by the maximum number of users.

Scenario examples:

- If you expect a maximum of 100 users to connect concurrently from the Internet, you will probably need 1.5 Mb/s x 100 = 150 Mb/s of available bandwidth on your ISP connection and through your external firewall to the Internet Reverse Proxy. For details about Internet Reverse Proxy, see Network Considerations for the Internet Reverse Proxy, on page 45
- Assume you have a 2000 user system with all connections going through the Internet Reverse Proxy. In this scenario, you need to assume traffic for all 2000 users will connect to the Internet Reverse Proxy, and then from the Internet Reverse Proxy to the internal virtual machines. The aggregate bandwidth coming into the Internet Reverse Proxy from other parts of the network will be 2000 x 1.5 Mb/s = 3 Gb/s. For details about non-split-horizon, see Non-Split-Horizon Network Topology, on page 39.

Note The same 3 Gb/s of traffic passes inbound and outbound through the Internet Reverse Proxy, requiring the NIC on the Internet Reverse Proxy to handle 6 Gb/s of user traffic. See the next section for more information about bandwidth requirements for the NIC on the Internet Reverse Proxy.

- Assume you have 2000 user system in a split-horizon DNS deployment. In this scenario, your Internet users will connect to the Internet Reverse Proxy while intranet users connect directly to the internal virtual machines. Assume ten percent of your users connect to a meeting using the Internet versus 90 percent of users connect to their meetings through the Intranet. The result is the aggregate bandwidth coming into the Internet Reverse Proxy will now be approximately 300 Mb/s (10 percent of 2000 users times 1.5 Mb/s equals 300 Mb/s). If that same 300 Mb/s of traffic passes from the Internet Reverse Proxy, the NIC on the Internet Reverse Proxy may be required to handle 600 Mb/s of user traffic. This is a dramatically lower bandwidth requirement than with a non-split-horizon DNS deployment described in the previous scenario. The reduction in network traffic has direct bearing on the recommendations for NIC or switch interface speed (see next section) which can result in you being able to deploy less expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network. For more details about split-horizon, see Split-Horizon Network Topology, on page 42.

Note You may be required to deploy 1 Gigabit Ethernet NICs configured for NIC Teaming if the Internet Reverse Proxy usage is marginally close to the 1000 Mb/s threshold.

See NIC Teaming for Bandwidth Aggregation, on page 51 for more details.

Bandwidth on Cisco Webex Meetings Server Network Interfaces

For direct interfaces between your switching architecture and your system, we recommend provisioning your interface NICs to the maximum speeds shown in the following table. These speeds apply to the connectivity between the Cisco UCS Servers and ports on head-end switches in your local switching infrastructure only. These are the recommended speeds needed to support worst-case traffic requirements.

System Capacity	NIC or Switch Interface Speed
50 user system	1 Gb/s

System Capacity	NIC or Switch Interface Speed
250 user system	1 Gb/s
800 user system	10 Gb/s [15][16]
2000 user system	10 Gb/s[17]

15 You may optionally choose to reduce network infrastructure costs by deploying NIC Teaming using two or more Gigabit Ethernet NICs on the UCS Server and NIC Teaming on the head-end switch.

16 For 800 user systems, if your deployment is using internal DAS storage, you can optionally choose to reduce network infrastructure costs by deploying NIC Teaming using two or more Gigabit Ethernet NICs on the UCS Server and NIC Teaming on the head-end switch. However, if your deployment is using SAN or NAS storage, you will need a 10 Gigabit Ethernet link.

17 If you have a non-split-horizon DNS deployment, the 10 Gb/s requirement pertains to the IRP and internal virtual machines. If you have a split-horizon DNS deployment, you may be able to reduce the network infrastructure demands on your IRP (and DMZ network), which can result in you being able to deploy less expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network, as described in the "Bandwidth on Network Paths" section. However the 10 Gb/s speed requirement holds true for the internal virtual machines (and internal network).

See the next section, "Bandwidth Considerations for Split-Horizon DNS Deployments," for more information about using 1 Gb/s NICs and Ethernet switches for a split-horizon DNS deployment.

Assumptions for NIC Speed Calculations:

- The aggregate end-user session bandwidth (1.5 Mb/s) was used to calculate the NIC speeds shown in the preceding table.
- The inter-virtual machine control traffic must be free of congestion. This especially applies to 2000 user systems and any system provisioned for high availability. Severe congestion on virtual machine links can result in system instability and consequent interruption of service.
- The connections to NAS storage, used for recording and database backup, must not be congested.
- Protocol overhead and implementation inefficiencies result in usable link bandwidth that is significantly less than the 1 Gb/s or 10 Gb/s speed labels.
- If a large percentage of your traffic will hit the Internet Reverse Proxy when users log in to meetings, you need to remember that every user connection passes twice through the NIC on the Internet Reverse Proxy (inbound and outbound). Using the 2000 user system as an example, this means the NIC on the Internet Reverse Proxy may be required to handle 6 Gb/s of user traffic (2000 users times 1.5 Mb/s equals 3 Gb/s, times two for inbound and outbound traffic equals 6 Gb/s).

Conservatively, we ask that the local connections be no more than 60 percent used for end user media traffic, allowing the remaining 40 percent to be available for other traffic, unusual traffic bursts, and network overhead. Using the 800 user system as an example, we estimate the end user traffic at 1.2 Gb/s for the Admin and Media virtual machines and 2.4 Gb/s for the Internet Reverse Proxy virtual machine. Applying the 60 percent rule, we want the NIC to be capable of handling 2 Gb/s for the Admin and Media virtual machines (1.2 Gb/s estimated user traffic for the Admin and Media virtual machines divided by 60 percent estimated normal bandwidth consumption equals 2.0 Gb/s) and 4 Gb/s for the Internet Reverse Proxy virtual machine.

Note The NIC speeds shown in the preceding table do not account for bandwidth used for accessing SAN storage. If Fibre Channel over Ethernet (FCoE) is used for a SAN connection, it should be provisioned to use an independent network interface.

Bandwidth Considerations for Split-Horizon DNS Deployments

With a split-horizon DNS deployment, some of your users will be logging in to meetings from the Internet and that traffic will hit the Internet Reverse Proxy, while the majority of users who are on the internal network will be logging into meetings without hitting the Internet Reverse Proxy. With a split-horizon DNS deployment, if you speed up your network and segment your traffic so that most of your traffic stays within the internal network (as opposed to hitting the Internet Reverse Proxy), you can potentially use NIC Teaming and provision a lower-end NIC (1 Gb/s NIC) on the Internet Reverse Proxy and provision the switching infrastructure between the Internet Reverse Proxy and the Internet to be 1 Gb/s, or at least lower than the recommended 10 Gb/s, for a 2000 user system.

For example, if a company has 100 users who want to access a 2000 port user system from the Internet concurrently, you would need a bandwidth of 150 Mb/s (1.5 Mb/s aggregate user session bandwidth * 100 users = 150 Mb/s). This implies that a network infrastructure from the DMZ network to the Internet Reverse Proxy can be 1 Gb/s Ethernet switches, and the Ethernet NIC interface on the Internet Reverse Proxy can be 1 Gb/s, as opposed to the stated 10 Gb/s interface requirement. Even when you factor in that the Internet Reverse Proxy sees double the traffic (meaning its NIC would have to handle 300 Mb/s of user traffic), applying the 60 percent rule (explained in the "Bandwidth on Cisco Webex Meetings Server Network Interfaces" section) translates to 500 Mb/s. A 1 Gb/s link is still sufficient, but it would not be sufficient if we assumed 250 users instead of 100 users.

Note The optimization of bandwidth is only applicable for the NIC on the Internet Reverse Proxy in a split-horizon DNS deployments.

For non-split-horizon DNS deployments, you must deploy 10 Gb/s Ethernet switches and Ethernet NIC interfaces on the Internet Reverse Proxy.

Network Requirements for Multi-data Center

Requirements for a network link between two data centers:

- Guaranteed bandwidth of 4.5 Mbps for essential inter-data center communications.
- Less than 200 ms latency (round-trip time delay).

Data center network requirements for inter-data center cascaded meetings:

- Each cascaded meeting with audio and Web requires 0.16 Mbps.
- Each cascaded meeting with LQ video at 180p, audio, and Web requires 0.66 Mbps.
- Each cascaded meeting with HQ video at 360p, audio, and Web requires 1.20 Mbps.
- Less than 200 ms latency (round-trip time delay).

For example, a worst case a 2000 user system (maximum number of 1000 meetings are cascaded. Half of them can have Video, and half are without:

- *HQ video :* 500 x 1.2 + 500 x 0.16 = 680 Mbps
- *LQ video:* 500 x 0.66 + 500 x 0.16 = 410 Mbps

For an 800 user system:

- *HQ video:* 680 / 2000 x 800 = 272 Mbps
- *LQ video:* 410 / 2000 x 800 = 164 Mbps

For a 250 user system:

- *HQ video:* 680 / 2000 x 250 = 85 Mbps
- *LQ video:* 410 / 2000 x 250 = 51.25 Mbps

Additional information can be found at http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/white-paper-listing.html.

NIC Teaming for Bandwidth Aggregation

Configuring NIC Teaming on your UCS Servers that contain the ESXi host with the internal virtual machines provides two advantages: NIC Teaming load balances the network traffic between physical and virtual networks, and provides failover in the event of a hardware failure or a network outage. In addition, for deployments where 10 Gb/s infrastructure is not available, it may be possible for you to team multiple 1 Gb/s NICs to achieve an equivalent result.

Note For more information about NIC speeds required for different size user systems, see the section "Bandwidth on Cisco Webex Meetings Server Network Interfaces" in this chapter.

Cisco supports NIC Teaming for bandwidth load balancing for all user system sizes--50, 250, 800, and 2000 user systems--but it is most useful for customers who are trying to optimize networking costs for an 800 user system. If your deployment is using internal DAS storage, the aggregate bandwidth requirements to and from Cisco UCS Servers and the head-end switches for an 800 user system are projected to be similar to using Dual 1 Gigabit Ethernet NICs (or Quad 1 Gigabit Ethernet NICs on a system with HA) to support worst-case traffic requirements, thereby alleviating the need to provision the UCS Servers with 10 Gigabit Ethernet NICs (or to purchase 10 Gigabit Ethernet head-end switches).

Note If your deployment is using SAN or NAS storage, the aggregate bandwidth requirements to and from Cisco UCS Servers and the head-end switches for an 800 user system is 10 Gigabits Ethernet.

Note For information about provisioning NIC teaming in VMware, refer to the VMware documentation at http://kb.vmware.com and search for "NIC teaming in ESXi/ESX".

Assuming the use of traditional network interfaces and Ethernet switches, you can provide redundancy by using NIC teaming and duplicate switches, as outlined in the following process:

- Set up an Ethernet switch which supports IEEE 802.3ad/IEEE 802.1ax Link Aggregation Control Protocol (LACP).
- Using vCenter, connect the virtual machine port group associated with the Cisco Webex Meetings Server virtual machines to both physical adapters.
- Connect both physical adapters to the switch.
- Provision the switch to statically provision the two ports as a team.
- Using VMware vSphere, set NIC Teaming to Active/Active to allow throughput on both NIC interfaces.

For example, for an 800 user deployment, two 1 Gb/s links may be substituted for each 10 Gb/s link on the ESXi host with the internal virtual machines, and four 1 Gb/s links may be substituted for each 10 Gb/s link on the Internet Reverse Proxy. (To get fault tolerance on a system with HA, as described in the section "Redundant Network Connections for HA Deployments", it is necessary to double the number of links.) With the ESXi host with the internal virtual machines, connect two 1 Gb/s links to the first Ethernet switch *plus* two 1 Gb/s links to the second Ethernet switch.

Note The example server configurations shown in the *Cisco Webex Meetings Server System Requirements* do not include sufficient network interfaces to support NIC Teaming for this purpose.

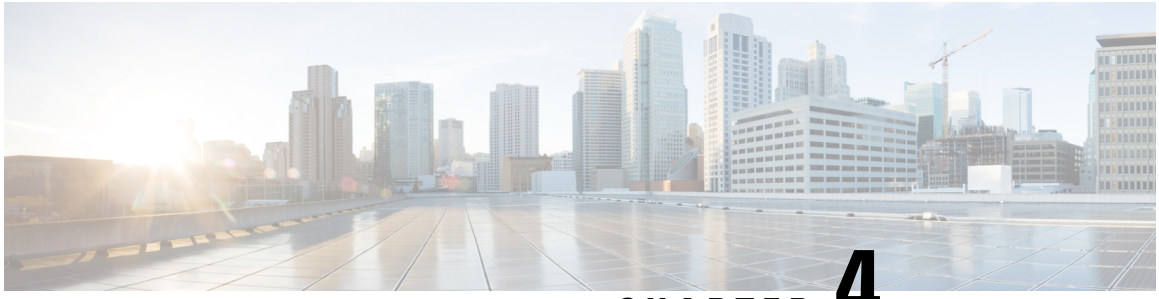
Load Balancing

Load balancing is always done on CWMS no matter what type of traffic is being handled and it is not configurable.

The system attempts to balance the load equally on all web nodes. When the deployment is a system without High Availability (HA), connections are balanced among all web nodes on that system. In the case of a HA deployment, the system uses the web nodes on both the primary system and the HA system for load balancing. In the event of a failure of one, but not all web nodes, the system remains active, but capacity is reduced.

The Internet Reverse Proxy (IRP) node is an entry point and most load balancing decisions are made there. Only one IRP node is active on a system. A system without HA deployment has only one IRP node. A system with HA deployment has two IRP nodes, one IRP is active while the other is inactive. Depending on the DNS configuration, IRP serves all external traffic (and all internal traffic in case of non-split DNS).

If there is a failure involving multiple hosts, functionality and capacity might be affected.



CHAPTER 4

Networking Changes Required For Your Deployment

Networking Checklist for Your System

The networking checklist lists the networking changes required for your system, depending on your DNS configuration and whether or not you enable public access (allowing users to host or attend meetings from the Internet or a mobile device).

Choose the appropriate checklist depending on whether you are using automatic system deployment (recommended for 50, 250, or 800 user deployments) or manual system deployment (required for a 2000 user deployment).

- All virtual machines, including the Internet Reverse Proxy, are in your internal network (easiest configuration)
  - Networking Checklist for an Installation or Expansion, with an Automatic Deployment and Public Access, on page 54
  - Networking Checklist for an Installation or Expansion, with a Manual Deployment, Public Access, and All Internal Virtual Machines, on page 56
- Non-split-horizon DNS (the most common DNS configuration)
  - Networking Checklist for an Installation or Expansion, with Automatic Deployment, Public Access, and a Non-Split-Horizon DNS, on page 59
  - Networking Checklist for an Installation or Expansion, with Manual Deployment, Public Access, and a Non-Split Horizon DNS, on page 61
- Split-horizon DNS
  - Networking Checklist For an Installation or Expansion, with Automatic Deployment, Public Access, and a Split-Horizon DNS, on page 64
  - Networking Checklist for an Installation or Expansion, with Manual Deployment, Public Access, and a Split-Horizon DNS, on page 66
- Systems without public access
  - Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access, on page 69
  - Networking Checklist For an Installation or Expansion, with Manual Deployment and No Public Access, on page 71

Networking Checklist for an Installation or Expansion, with an Automatic Deployment and Public Access

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. We recommend that you choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Verify that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Verify that the Internet Reverse Proxy virtual machines are in your internal network.
- Verify that the ESXi hosts for all your virtual machines (including the Internet Reverse Proxy) are managed from the same VMware vCenter.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	Internal (may be on the same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to the public VIP address)	Internal (same subnet as the Internet Reverse Proxy). This IP address must be publicly routable.	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	Internal [same subnet as the primary system Internet Reverse Proxy (but can use NAT with a private IP address)]	

DNS Configuration

Update the DNS server as follows. There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you cannot use, see Webex Site and Webex Administration URLs, on page 73.

Task	Examples
Hostnames and IP addresses of the internal virtual machines: Admin virtual machine and, if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Administration site URL and Private VIP address.	• <Administration-site-URL> <Private-VIP-address>
Webex site URL and Public VIP address.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a subnet that is separate from the internal (Admin or Media) virtual machines. See Port Access When All the Virtual Machines Are in the Internal Network, on page 74.

Network Routing Configuration

Task	Examples
Enable Layer 3 routing between the internal and DMZ networks.	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
Verify that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet. [As you are deploying all your system virtual machines internally (the Internet Reverse Proxy is not in the DMZ), this subnet must be in the internal network.]	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verify that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist for an Installation or Expansion, with a Manual Deployment, Public Access, and All Internal Virtual Machines

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your internal network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	Internal (may be on the same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to the public VIP address)	Internal (same subnet as the Internet Reverse Proxy) **Note** This IP address must be publicly routable.	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	Internal—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you may not use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Update your DNS Server with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with Webex site URL and Public VIP address information.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines.

Although it is not recommended, we do also support placing all of your virtual machines (Internet Reverse Proxy and internal) on the same subnet. See Port Access When All the Virtual Machines Are in the Internal Network, on page 74.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Task	Compare These IP Addresses
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet. **Note** As you are deploying all your system virtual machines internally (the Internet Reverse Proxy is not in the DMZ), then this subnet must be in the internal network.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist for an Installation or Expansion, with Automatic Deployment, Public Access, and a Non-Split-Horizon DNS

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. We recommend that you choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Verify that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Verify that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the Internet Reverse Proxy	DMZ (but can use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to the public VIP address)	DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ [same subnet as the primary system Internet Reverse Proxy (but can use NAT with a private IP address)]	

DNS Configuration

Update the DNS server as follows. There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you cannot use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Hostnames and IP addresses of the internal virtual machines: Admin virtual machine and, if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Administration site URL and Private VIP address.	• <Administration-site-URL> <Private-VIP-address>
Webex site URL and Public VIP address.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a subnet that is separate from the internal (Admin or Media) virtual machines. See Port Access When All the Virtual Machines Are in the Internal Network, on page 74.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable Layer 3 routing between the internal and DMZ networks.	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
Verify that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verify that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist for an Installation or Expansion, with Manual Deployment, Public Access, and a Non-Split Horizon DNS

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to the public VIP address)	DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you may not use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Update your DNS Server with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with Webex site URL and Public VIP address information.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 75.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>

Task	Compare These IP Addresses
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist For an Installation or Expansion, with Automatic Deployment, Public Access, and a Split-Horizon DNS

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. We recommend that you choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Verify that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Verify that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but can use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to two VIP addresses):	• Internal users—Internal (same subnet as Admin virtual machine) • External users—DMZ (same subnet as the Internet Reverse Proxy)	

Description	Network Location	IP Address
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ [same subnet as the primary system Internet Reverse Proxy (but can use NAT with a private IP address)]	

DNS Configuration

Update the DNS server as follows. There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you cannot use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Hostnames and IP addresses of the internal virtual machines: Admin virtual machine and, if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Hostname and IP address for the DMZ virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Webex site URL, Administration site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <Webex-site-URL> <Private-VIP-address>
Webex site URL and Public VIP address.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a subnet that is separate from the internal (Admin or Media) virtual machines. See Port Access When All the Virtual Machines Are in the Internal Network, on page 74.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable Layer 3 routing between the internal and DMZ networks.	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
Verify that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verify that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist for an Installation or Expansion, with Manual Deployment, Public Access, and a Split-Horizon DNS

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to two VIP addresses) • internal users—private VIP address • external users—public VIP address	• Internal users—Internal (same subnet as Admin virtual machine) • External users—DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you may not use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Task	Example
Update your DNS server (that enables internal lookup) with the hostname and IP address for the DMZ virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server (that enables internal lookup) with Webex site URL, Administration site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <Webex-site-URL> <Private-VIP-address>
Update your DNS server (that enables external lookup) with Webex site URL and Public VIP address information.	• <Webex-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, we recommend that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 75.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>

Task	Compare These IP Addresses
Ensure that the Private VIP address and internal virtual machines (Admin virtual machine and if applicable, the Media and Web virtual machines) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. We recommend that you choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

Verify that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	Internal (same subnet as primary system Admin virtual machine)	

DNS Configuration

Update the DNS server as follows. There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you cannot use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Hostnames and IP addresses of the internal virtual machines: Admin virtual machine and, if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Webex site URL, Administration site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <Webex-site-URL> <Private-VIP-address>

Firewall Configuration

Task	Example
Configure all the firewalls inside your internal network to permit web browsers to access the Private VIP address.	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

Network Routing Configuration

Task	Compare These IP Addresses
Verify that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist For an Installation or Expansion, with Manual Deployment and No Public Access

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Webex site URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the Webex site URL and the Administration site URL. For a list of the words that you may not use, see Webex Site and Webex Administration URLs, on page 73.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server with Administration site URL, Webex site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <Webex-site-URL> <Private-VIP-address>

Firewall Configuration

Make the following changes to your firewalls.

Task	Example
Configure all the firewalls inside your internal network to permit web browsers to access the Private VIP address.	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Webex Site and Webex Administration URLs

Webex Site URL

Users access the Webex site URL to schedule, host, or attend meetings. This URL resolves to either the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.

- Resolves to the public VIP address for all users, when you do not have split-horizon DNS.
- Resolves to the public VIP address for external users when you have split-horizon DNS.
- Resolves to the private VIP address for internal users when you have split-horizon DNS.

Note Ports 80 and 443 must be open for the Webex site URL.

Webex Administration URL

Administrators access the Webex Administration URL to configure, manage, and monitor the system. This URL resolves to the private VIP address.

Note Ports 80 and 443 must be open for the Webex Administration URL.

Names for the Webex Site and Webex Administration URLs

You may choose almost any names for these URLs, comprising all lowercase characters. However, you cannot use the following as the hostname in the URLs:

- the same name as the hostnames for any of the virtual machines in the system
- authentication
- client

- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- webex

Port Access When All the Virtual Machines Are in the Internal Network

This section describes the port access required in the external firewall when all the system virtual machines (Admin, and if applicable, Media, Web, and Internet Reverse Proxy) are in the internal network. This is the Internal Internet Reverse Proxy network topology.

Ensure that the firewall or any load balancing solution redirects requests to the ports listed below to ensure end users can host and join meetings successfully.

- TCP Port 80 to the public virtual IP (VIP) address

- TCP Port 443 to the public virtual IP (VIP) address

Note The Web node and Admin node send SMTP requests to the configured Email server. If there is a firewall between the internal Web and Admin virtual machines and the Email server, SMTP traffic might be blocked. To ensure Email server configuration and Email notification work properly, port 25 or 465 (secure SMTP port number) must be open between the Email server and the Web and the Admin virtual machines.

Port Access With an Internet Reverse Proxy in the DMZ Network

This section describes the port access required in the internal and external firewalls when you have internal virtual machines (Admin, and if applicable, Media and Web) in the internal network, and the Internet Reverse Proxy (IRP) in the DMZ network.

Configure access control lists (ACLs) on the switch that permits traffic to the ESXi hosts for the system virtual machines.

Port Access in the External Firewall

Enabled public access by opening port 80 (HTTP) in addition to port 443 (HTTPS), so users can enter the Webex site URL without having to remember whether it is HTTP or HTTPS. Although port 80 is open, all the network traffic flows over port 443 (SSL encrypted HTTPS).

Important Ensure that the firewall or any load balancing solution redirects requests to the ports listed below to ensure users can host and join meetings successfully.

Restriction Configure TCP port 64700 on the IRP machine to deny any requests that come to the public VIP address. In the external firewall, this limits access to this port for requests only from the Admin virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	443	Any external clients.	Public VIP (Eth1) of the IRP.	External clients access the Webex site URL by using HTTPS. TCP connections are initiated from the external client machines to the IRP virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	80	Any external clients.	Public VIP (Eth1) of the IRP.	External clients accessing the Webex site URL by using HTTP. TCP connections are initiated from the external client machines to the IRP virtual machines.
TCP	8444 (Introduced in 2.5MR1, 2.6, and 2.0MR6HF.)	Any external clients.	Public VIP (Eth1) of the IRP.	External clients accessing the Webex recordings by using HTTPS. TCP connections are initiated from the external client machines to the IRP virtual machines.
UDP	53	Real IP (Eth0) of the IRP.	DNS server.	This is needed if you have a firewall between the virtual machines and the DNS server, for your system to deploy and operate successfully.

Port Access in the Internal Firewall

If you have restrictions on connections from the internal network to the DMZ network, then the table in this section applies. Allow TCP connections *outbound* from the internal network to the DMZ network segment.

Note No TCP connections need to be allowed from the DMZ segment in to the internal network for this product to work properly.

Note Using iptables or access control lists (ACLs), configure the firewall so that connections to port 64616 only come from the Admin virtual machine.

Note The Web node and Admin node send SMTP requests to the configured Email server. If there is a firewall between the internal Web and Admin virtual machines and the Email server, SMTP traffic might be blocked. To ensure Email server configuration and Email notification work properly, port 25 or 465 (secure SMTP port number) must be open between the Email server and the Web and the Admin virtual machines.

Note Especially when the IRP is in the DMZ network, allow Internet Control Message Protocol (ICMP) echo requests and replies. Otherwise, the IRP detect and the DNS server availability validation might fail if the ICMP echo reply is not received.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64001	All internal virtual machines (Eth0 IP).	Real IP (Eth0) of the IRP virtual machines.	Establishes reverse connections to the IRP. TCP connections are established from the internal virtual machines to the IRP virtual machines.
TCP	64002	Admin and web virtual machines (Eth0 IP).	Real IP (Eth0) of the IRP virtual machines.	Establishes reverse connections to the IRP. TCP connections are established from the internal virtual machines to the IRP virtual machines.
TCP	7001	All internal virtual machines (Eth0 IP).	Real IP (Eth0) of the IRP virtual machines.	Establishes reverse connections to the IRP. TCP connections are initiated from the internal virtual machines to the IRP virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64616	Admin virtual machines (Eth0 IP).	Real IP (Eth0) of the IRP virtual machines.	Bootstrap the IRP. TCP connections are initiated from the Admin virtual machines to the IRP virtual machines. **Note** Using iptables or access control lists (ACLs), configure the firewall so that connections to port 64616 only come from the Admin virtual machine.
TCP	22	Any internal client machines.	Real IP (Eth0) of the IRP virtual machines.	Troubleshooting the IRP virtual machines using a Remote Support Account.
TCP	443	Any internal client machines.	Private VIP (Eth1) of the Admin virtual machines. Real IP (Eth0) of the Media virtual machines.	Internal users accessing the Webex site URL by using HTTPS. TCP connections are established from the internal client machine to the Admin virtual machine.
TCP	443	Private VIP (Eth1) of the Admin virtual machines and Real IP (Eth0) of the Media virtual machines.	Public VIP (Eth1) of the IRP.	
TCP	65002	Any internal client machines.	Any internal virtual machines.	Controls network traffic between internal virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	65102	Any internal client machines.	Any internal virtual machines.	Controls network traffic between internal virtual machines.
TCP	80	Any internal client machines.	Private VIP (Eth1) of the Admin virtual machines.	Internal users accessing the Webex site URL using HTTP. TCP connections are established from the internal client machine to the Admin virtual machine.
UDP	53	All internal virtual machines (Eth0 IP).	DNS server.	If you have a firewall between the virtual machines and the DNS server, for your system to deploy and operate successfully.
TCP	8443	Cisco Webex Meetings Server Web Node.	CUCM	For AXL traffic in a multi-data center system between Cisco Webex Meetings Server and CUCM to allow LDAP CUCM failover.

VMware vCenter Ports

Ports Open for Deployment

These are some of the ports that are used during the deployment of a Single-data Center (SDC) Cisco Webex Meetings Server (CWMS). Once the deployment completes, you can close any ports that were opened solely for the deployment.

TCP Port 443 should be open, in both directions, between vCenter and the Admin virtual machine for secure https management during an automatic system deployment. The Admin virtual machine uses this port to provide vCenter credentials to deploy the virtual machines automatically in vCenter.

The ports listed below are used for communication between the ESXi host and vCenter. If the ESXi host and vCenter are connected to a *separate management network*, you may not need to open these ports through the firewall. For a complete list of ports used by vCenter and the ESXi host, see your VMware documentation.

- UDP/TCP Port 902 in both directions between vCenter and the ESXi hosts for vCenter management
- (Optional) TCP Port 22 from the vSphere client to the ESXi hosts for SSH management
- UDP Port 514 from the ESXi hosts for your system to the internal syslog
- TCP Port 5989 in both directions between vCenter and the ESXi hosts for XML management

The default UDP port used for external clients for audio and video data transmission is SSL (port 443).

Ports Open to Support Multi-data Center

Ports to open between the CWMS internal virtual machines	tcp 8080 tcp 8081 tcp 8082 tcp 9809 tcp 9810 tcp 9811 tcp 9812 tcp 9813 tcp 9814 tcp 9815 tcp 9816 tcp 9817 tcp 9818 tcp 9819 tcp 9820 tcp 9840 tcp 6502 tcp 12340 tcp 12342 tcp 12442 tcp 7001 tcp 7003 tcp 7004 tcp 7005 tcp:5060 tcp 5061 tcp 5062 tcp 5063 tcp 22
Ports to open between the CWMS internal virtual machines and Virtual IPs	tcp 443 tcp 80
Ports to open between Internet Reverse Proxy IPs and the CWMS internal virtual machines	tcp 7001 tcp 64001 tcp 64700 tcp 64616
UDP ports to open between the CWMS internal virtual machines [18]	udp range:10000:19999 udp range:16000:32000 udp-rtp range:16384:32767 udp range:9000:9011 (Medium system) udp range:9000:9009 (Large system) udp 5060 udp 5062

[18] Media components for PC audio and video use these ports.

Cisco Webex Meeting Center Ports

- The UDP ports used for internal clients for audio and video data transmission between UDP and SSL include:
  - For 50 user systems, use UDP port 9000
  - For 250 user systems, use UDP ports 9000, 9001, 9002, 9003
  - For 800 user systems, use UDP ports 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009, 9010, 9011
  - For 2000 user systems, use UDP ports 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009
- With the appropriate network settings, internal media servers allow connections through any port used by Meeting Center.
- The Internet Reverse Proxy only accepts connections from Webex Meetings through TCP ports 80 and 443.

Using NAT With Your System

Network Address Translation (NAT) traversal is supported for virtual machine IP addresses and for the virtual IP addresses (Public and Private VIPs) that are used in your system.

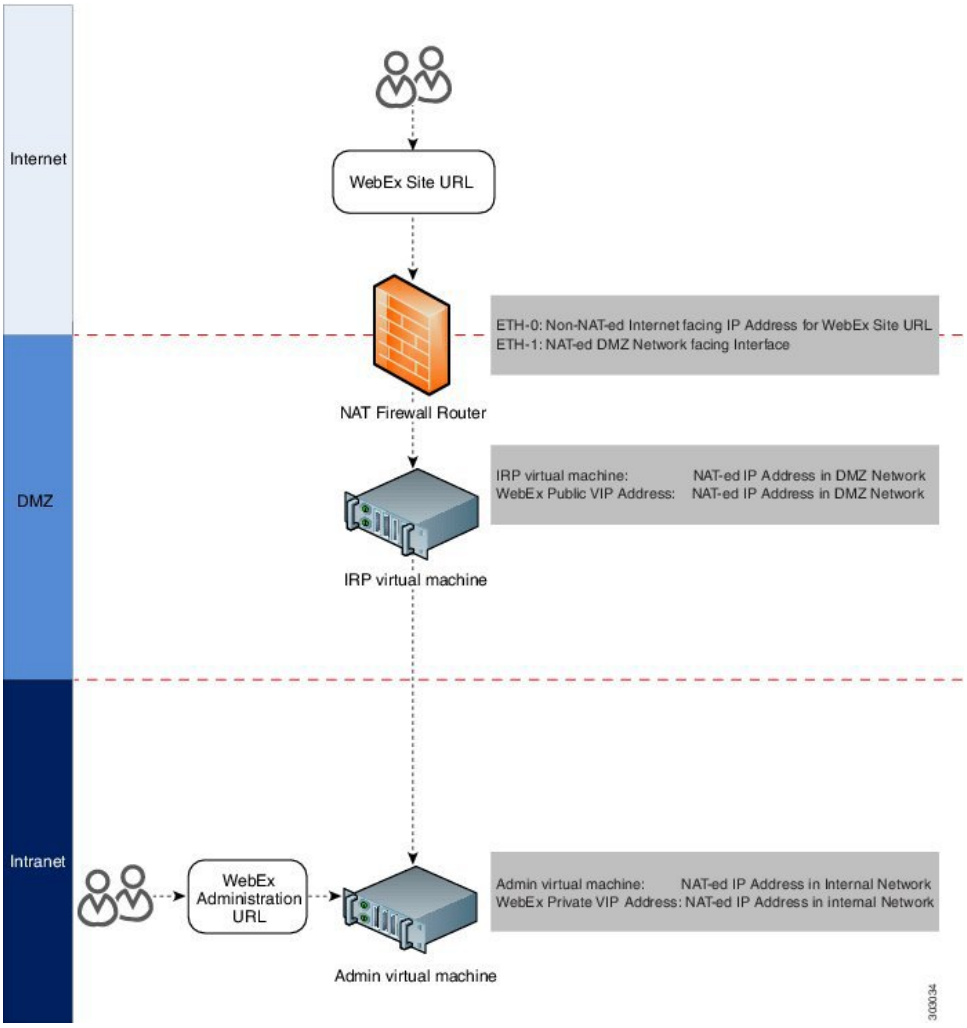
The following schematic diagram illustrates a typical NAT traversal for a 50 user system without High Availability (HA). By using NAT, you can reduce the number of *public IP addresses* required for the product to just one IP address, instead of two (or three if you deploy HA). You can also deploy similar NAT deployments as long as these meet the overall system requirements.

Important The use of multiple NATs and firewalls tends to increase latency, affecting the quality of real time-traffic for users.

Also, when using multiple NAT domains, routing between these various NAT domains can be challenging. You can use NAT-ed IP addresses as long as the following requirements are met:

- All the virtual machines in the system can use NAT-ed IP addresses, with the exception of the Internet Reverse Proxy virtual machine. NAT between the Administration virtual machine and the Internet Reverse Proxy virtual machine is not supported. The IP address of the Internet Reverse Proxy virtual machine (its real IP address) must be reachable by the Administration virtual machine through the internal network.
- The public VIP address itself does not need to be publicly visible, but it must be translatable from the Internet.
- When deploying public access, the Webex site URL must be mapped to an Internet-visible IP address. This Internet-visible IP address must be accessible by external users and *also* map to the public VIP address you configure during the system deployment.

  You can choose to make the public VIP address visible from the Internet. If you choose not to make it publicly visible, then it must be translatable from the Internet.



In the diagram, an external user accesses the Webex site to join or host a meeting. Following a DNS lookup, the IP address for the Webex site is the NAT public IP address (Eth0). This NAT public IP address is for the external NAT firewall router (Firewall and NAT router 1), between the external network and the DMZ network.

The firewall router receives this request from the external user, and internally routes the request to the NAT private IP address for the router (Eth1, exposed to the DMZ network). Eth1 then sends the request to the public VIP address (also a NAT IP address in the private networking segment for the Webex site).

You can use NAT IP addresses for the public VIP address, and the Internet Reverse Proxy IP addresses. The only NAT public IP address is the Eth0 IP address for the NAT firewall router.

Note To ensure this NAT firewall router (between the Internet and DMZ network) routes the incoming packet correctly, set port mapping configuration on the NAT device, or apply other similar mechanisms to ensure the packet is routed correctly to the public VIP address and the Internet Reverse Proxy.

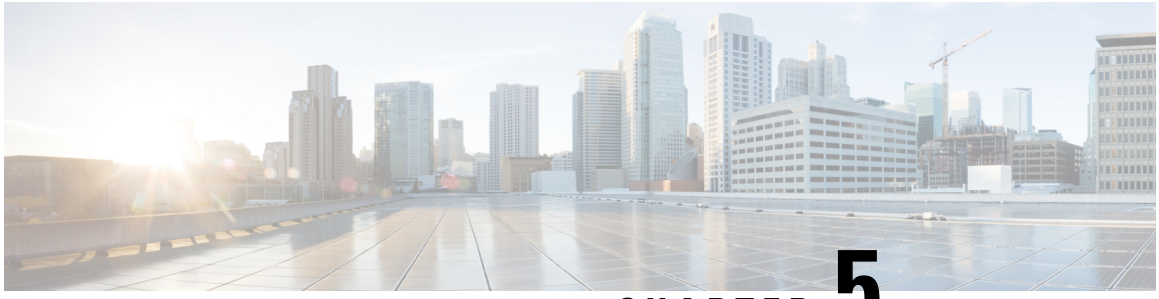
There is usually a second internal NAT firewall router between the DMZ network and the internal network. Similar to the external NAT firewall router, Eth0 is a DMZ NAT private IP address and is an interface to the DMZ network. Eth1 is also a NAT private IP address that is an interface to the internal network.

You can use NAT IP addresses for the private VIP address and the Administration virtual machine IP addresses.

For more information about NAT, see http://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html.

Forward Proxies

If your network topology includes forward proxies, they *must meet specific requirements* for the Internet Reverse Proxy to work properly. See "Use of Forward Proxies in Your System" in the *Cisco Webex Meetings Server Troubleshooting Guide* for complete details.



CHAPTER 5

Configuring Cisco Unified Communications Manager (CUCM)

Configuring Cisco Unified Communications Manager

To enable teleconferencing on Cisco Webex Meetings Server you must configure one (or more) Cisco Unified Communications Manager (CUCM) system to manage call control. Optionally you can configure a second CUCM system for audio high availability.

CUCM in an MDC Environment

The CUCM configurations in a Multi-data Center (MDC) environment are the same as in a Single-data Center (SDC) environment. Configuration parameters modified on one data center are automatically matched on the other data center.

On CUCM, the basic configurations in a Multi-data Center (MDC) environment are the same as in a Single-data Center (SDC) environment. However, you must configure trunks to all data centers. Each data center can have

a different route pattern. If you want to use more than one CUCM, each data center must have a SIP trunk to the CUCM in the other data centers for calls to transfer.

CUCM Secure Teleconferencing in an MDC Environment

It is not possible to import certificates from all data centers in a Multi-data Center (MDC) into a single Cisco Unified Call Manager (CUCM) as needed to secure teleconferencing when the common name of both certificates is the same.

By default, the common name for all data centers is the global site URL of the system. However, to make the common name unique, you can generate certificates. For more information, see Generating a Certificate Signing Request (CSR), on page 100. Select the local site URL instead of the global site URL to use in the common name.

Self-signed certificates generated during any system altering procedure (such as changing the site or administration URL, changing hostnames) results in a certificate that has the global site URL in the common name, so you must manually create certificates with the local site URL after this type of operation.

CUCM Configuration for Extended Systems

When you extend a large system, you must configure another SIP Trunk for each new media server that you add. A large system requires 3 SIP Trunks, so an extra large system requires 4–6, depending on the numbe of extension units.

Before You Begin

Obtain your Load Balancer Point and Application Point information from your Cisco Webex Meetings Server **Audio** page. Load balancer points manage call load balancing and application points manage calls, conference flow, and feature control. Systems of different sizes have different numbers of load balancer points and application points and the numbers are not customized. Sign into your Administration site and select **Settings** > **Audio** to see this information.

- Size (50/250/800/2000)
- High availability
- Transport type

On the **Audio** page, there is a SIP Configuration Table that displays load balancer point and application point information including IP addresses and ports. This table is also displayed on the **Configuring Your Audio Settings for the First Time** page that appears the first time you configure your audio settings.

To make CUCM work with Cisco Webex Meetings Server, CUCM requires the following base and specific configurations:

- Base configuration

Note These configurations can be shared with multiple Cisco Webex Meetings Server systems.

- SIP trunk security profile
- SIP profile

- Specific configuration

Note These configurations must be made for individual Cisco Webex Meetings Server systems and cannot be shared by multiple systems.

- Certificate management
- SIP trunk
- Route group
- Route list
- Route pattern
- SIP route pattern

CUCM Configuration Checklist for Multi-data Center

The configuration checklist displays the number of each Cisco Unified Communication Manager (CUCM) configuration type that you must configure for your system with Multi-data Center (MDC).

System Size	Security Profiles (Base Configuration)	SIP Profiles (Base Configuration)	SIP Trunks (Specific Configuration)	Route Groups (Specific Configuration)	Route Lists (Specific Configuration)	Route Patterns (Specific Configuration)	SIP Route Patterns (Specific Configuration)
250 users	2	1	4	1	1	N	2
800 users	2	1	4	1	1	N	2
2000 users with HA	2	1	6	1	1	N	4

CUCM Configuration Checklist with or without High Availability

The configuration checklist displays the number of each Cisco Unified Communication Manager (CUCM) configuration type that you must configure for your Single-data Center (SDC) system with or without High Availability (HA).

System Size	Security Profiles (Base Configuration)	SIP Profiles (Base Configuration)	SIP Trunks (Specific Configuration)	Route Groups (Specific Configuration)	Route Lists (Specific Configuration)	Route Patterns (Specific Configuration)	SIP Route Patterns (Specific Configuration)
50 users	2	1	2	1	1	N[19]	1

System Size	Security Profiles (Base Configuration)	SIP Profiles (Base Configuration)	SIP Trunks (Specific Configuration)	Route Groups (Specific Configuration)	Route Lists (Specific Configuration)	Route Patterns (Specific Configuration)	SIP Route Patterns (Specific Configuration)
50 users with HA	2	1	4	1	1	N	2
250 users	2	1	2	1	1	N	1
250 users with HA	2	1	4	1	1	N	2
800 users	2	1	2	1	1	N	1
800 users with HA	2	1	4	1	1	N	2
2000 users	2	1	5	1	1	N	3
2000 users with HA	2	1	6	1	1	N	4

[19] N is the number of Call-In Access Numbers that you configure in Cisco Webex Meetings Server.

Configuring CUCM in a CWMS Multi-data Center System

Typically, each site in a Multi-data Center (MDC) environment has a dedicated CUCM cluster associated with it. CUCM clusters are connected by using inter-cluster trunks (ICT). Each CUCM cluster has call-in/in-dial trunks to the local CWMS site. Session Manager Edition (SME) is supported. CWMS can be configured behind the local CUCM clusters. Each CUCM has SIP REFER trunks to all the media virtual machines in the MDC.

For redundancy, each CUCM cluster can have INVITE trunks to all the data centers. The call-in route pattern gives priority to the INVITE trunk associated with the local data center and uses the INVITE trunk to the remote data center only upon failure.

Note The Extended Capacity feature is not supported in an MDC deployment.

Table 5: CUCM SIP Trunks Configured on Each CUCM Cluster

Deployment	INVITE Trunks - Load Balancer (MACC)	REFER Trunks—Application Point (TAS)
Small	2	2
Medium	2	2
Large	4	6

Configuring CUCM on a 250- or 800-user Multi-data Center System

Configure Cisco Unified Communication Manager (CUCM) for 250- or 800-user Multi-data Center systems. Typically, each data center has a local CUCM cluster.

Before you begin

Collect the following information:

- One load balance point IP address for each data center
- One application point IP address for each data center
- The number of call-in access numbers you will configure on your system

Procedure

Step 1 Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.

Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.

Step 2 Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.

Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure two SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 7 Configure *N* route patterns by using the above route list.

N is the number of call-in access numbers that you configured in your audio settings on the Administration site. See Configuring a Route Pattern.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

Configuring CUCM on a 2000-user Multi-data Center System

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user Multi-data Center (MDC) system. Typically, each data center has a local CUCM cluster.

Before you begin

Information required:

- Two load balance point IP addresses for each data center
- Three application point IP addresses for each data center
- The number of call-in access numbers you will configure on your system

Procedure

Step 1 Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.

Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.

Step 2 Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.

Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure four SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 7 Configure *N* route patterns by using the above route list.

N is the number of call-in access numbers that you configured in your audio settings on the Administration site. See Configuring a Route Pattern.

Step 8 Configure four SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

Configuring CUCM for High-Availability and Non-High-Availability Systems

The following sections provide a description of the tasks required to configure high-availability and non-high-availability systems of various sizes.

Configuring CUCM on 50-, 250-, and 800-User Systems without High Availability

Configure CUCM for 50-, 250-, and 800-user systems without High Availability.

Before you begin

Obtain the following information:

- One load balance point IP address
- One application point IP address
- The number of call-in access numbers you will configure on your system

Procedure

Step 1 Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.

Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.

Step 2 Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.

Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.

Step 3 Configure one SIP trunk for your load balance point.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure one SIP trunk for your application point.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 7 Configure *N* route patterns by using the above route list.

N is the number of call-in access numbers that you configured in your audio settings on the Administration site. See Configuring a Route Pattern.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

Configuring CUCM on 50-, 250-, or 800-User Systems with High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 50-, 250-, or 800-user systems with high availability.

Information Required

- Two load balance point IP addresses
- Two application point IP addresses
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.
2	Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.	Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.
3	Configure two SIP trunks for your load balance points.	See Configuring a SIP Trunk on a Load Balance Point.
4	Configure two SIP trunks for your application points.	See Configuring a SIP Trunk for an Application Point.
5	Configure one route group by using the SIP trunk that you configured for your load balance point in Task 3, above.	See Configuring a Route Group.
6	Configure one route list by using the route group that you configured in Task 5, above.	See Configuring a Route List.

Task	Description	Detailed Information
7	Configure *N* route patterns by using the above route list. *N* is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See Configuring a Route Pattern.
8	Configure two SIP route patterns for your application points.	See Configuring a SIP Route Pattern.

Configuring CUCM on a 2000-User System without High Availability

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user system without High Availability.

Before you begin

Obtain the following information:

- Two load balance point IP addresses
- Three application point IP addresses
- The number of call-in access numbers you will configure on your system

Procedure

Step 1 Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.

Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.

Step 2 Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.

Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.

Step 3 Configure two SIP trunks for your load balance point.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure three SIP trunks for your application point.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 7 Configure *N* route patterns by using the above route list.

N is the number of call-in access numbers that you configured in your audio settings on the Administration site. See Configuring a Route Pattern.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

What to do next

Configuring CUCM on a 2000-User System with High Availability

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user system with High Availability.

Before you begin

Obtain the following information:

- Two load balance point IP addresses
- Four application point IP addresses
- The number of call-in access numbers you will configure on your system

Procedure

Step 1 Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.

Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 95 and Configuring a SIP Trunk Security Profile for an Application Point, on page 96.

Step 2 Review the existing SIP profile and determine whether or not it satisfies your Cisco Webex Meetings Server setup requirement. If it does not, configure one SIP profile.

Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 97.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure four SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 7 Configure *N* route patterns by using the above route list.

N is the number of call-in access numbers that you configured in your audio settings on the Administration site. See Configuring a Route Pattern.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

What to do next

Configuring a SIP Trunk Security Profile

Configuring a SIP Trunk Security Profile for a Load Balance Point

Before you begin

If your Cisco Webex Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **System** > **Security** > **SIP Trunk Security Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields.

- Name—Enter a name to identify your SIP trunk security profile.
- Device Security Mode—Select **No Secure** if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

  Note If you want CUCM to communicate with Cisco Webex Meetings Server by using TLS, a different Cisco Webex Meetings Server system cannot share the same SIP Trunk Security Profile because each system must have a different certificate. Obtain the Cisco Webex Meetings Server certificate name from the Administration site. For more information refer to "Managing Certificates" in the *Administration Guide*.

- Incoming Port— Enter `5060` if you want CUCM to communicate with Cisco Webex Meetings Server using UDP/TCP. Enter `5061` if you want CUCM communicates Cisco Webex Meetings Server using TLS.

Note Do not configure any of the other fields on the page; leave the default settings.

Step 6 Select **Save**.

Configuring a SIP Trunk Security Profile for an Application Point

Before you begin

If your Cisco Webex Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **System** > **Security** > **SIP Trunk Security Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name to identify your SIP trunk security profile.
- Device Security Mode—Select **Non Secure** if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

  Note If you want CUCM to communicate with Cisco Webex Meetings Server by using TLS, a different Cisco Webex Meetings Server system cannot share the same SIP Trunk Security Profile, because each system must have a different certificate. Obtain the Cisco Webex Meetings Server certificate name from the Administration site. For more information refer to "Managing Certificates" in the *Administration Guide*.

- Incoming Port— Enter `5062` if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Enter `5063` if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

Note Do not configure any of the other fields on the page; leave the default settings.

Step 6 Select **Save**.

Configuring a SIP Profile

Configuring a Standard SIP Profile

The standard Session Initiation Protocol (SIP) profile uses the default settings and requires no additional configuration steps.

Configuring a TLS SIP Profile

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Device Settings** > **SIP Profile**.

Step 4 Click **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.
- Redirect by Application—Select the check box.

Do not configure any of the other fields on the page; leave the fields with their default settings.

Step 6 Click **Save**.

Configuring an IPv6 SIP Profile

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Device Settings** > **SIP Profile**.

Step 4 Click **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.

- Enable ENAT—Select the check box.

Do not configure any of the other fields on the page; leave the fields with their default settings.

Step 6 Click **Save**.

CUCM Certificate Management by Using TLS

If you want Cisco Unified Communications Manager (CUCM) to communicate with Cisco Webex Meetings Server (CWMS) by using TLS, you must perform the following actions:

- Obtain a CWMS certificate from the Administration site and upload it to CUCM.

Note If CWMS uses third-party certificates, all certificates in the certificate chain must be uploaded to CUCM.

- Download your CUCM certificate, and then upload it to CWMS Administration site.

Note If CUCM uses third-party certificates, only the last certificate in the certificate chain (Root Certificate Authority (CA) certificate) must be uploaded to CWMS.

If you use TLS to connect all the data centers in a Multi-data Center (MDC) system to the same CUCM, CWMS cannot use the common site URL for the certificate common name. You must use each data center local site URL for each certificate common name, because the CUCM 10.5 and older versions treat multiple certificates with a common name as same certificate. If the names are not different, the second data center certificate replaces the first data center certificate after uploading the second data center certificate into CUCM.

Refer to "Managing Certificates" in the *Administration Guide* for more information. See http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html for more details.

Uploading Cisco Webex Meetings Server Certificates

Procedure

Step 1 Download and export your Cisco Webex Meetings Server certificate.

a) Sign in to the Cisco Webex Meetings Server Administration site.
b) Select **Settings** > **Security** > **Certificates**.
c) Copy the certificate name from the SSL Certificate section.
d) Select **More Options** > **Export SSL certificate**.
e) Save your certificate to your local hard drive.

Step 2 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 3 Click **Cisco Unified OS Administration**.

Step 4 Click **Security** > **Certificate Management**.

Step 5 Click **Upload Certificate/Certificate Chain**.

Step 6 Click **CallManager-trust** in the Certificate name drop-down menu.

Step 7 Click **Browse** button and select the certificate that you saved to your local hard drive.

Step 8 Click **Upload File**.

The system displays a "Success: Certificate Uploaded" message.

Step 9 Click **Close**.

Installing a Third-Party CUCM Certificate

This procedure explains how to upload a third-party certificate to your Cisco Webex Meetings Server.

Before you begin

Generate a Certificate Signing Request (CSR) and send it to a third part certificate authority to apply for certificates.

The certificate authority sends you a certificate chain that can have the following:

- Certificate 1 (user) - issued to a user entity by an intermediate certificate authority.
- Certificate 2 (intermediate) - issued to an intermediate certificate authority by a root certificate authority.
- Certificate 3 (Root CA) - issued by the root certificate authority.

When you receive multiple certificates in a certificate chain, concatenate the three certificates into one file, with the user certificate first.

Procedure

Step 1 Import your third-party certificate file into your Cisco Webex Meetings Server as described in the *Cisco Webex Meetings Server Administration Guide* available from http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Step 2 Sign in to http://ccm-server/, where *ccm-server* is the fully qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 3 Select **Cisco Unified OS Administration**.

Step 4 Select **Security** > **Certificate Management**.

Step 5 Select **Upload Certificate/Certificate Chain**.

Step 6 Select **CallManager-trust** in the Certificate name drop-down menu.

Step 7 Select **Browse** button and select the Root Certificate Authority (CA) certificate that you saved to your local hard drive.

This is the last, self-signed certificate from the verification chain, which is used to verify the `CallManager.pem` certificate.

Note You can obtain the Root CA certificate from a certificate authority directly, at the same time the `CallManager.pem` certificate is created.

Step 8 Select **Upload File**.

Wait for your system to indicate "Success: Certificate Uploaded."

Step 9 Select **Close**.

What to do next

For more information about certificates, refer to the *Managing Certificates* section in the *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Downloading CUCM Certificates

This procedure is required only if CUCM uses self-signed certificates. If CUCM uses third party certificates, upload only the last certificate (Root CA certificate) in the certificate chain to your Cisco Webex Meeting Server. Contact your Certificate Authority (CA) for information about how to obtain a Root CA certificate.

For more information about generating CUCM certificates, see the CUCM documentation.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified OS Administration**.

Step 3 Click **Security** > **Certificate Management**.

Step 4 Search for the certificate in "Certificate Name" field for the certificate with name "CallManager". Select the ".PEM File" field.

Step 5 Click **Download** to save the CUCM certificate `CallManager.pem` on your local hard drive.

What to do next

For more information on uploading CUCM certificates to Cisco Webex Meetings Server, refer to "Managing Certificates" in the *Administration Guide*. See http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html.

Generating a Certificate Signing Request (CSR)

The hashing method used to generate Certificate Signing Request (CSR) and private key for SSL certificates uses SHA2 (SHA256).

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Click **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.

On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Click **Generate CSR** for the desired type of CSR.

On November 1, 2015, Certification Authorities (e.g. VeriSign, GoDaddy, and so forth) stopped issuing certificates for internal domain names (e.g. domain.local , domain.internal). Before CWMS version 2.0MR9, you could upload only a single SSL certificate with Subject Alternative Names for all components in the deployment, but this requires you to purchase expensive SAN SSL certificates for a complete solution. As of CWMS version 2.5MR5 you can purchase on Webex Site URL SSL a certificate from Certification Authority for use on IRP servers, and use Self-signed SSL certificates for the internal network virtual machines.

Step 4 Complete the fields on the **Generate CSR (Certificate Signing Request)** page.

Option	Description
Common Name	Click **Local Site URL** certificate, **Global Site URL** certificate, or **Wildcard** certificate.
Subject Alternative Names This option appears only if you select **Subject Alternative Name** for your Common Name type.	Your administration site and virtual machine names. No subject alternative names are required if you selected a wildcard common name.
Organization	Enter the organization name.
Department	Enter the department name.
City	Enter the city.
State/Province	Enter the state or province.
Country	Click the country.
Key Size	Click the key size.2048.
Hash Algorithm	Click the Hash Algorithm SHA256.

Step 5 Click **Generate CSR**.

The **Download CSR** dialog box appears.

Step 6 Click **Download**.

You receive a ZIP file that contains the CSR and the associated private key. The CSR file is called `csr.pem` and the private key file is called `csr_private_key.pem`.

Step 7 Back up your system by using VMware Data Recovery or VMware vSphere Data Protection.

Backing up your system preserves the private key if it becomes necessary to restore it.

Configuring a SIP Trunk

Note When deploying a 2000-user system with High Availability (HA) and multiple load balance and application points, each load balancer and application point in the CWMS solution requires a dedicated SIP trunk. Multiple destination IP addresses within the same SIP trunk are not supported.

Configuring a SIP Trunk on a Load Balance Point

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Trunk**.

Step 4 Click **Add New**.

Step 5 On the **Trunk Type** drop-down menu, select **SIP Trunk**.

Note Do not change any other fields on this page; leave the parameters at their default settings.

Media Termination Point Required should be unchecked on the **Trunk Configuration** page when CUCM is communicating with Cisco Webex Meeting Server. If you are not using Cisco Webex Meetings Server with CUCM SIP audio, select **Media Termination Point Required** when providing telephony services by using a third-party PBX infrastructure.

Step 6 Click **Next**.

Step 7 Configure the following fields:

- Device Name—Enter a name for the SIP trunk.
- Device Pool—Select an appropriate device pool from the drop-down menu.

  To determine which Cisco Unified Communications Manager Group has been configured on that device pool, go to **System** > **Device Pool menu**. To verify which Cisco Unified Communications Managers are part of this group, go to **System** > **Cisco Unified CM Group**.

  Note Record the IP addresses of the primary and secondary server. These IP addresses are entered when you configure your audio settings in Cisco Webex Meetings Server. See "Configuring Your Audio Settings for the First Time" in the *Administration Guide* for more details. See Cisco Webex Meetings Server Install and Upgrade Guides.

- Destination Address—Enter your load balance point IPv4 address. Refer to the SIP Configuration table on your Administration Site Audio page for the IP address.
- Destination Address IPv6—Enter your load balance point IPv6 address if you want to enable IPv6 between CUCM and Cisco Webex Meetings Server.
- Destination Port—Enter `5060` if you want CUCM to communicate with Cisco Webex Meetings Server using UDP/TCP. Enter `5061` if you want CUCM to communicate with Cisco Webex Meetings Server using TLS.
- SIP Trunk Security Profile—Select a security profile for your load balance point, from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco Webex Meetings Server using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco Webex Meetings Server using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco Webex Meetings Server.
- Calling Search Space—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM. Go to **Call Routing** > **Class of Control** > **Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
- Rerouting Calling Search Space and Out-Of-Dialog Refer Calling Search Space—Select a Calling Search Space and Out-Of-Dialog Refer Calling Search Space that contains the route partition that is configured for the SIP route pattern. See Configuring a SIP Route Pattern. If it is set to **< None >**, then the system only routes calls to route patterns with the route partition set to **< None >**, so the SIP route pattern must have the route partition set to **< None >**. This configuration is necessary to enter meetings in Cisco Webex Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide* for more information.

Note Do not change any other fields on this page; leave the parameters at their default settings.

Step 8 Click **Save**.

Step 9 Click **Reset** and then select **Reset and Restart** in the popup window.

Configuring a SIP Trunk for an Application Point

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Trunk**.

Step 4 Click **Add New**.

Step 5 On the **Trunk Type** drop-down menu select **SIP Trunk**.

Note Do not change any other fields on this page; leave the values at their default settings.

Step 6 Click **Next**.

Step 7 Configure the following fields:

- Device Name—Enter a name for your SIP trunk.
- Device Pool—Select **Default** from the drop-down menu.
- Destination Address—Enter the application server IPv4 address.
- Destination Address IPv6—Optionally enter the application server IPv6 address to enable IPv6 between CUCM and Cisco Webex Meetings Server.
- Destination Port—Enter `5062` if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Enter `5063` if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.
- SIP Trunk Security Profile—Select your application server security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco Webex Meetings Server.
- Calling Search Space—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM that you want to enable Cisco Webex Meetings Server to call. Select **Call Routing** > **Class of Control** > **Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. If this is set to **< None >**, this will only be able to call devices or route patterns with a partition set to **< None >**. For more information, refer to *Calling Search Space Configuration* in the *Cisco Unified Communications Manager Administration Guide* or *Partitions and Calling Search Spaces* in the *Cisco Unified Communications Manager System Guide*.

Note Do not change any other fields on this page; leave the values at their default settings.

Leave the **Media Termination Point Required** check box deselected on the **Trunk Configuration** page when CUCM is communicating with Cisco Webex Meeting Server. If you are not using Cisco Webex Meetings Server with CUCM SIP audio, you can select the **Media Termination Point Required** check box when providing telephony services using a third-party PBX infrastructure.

Step 8 Click **Save**.

Step 9 Click **Reset** and then select **Reset and Restart** in the pop-up window.

You must reset the SIP trunk to complete the configuration.

Configuring a Route Group

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Call Routing** > **Route/Hunt** > **Route Group**.

Step 4 Click **Add New**.

Step 5 Configure the following fields

- Route Group Name—Enter a name for your route group.
- Distribution Algorithm. Select **Circular** from the drop-down menu.

  Note By selecting **Circular**, you enable CUCM to distribute a call to idle or available users starting from the (N+1)th member of a route group, where the Nth member is the member to which CUCM most recently extended a call. If the Nth member is the last member of a route group, CUCM distributes a call starting from the top of the route group.

- Find Devices to Add to Route Group—Select **SIP trunk of Load Balance Point** from the **Available Devices** list. Then click **Add to Route Group**.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 6 Click **Save**.

What to do next

Create a route list for your route group. Proceed to Configuring a Route List, on page 105.

Configuring a Route List

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Call Routing** > **Route/Hunt** > **Route List**.

Step 4 Click **Add New**.

Step 5 Configure the following fields

- Name—Enter a name for your route list.

- Cisco Unified Communications Manager Group—Select **Default** from the drop-down menu.

Note Do not change any other fields on this page; leave the fields at their default settings.

Step 6 Click **Save**.

Step 7 Click **Add Route Group**.

The **Route List Detail Configuration** page appears.

Step 8 Select the previously configured route group from the **Route Group** drop-down menu, and the click **Save**.

The **Route List Configuration** page appears.

Step 9 Click **Save**.

What to do next

Configure a route pattern for your route list. Proceed to Configuring a Route Pattern, on page 106.

Configuring a Route Pattern

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 4 Click **Add New**.

Step 5 Configure the following fields

- **Route Pattern**—Enter a name for your route pattern.

  Note Add a route pattern for each Blast Dial group. Record this name because you must enter it on the Administration **Settings** > **Audio** > **Blast Dial Group** page when you create a Blast Dial group.

- **Route Partition**—Select a route partition that is accessible by phones or devices that can call Cisco Webex Meetings Server. If this set to **< None >** any device configured in CUCM would be able to call Cisco Webex Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

- **Gateway/Route List**—Select the previously configured route list from the drop-down menu.

Note Do not change any other fields on this page; leave these fields at their default settings.

Step 6 Click **Save**.

Configuring a SIP Route Pattern

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Click **Cisco Unified CM Administration**.

Step 3 Click **Call Routing** > **SIP Route Pattern**.

Step 4 Click **Add New**.

Step 5 Configure the following fields

- Route Partition—Select a route partition that is included in the calling search space that is configured as the Rerouting Calling Search Space from the section "Configuring a SIP Trunk for an Application Point" above. If this set to **< None >** then the Rerouting Calling Search Space configured for the SIP trunk for an application point must be set to **< None >**. For more information refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
- Pattern Usage—Select **IP Address Routing**.
- IPv4 Pattern—Enter the application point IP address. See the SIP Configuration table on the Audio page in Webex Site Administration, to locate the IP address.
- SIP Trunk—Select the previously configured SIP trunk for the application point from the drop-down menu.

Note Do not change any other fields on this page; leave these fields at their default settings.

Step 6 Click **Save**.

IP Addressing Mode Preferences

You can configure IP Addressing Mode Preferences globally, or make the preferences device specific by creating a Common Device Configuration.

To configure global settings, go to **System** > **Enterprise Parameters**. Configure your preferences on the **CUCM Enterprise Parameters** page.

To make the configuration device specific, go to **Device** > **Common Device Configuration**. Configure your preferences on the **CUCM Common Device Configuration** page.

Save the configuration, which you can later select when you create the trunks for CWMS.

Important CWMS supports either the IPv4 or IPv6 setting for **IP Addressing Mode Preference for Media**.

CWMS doesn't support the IPv6IP setting for **Addressing Mode Preference for Signaling**. CWMS supports only IPv4 for SIP Signaling. Setting **IP Addressing Mode Preference for Signaling** to use IPv6 disables the connection between CUCM and CWMS, and therefore disables teleconferencing.

CUCM Feature Compatibility and Support

CUCM Feature Compatibility

Cisco Webex Meetings Server (CWMS) supports Cisco Unified Call Manager (CUCM) 8.6 or 9.0 without TLS/SRTP, and CUCM 9.1, 10.0, 10.5, 11.0(1a), 11.5, 11.5(1)SU1 and later service updates (SU), and 12.0SU1 and later SUs.

For a list of CUCM releases tested with CWMS, see the *Release Notes for Cisco Webex Meetings Server* for your release.

Important TLS connections between CUCM and CWMS fail with releases of CUCM that do not support certificates that are signed with a signature algorithm SHA256 with RSA encryption.

Upgrade CUCM to a version that supports this signature algorithm or obtain a third-party certificate that is signed with SHA1 with RSA encryption. According to the latest National Institute of Standards and Technology (NIST) recommendation, SHA1 should no longer be used for digital signature generation as this has a security vulnerability.

The following table provides feature compatibility for the supported versions of CUCM. Cisco Webex Meetings Server system capacity is not affected by any of your configuration choices.

Note CWMS does not support any unlisted CUCM versions or other third-party SIP proxy management applications.

Table 6: Feature Compatibility for the Supported Versions of CUCM

Feature	Pre-Conditions/Remarks
Call out (IPv6)	Configure CWMS with IPv6 addresses during the installation process.
Call in (IPv6)	Configure CWMS with IPv6 addresses during the installation process.
TLS/SRTP	Configure CWMS system security certificates.
RFC2833	Select this option during CUCM SIP trunk configuration.
KPML	Select this option during CUCM SIP trunk configuration.

Feature	Pre-Conditions/Remarks
Keepalive—CWMS sending	Performed by using the SIP OPTIONS message.
Keepalive—CWMS receiving	Performed by using the SIP OPTIONS message.
Quality of Service	Control packets.
TCP	Make sure that your default ports are: 5060 for conferencing load balance points; 5062 for conferencing application points.
TLS	Make sure that your default ports are: 5061 for conferencing load balance points; 5063 for conferencing application points.
UDP	Make sure that your default ports are: 5060 for conferencing load balance points; 5062 for conferencing application points.
Self-signed certificates	n/a
Third-party certificates	n/a

Supported Telephony Call Features

Note The CUCM 9.0 software that is part of the BE6K (Business Edition 6000) product is supported by CWMS.

- Call hold
- Call un-hold
- Caller ID display on EP
- Calling name display on EP
- Call transfer (IPv4 to IPv4)
- Call transfer (IPv6 to IPv4)
- Call transfer (IPv4 to IPv6)
- Call transfer (IPv6 to IPv6)

Telephony Media Features

CWMS supports participants with G.711, G.722, and G.729 codecs at the same time. Changing your codec configuration does not affect system performance. Packet sizes supported on CWMS:

- 10, 20, or 30ms for g.711 audio codecs
- 20ms for g.722 audio codec
- 10, 20, 30, 40, 50, or 60ms for g.729 audio codecs

Feature	G.711	G.722	G.729
Noise Compression	Yes	Yes	Yes
Comfort noise	Yes	No	No
Echo cancellation	No	No	No
Packet loss concealment	Yes	Yes	No
Automatic gain control	Yes	Yes	Yes
Quality of Service	Yes	Yes	Yes

Note All custom audio prompts, including Blast Dial prompts, are: 8KHz, 16-bit, 64kbps, momo, CCITT u-law (G.711).

Audio Endpoint Compatibility

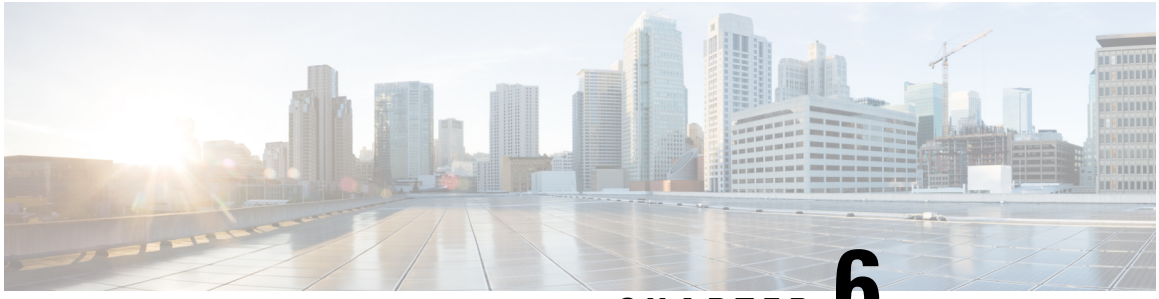
You can use any standards-based audio endpoint that connects to Cisco Unified Communications Manager to join a Webex meeting. The supported audio endpoints include the Cisco IP Phones, Telepresence endpoints, and PSTN devices such as mobile phones and land line phones. Many audio endpoints support audio and video connectivity. However, only audio connectivity to the Cisco Webex Meetings Server is supported.

To permit users to join Webex meetings by using PSTN devices, you must deploy Analog-to-VoIP Gateways, such as Cisco Integrated Service Routers (ISR). The IP phones listed below have been tested with Cisco Webex Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Lifesize video phone
- Tandberg 1000
- Tandberg 1700
- Polycom

- Cisco Cius
- C20
- EX 60
- EX 90

Other Cisco UC-compatible endpoints should also operate normally. For a list of Cisco Unified IP Phones supported by Cisco Unified Communications Manager and the Device Packs available for each model, see Cisco Unified IP Phone Feature and Cisco Unified Communications Manager Device Pack Compatibility Matrix .



CHAPTER 6

Downloading and Mass Deploying Applications

Use of this product requires additional applications that must be downloaded to your users' computers.

About Application Downloads

You can mass-deploy CWMS applications by using the tools available to you on the Webex Site Administration site. The applications available for download include are:

- Webex Meetings desktop app—The core application for scheduling, attending, or hosting meetings.

  If a user does not have the Webex Meetings desktop app installed, the first time that they join a meeting it automatically downloads to the PC. You can configure this to occur on-demand or silently. The user has the option of using the Cisco Webex Meetings desktop app for the duration of the meeting and having it removed when the meeting is over, or performing an installation of the application. Performing an installation speeds up the process of starting or joining future meetings. Installation fails if the user does not have administrator privileges.

- Webex Meetings Desktop Application—Adds meeting management functionality to other applications, such as Microsoft™ Outlook®.

  After an update or upgrade to a system, we recommend that you remove any old versions of Webex Meetings Desktop Application and install the latest version.

- Webex Network Recording Player—Plays back the recordings of meetings. This can include any material displayed during the meeting.

In CWMS the .MSI installer for the applications is available from the **Admin** > **Settings** > **Downloads** page. See "Downloading Applications from the Administration Site" in the CWMS Planning Guide for more information.

We recommend that you push the applications to user computers offline, before you inform those end-users that accounts have been created for them. Pushing the applications ensures that your users can start and join meetings and play network recordings the first time they sign in.

If users have administrator privileges, you can enable users to download the applications from the end-user **Downloads** page and install the applications themselves. No additional administrator action is required.

When **upgrading** to Cisco Webex Meetings Server in a locked-down environment where user PCs do not have administrator privileges, before you start the upgrade procedure push the new version of the Webex Meetings application to all user PCs.

Configure Your Application Download Settings

You can permit users to download the Webex Meetings Desktop Application and the Network Recording Player, or choose to push the applications to users.

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Go to **Settings** > **Downloads**.

Step 3 Choose one of the following options:

- **Allow users to download application**
- **Manually push application to users' desktops**

  If you select this option, click each of the **Download** buttons to download the Webex Meetings Desktop Application and the Network Recording Player.

Step 4 (Optional) Check **Automatically update Webex Meetings Desktop Application when new versions are available**.

Application Language Key

The English application installer file in each ZIP file is without a language suffix. The application installer file for each of the other languages contains an abbreviation in the filename that indicates the language of the application it contains. The table lists the abbreviation used for each language:

Abbreviation	Language
B5	Traditional Chinese
DE	German
ES	Latin American Spanish
FR	French

Abbreviation	Language
GB	Simplified Chinese
IT	Italian
JP	Japanese
KO	Korean
NL	Dutch
PT	Portuguese
RU	Russian
SP	Spanish

Silent Installation Limitations for CWMS Applications When Using SMS

The following limitations apply when you perform a silent installation by using Microsoft Systems Management Server 2003 (SMS):

- SMS per-user mode is not supported.
- If the SMS administrator wants to add a feature for Webex Meetings Desktop Application, run the **REMOVE** command first, and then run the **ADDSOURCE** command.
- If users log on to their computers using remote desktop while their administrator advertises the package, have the users restart their computers.
- Mass deployment is possible, but each user must enter their credentials.
- Before you update to a maintenance release or upgrade to a newer release, have all users uninstall Cisco Webex Meetings Desktop Application. After the update or upgrade, you can manually push the application to your users or they can download it from the **Downloads** page.
- If you are using Lync integration, after a silent installation your users must restart their computers to ensure that all instant messenger integrations work properly.

Create a Package from a Definition

Procedure

Step 1 Open the SMS Administrator Console, and go to **Site Database** > **Package**.

Step 2 Right-click **Package**.

Step 3 Go to **New** > **Package From Definition**.

Step 4 On the **Create Package from Definition** wizard, click **Next**.

Step 5 Click **Browse** to locate and select the MSI package, and then click **Next**.

Step 6 Select **Always obtain files from a source directory**, and then click **Next.**

Step 7 Select Source directory location, and then click **Next**.

Step 8 Click **Finish**.

Cisco Webex Meetings Desktop Application Deployment

Install the Webex Meetings Desktop Application

Installing the Cisco Webex MSI package requires administrator privileges. The MSI package installs to the default OS Programs folder, which requires administrator privileges to access.

If the version of your Windows Installer Service is outdated, an error message appears. To install the Webex MSI package, upgrade to a newer version of the Windows Installer Service.

Procedure

Step 1 Run the installer on the user's computer.

The installation wizard appears with an introductory message.

Step 2 Click **Next** in the following dialogue boxes until you reach the installation dialogue box.

Step 3 Click **Install**.

Step 4 Click **Finish** when the installation is complete.

Uninstall the Webex Meetings Desktop Application

Procedure

Step 1 Sign in to the user's computer.

Step 2 Go to **Start** > **Control Panel** > **Programs and Features**.

Step 3 From the list of programs, choose **Cisco Webex Meetings**, and then click **Uninstall/Change**.

Install Silently—Command Line

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer hard drive.

Step 3 Open the Windows Command prompt.

On Windows 7 and later, you must use run as administrator to open the prompt window.

Step 4 Install all components of the MSI package webexapp.msi by entering the command **`msiexec.exe /qn /i "webexapp.msi"`**.

Uninstall Silently—Command Line

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer hard drive.

Step 3 Open the Windows Command prompt.

On Windows 7 and later, you must use run as administrator to open the prompt window.

Step 4 Uninstall all components of the MSI package webexapp.msi by entering the command **`msiexec.exe /q /x "webexapp.msi"`**.

Advertise—SMS Per-System Unattended Program

You can use Webex Administration to manually push the Cisco Webex Meetings Desktop Application to your users. Alternately you can allow users to download the Webex Meetings Desktop Application from the end-user **Downloads** page.

If you are the Microsoft Systems Management Server 2003 (SMS) administrator, you can advertise Cisco Webex Meetings Desktop Application by using the SMS per-system unattended program.

Procedure

Step 1 Create a package from the definition.

See Create a Package from a Definition, on page 115.

Step 2 Change the program options for **Per-system unattended** before advertisement:

a) Open the SMS administrator console and go to **Site Database** > **Packages** > **Cisco Webex LLC Cisco Webex Productivity Tools 2.82** > **Programs**.

b) Right-click Per-system unattended and select **Properties** to open the **Per-system unattended Program Properties** dialog box.

c) Click the **Environment** tab.

- For the **Program can run** option, select **Only when a user is logged on**.
- For the **Run mode** option, select **Run with administrative rights**. (Do not turn on **Allow users to interact with this program**.)

d) Click the **General** tab.
e) Append additional parameters to the command line, to specify options for Cisco Webex Meetings Desktop Application:

- **`SITEURL="http://sample.webex.com"`** specifies the Webex Site URL used by your company.
- Integration parameters should be uppercase and the default value is 0 (Disabled).

  In the following example, the initial command line is **`msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "webexapp.msi"`**.

  Append Productivity Tools flags and parameters to the command line: **`msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "webexapp.msi" SITEURL="https://sample.webex.com" OI=1 MSN=1`**.

Step 3 Advertise the program.

a) Open the SMS administrator console and go to **Site Database** > **Packages** > **Cisco Webex LLC Cisco Webex Meetings Desktop Application English** > **Programs**.
b) Right-click **Per-system unattended**.
c) Click **All Tasks** > **Distribute Software**.
d) Click **Next** in the **Distribute Program Wizard**.
e) Select the SMS Server, and then click **Next**.
f) Select the collection, and then click **Next**.
g) Enter the advertisement name in the **Name** field, and then click **Next**.
h) Specify whether the advertisement should apply to subcollections, and then click **Next**.
i) Specify when the program will be advertised, and then click **Next**.
j) Specify whether to assign the program, and then click **Next**.
k) Click **Finish** on the **Completing the Distribute Program Wizard** page.
l) Navigate to the **`\Site Database\System Status\Advertisement Status`** directory and check the advertisement status.

   If you enable notification, the user sees a message indicating that the assigned program will run after the program advertisement. The assigned program runs silently.

Install Components—SMS Per-System Unattended Program

To install components of Cisco Webex Meetings Desktop Application, you must first run **`REMOVE`** and then run **`ADDSOURCE`**, even though the components were not previously installed.

Procedure

Step 1 Create a new program named `Add-phase1`, copy all the options from the "per-system unattended program," and then update the command line:

a) Open the SMS administrator console and go to **Site Database** > **Packages** > **Cisco Webex LLC Webex Meetings Desktop Application** > **Programs**.
b) Right-click the blank area and then select **New** > **Program**.

c) Enter the program name and default command line.
d) On the properties dialog, select the **Environment** tab.
   - For the **Program can run** option, select **Only when a user is logged on**.
   - For the **Run mode** option, select **Run with administrative rights**. (Do not turn on **Allow users to interact with this program**.)
e) Update the command-line on the **General** tab.
f)
g) Append **`REMOVE`** to the command line and specify the features that must be added.

   Example:

   If you want to add **`OI`** and **`PITM`** (the PITM value is for the Webex integration to instant messengers), you must **`REMOVE`** them first, even if they are not already installed: **`msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "webexapp.msi" REMOVE="OI,PTIM"`**

Step 2 Advertise the program to the specified collection of work machines in the domain.

Step 3 Create a second program name, “Add-phrase2”, and copy all the options from the “per-system unattended program” and then update the command line:

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco Webex LLC Webex Meetings Desktop Application** > **Programs**.
b) Right-click the blank area and then select **New** > **Program**.
c) Enter the program name and default command line.
d) On the properties dialog box, select the **Environment** tab.
   - For the **Program can run** option, select **Only when a user is logged on**.
   - For the **Run mode** option, select **Run with administrative rights**. (Do not turn on **Allow users to interact with this program**).
e) On the properties dialog box select, the **Advanced** tab.
f) Turn on **Run another program first** and select program **Add-phase1**.
g) Update the command-line on the **General** tab.
h) Append **`ADDSOURCE`** to the command line and specify the features to be added.

   Example:

   To add **`OI`** and **`PITM`**, use the following command: **`msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "webexapp.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1`**

Step 4 Advertise the program to the specified collection of work machines in the domain.

Uninstall Components—SMS Per-System Unattended Program

Perform the following procedure to remove Cisco Webex Meetings Desktop Application by using Microsoft Systems Management Server (SMS):

Procedure

Step 1 Create a new program and copy all the options from the "per-system unattended program" as described in Advertise—SMS Per-System Unattended Program, on page 117, and then update the command line:

a) Open the SMS administrator console and go to **Site Database** > **Packages** > **Cisco Webex LLC Cisco Webex Meetings Desktop Application** > **Programs**.

b) Right-click the blank area, and then go to **New** > **Program**.

c) Enter the program name and default command line.

d) In the **Properties** dialog box, click the **Environment** tab.

- For the **Program can run** option, select **Only when a user is logged on**.
- For the **Run mode** option, select **Run with administrative rights**. (Do not turn on **Allow users to interact with this program**).

e) Update the command-line on the **General** tab.

f) Append **`REMOVE`** to the command line and specify the features that you want to remove.

Example:

If you want to remove **`OI`**, enter the following command: **`msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "webexapp.msi" REMOVE="OI"`**

The PTIM value is for CWMS integration to instant messengers. Example:

```
msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "webexapp.msi" REMOVE="PTIM"
```

Step 2 Advertise the program to the specified collection of work machines in the domain.

Uninstall the Cisco Webex Meetings Desktop Application—SMS Per-System Unattended Program

Procedure

Step 1 Use the SMS Installation package that you created to deploy the Cisco Webex Meetings Desktop Application.

See Create a Package from a Definition, on page 115.

Step 2 Advertise the per-system uninstall program to uninstall the Cisco Webex Meetings Desktop Application.

Adverstise to Update or Upgrade the Version—SMS Per-System Unattended Program

Before you install a maintenance release or upgrade your system to a newer release, have users uninstall Cisco Webex Meetings Desktop Application. After the upgrade, you can use Webex Administration to manually push the application to your users, or users can download it from the end-user **Downloads** page.

Sign in to Webex Administration, go to **Settings** > **Downloads**, and then disable the following settings:

- **Automatically update Webex Meetings Desktop Application when new versions are available.**
- **Allow users to download application.**

Procedure

Step 1 Create a new SMS installation package by using webexapp.msi.

See Create a Package from a Definition, on page 115 for more information.

Step 2 Change the program options for **Per-system unattended** before advertisement.

For more information, see Install Components—SMS Per-System Unattended Program, on page 118.

Step 3 Advertise the program.

For more information, see Install Components—SMS Per-System Unattended Program, on page 118.

Cisco Network Recording Player Deployment

Install the Network Recording Player

If the version of your Windows Installer Service is outdated, an error message appears. To install the Webex MSI package, upgrade to a newer version of the Windows Installer Service.

Before you begin

Verify that you have administrator privileges on the computer. The Cisco Webex MSI package installs in the default OS Programs folder, which requires administrator privileges.

Procedure

Step 1 Run the installer on the computer.

The installation wizard appears with an introductory message.

Step 2 Click **Next** on each of the dialogue boxes until the installation dialogue box appears.

Step 3 Click **Install**.

Step 4 Click **Finish**.

Install Silently—Command Line

You can sign in to a user's computer and install the Cisco Webex Recording Player by using silent mode.

Procedure

Step 1 Sign in to the computer.

Step 2 Download the MSI package to the computer hard drive.

Step 3 Open the Windows Command prompt.

On Windows 7, you must use run as administrator to open the prompt window.

Step 4 Enter the MSI command to install Webex Recording Player silently.

Example:

Enter **`msiexec/i nbr2player_onprem.msi/qn`**.

Step 5 Restart the computer.

Uninstall Silently—Command Line Interface

You can sign in to a user's computer and remove the Network Recording Player by using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer hard drive.

Step 3 Open the Windows Command prompt.

On Windows 7, you must use run as administrator to open the prompt window.

Step 4 Uninstall all components of the MSI package onpremmc.msi by entering the command **`msiexec/i nbr2player_onprem.msi/qn`**.

Advertise—SMS Per-System Unattended Program

Before you begin

Sign in to Webex Administration, and then configure your Download settings to manually push the Webex desktop applications.

You must be an SMS administrator.

Procedure

Step 1 Create a package from the definition.

See Create a Package from a Definition, on page 115 for more information.

Step 2 Change the program options for "Per-system unattended" before advertisement:

a) Open the SMS administrator console, and go to **Site Database** > **Packages** > **Cisco Webex LLC Cisco Webex Network Recording Player English** > **Programs**.
b) Right click the **Per-system unattended** option, and theb click **Properties** to open the **Per-system unattended Program Properties** dialog box.
c) Click the **Environment** tab.
   - For the **Program can run** option, select **Only when a user is logged on**.
   - For the **Run mode** option, select **Run with administrative rights**. Do not select **Allow users to interact with this program**.
d) Click the **General** tab.
e) Append an additional parameter to the command line option to specify some options for the Webex Meetings application:

   Example:

   For example, the initial command line is: `msiexec /i "nbr2player_onprem.msi" /qn`

Step 3 Advertise the program.

a) Open the SMS administrator console, and go to **Site Database** > **Packages** > **Cisco Webex LLC Cisco Webex Network Recording Player English** > **Programs**.
b) Right-click **Per-system unattended**.
c) Go to **All Tasks** > **Distribute Software**.
d) Click **Next** in the **Distribute Program Wizard**.
e) Select the SMS Server and click **Next**.
f) Select the collection, and then click **Next**.
g) Enter the advertisement name in the **Name** field, and then click **Next**.
h) Specify whether the advertisement should apply to subcollections, and then click **Next**.
i) Specify when the program will be advertised, and then click **Next**.
j) Specify whether to assign the program, and then click **Next**.
k) Click **Finish** on the **Completing the Distribute Program Wizard** page.
l) Navigate to the `\Site Database\System Status\Advertisement Status` directory and check the advertisement status.

   If you enable notification, users see a message indicating that the assigned program will run after the advertisement. The assigned program runs silently.

Uninstall—SMS Per-System Uninstall Program

The SMS administrator can use the following procedure to uninstall the Cisco Webex Network Recording Player.

Procedure

Step 1 Create an SMS Installation package.

See Create a Package from a Definition, on page 115.

Step 2 Advertise the per-system uninstall program to uninstall the Cisco Webex Network Recording Player.

The Cisco Webex Network Recording Player silently uninstalls from the specified machines.

Paths to Mass-Deployed Applications

After you perform an update of your Cisco Webex Meetings Server (CWMS) software, you may need to update the paths to your mass-deployed applications. After an update, the path for the Network Recording Player automatically updates the first time it is used to play a recording.

Applications on both Windows and Mac systems are automatically updated to maintain compatibility with your updated system. In a locked down environment, you must perform updates manually for Windows systems, but not for Mac systems.

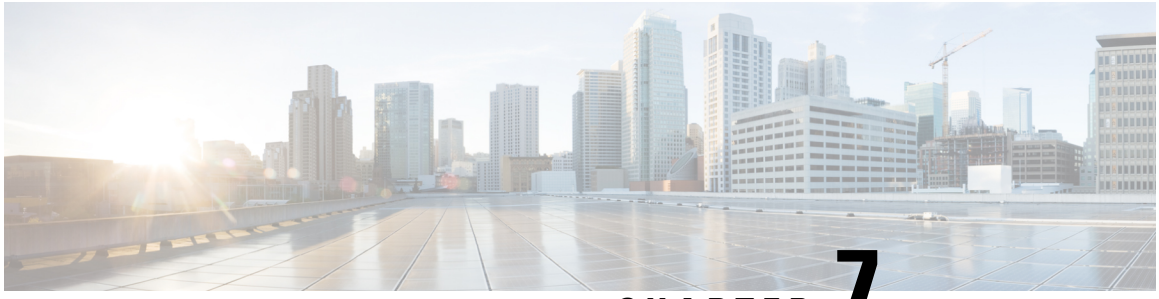
For Mac systems the path is `/Users/(Local User)/Library/Application Support/Webex Folder/`.

For Windows 7, 8.1, and 10 systems, the path is `<SystemDisk>\ProgramData\Webex`.

From Webex Meetings Desktop Application, use the Webex Meetings Desktop Application path.

If you are using MSI installation, always use a unique path. Your system ignores the existing file.

If you are using the download type with Windows 7, your system uses a unique path. Otherwise the system uses its own path, as described above.



CHAPTER 7

SAML SSO Configuration

Overview of Single Sign-On

Federated single sign-on (SSO) standards such as SAML 2.0 provide secure mechanisms for passing credentials and related information between different websites that have their own authorization and authentication systems. SAML 2.0 is an open standard developed by the OASIS Security Services Technical Committee.

The SAML 2.0 protocol has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. SAML 2.0 support has been implemented by all major web-access management vendors. The U.S. Government General Services Administration (GSA) requires all vendors participating in the U.S. E-Authentication Identity Federation program to be SAML 2.0-compliant.

SAML 2.0-compliant websites exchange user credential information using SAML assertions. A SAML assertion is an XML document that contains trusted statements about a subject including, for example, a username and privileges. SAML assertions are digitally signed to ensure their authenticity.

Many large enterprises have deployed federated Identity and Access Management (IAM) and Identity Provider (IdP) systems, such as Ping Identity Ping Federate, CA SiteMinder, Open AM, and Windows ADFS 2.0 on their corporate intranets. These IAM and IdP systems handle the user authentication and SSO requirements for employees and partners. IAM and IdP systems use the SAML protocols to interoperate with partner websites outside their firewalls. Users can utilize their IAM and IdP systems to automatically authenticate their users to Cisco Webex Meeting services. This increases efficiency because users do not have to remember their usernames and passwords to start or join meetings on their Cisco Webex sites.

Note Webex Meetings Server supports SAML 2.0 IdPs only. It does not support IdPs based on the older SAML 1.1 and WS-Federate standards. This restriction stands in contrast to the cloud-based Cisco Webex Meeting services which continue to support SAML 1.1 and WS-Federate. The following is a list of SAML 2.0 IdPs that have been validated to work with Cisco Webex Meetings Server:

- Microsoft ADFS 2.0 (a free add-on to Microsoft Windows Server 2008/Windows Server 2008 R2 or AD FS server role in Windows Server 2012)
- Microsoft ADFS 3.0 (AD FS server role in Windows Server 2012)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Because SAML 2.0 is an open standard, other SAML 2.0 IdPs might also operate with Cisco Webex Meetings Server. However, other SAML 2.0 IdPs have not been tested by Cisco. It is therefore the administrator's responsibility to make any such integration operational.

Benefits of Single Sign-On

Single sign-on (SSO) can benefit you in the following ways:

- Simplified user authentication—Out of the box, Cisco Webex Meetings Server requires users to sign in using email addresses and passwords that are specific to the Meetings Server system. While this approach works well for some small and mid-sized organizations, larger organizations prefer using corporate credentials—that is, Active Directory—for enhanced security. You can accomplish this by using SAML 2.0 SSO.

  Note Secure authentication—The SSO password is never sent to or stored in Cisco Webex Meetings Server after the user authenticates.

- Simplified user management—Large organizations with changing workforces due to normal attrition prefer to automate the process of user management when integrating with Webex Meetings Server. This means automating the following:
  - User account creation when employees join the organization
  - User account updates when employees take on different roles within the organization
  - User account deactivation when employees leave the organization

  To automate these events, configure **Auto Account Creation** and **Auto Account Update** in the SSO section of Webex Site Administration. We recommend that you turn on these features if they are also supported by your SAML IdPs. User accounts are automatically created and updated "on demand" when users authenticate, eliminating the need to create user accounts manually. Similarly, users can no longer sign into their accounts after they leave the organization, because the SAML 2.0 IdP blocks those users

from signing in after they are removed from the database, which is usually a proxy for the underlying corporate directory.

Overview of Setting Up SAML 2.0 Single Sign-On

Important Unless you or someone in your organization has experience with SAML 2.0 single sign-on (SSO), we recommend that you engage the services of a qualified Cisco AUC partner or Cisco Advanced Services. We make this recommendation because SAML SSO configuration can be complicated.

Caution If the SAML response has a carriage return in any of the fields, then the update, account creation, and authentication fails. Although the SAML provider calculates the digital signature with the carriage return, Cisco Webex Meetings Server removes the carriage return causing the digital signature to be invalid.

Review these general steps for setting up SAML 2.0 SSO:

1. Ensure that your SAML 2.0 SSO infrastructure is in place and is integrated with your corporate directory. This consists of setting up the SAML 2.0 IdP software and the SSO authentication website. The authentication website is a portal where users enter their corporate credentials.
2. Ensure that users can access the SSO authentication website. This step is important because, as part of the sign-in process, Cisco Webex Meetings Server redirects users to this authentication website.

   Note If your Cisco Webex Meetings Server system is enabled for public access, allowing users to sign in and join meetings from the Internet, the SSO authentication website must be accessible from the Internet. This usually involves deploying the SAML 2.0 IdP in your DMZ. Otherwise, users see "404 site not found" errors when signing in to Cisco Webex Meetings Server from the Internet.

3. Connect Webex Meetings Server to the SAML 2.0 IdP by using both of these methods:
   - Go to **Settings** > **Security** > **Federated SSO** in Webex Site Administration, and set the IdP parameters. See the Configuring Federated Single Sign-On (SSO) Settings section of the *Administration Guide for Cisco Webex Meetings Server*.
   - Follow the instructions in your SAML 2.0 IdP documentation. These instructions vary from vendor to vendor. We recommend that you contact a qualified Cisco AUC partner or Cisco Advanced Services to help you implement the solution.

   Note Do not use the instructions found on the Cisco Developer Network to set up a SAML 2.0 IdP. Those instructions are intended for cloud-based Cisco Webex meeting services and do not work with Cisco Webex Meetings Server.

SAML SSO for End-User and Administration Sign In

SAML SSO is typically configured only for sign-in purposes on the End-User site and not the Administration site. On SAML 2.0 SSO-integrated Cisco Webex Meetings Server sites the behavior mirrors SaaS Webex behavior when it comes to user authentication. A Cisco Webex Meetings Server administrator (and an SaaS Webex administrator) can sign in to an end-user account using SAML SSO but must sign in to an administrator account on the same system using a separate password. This ensures that in the event of catastrophic failures on the SAML SSO iDP, an administrator will still be able to access the Administration site. Without this failsafe, you might encounter a situation in which the Administration site becomes inaccessible not because of a product failure but because of a problem with the SAML SSO IdP software. The SAML SSO IdP software is on a server that is external to Cisco Webex Meetings Server (or SaaS Webex) and therefore outside of our control.

SAML 2.0 Single Sign-On Differences Between Cloud-Based Webex Meeting Services and Webex Meetings Server

While the cloud-based Cisco Webex meeting services employ unique user IDs when creating users accounts, Cisco Webex Meetings Server uses email addresses as the basis for creating user accounts. When deploying SAML 2.0 single sign-on (SSO) note that the cloud-based Cisco Webex Meeting services permit removal of the email domain, such as "@cisco.com," from the UPN (User Principal Name) when auto account creation is turned on. This results in the creation of a user account that resembles a user ID. Because Cisco Webex Meetings Server requires a complete email address to create user accounts, you cannot remove the email domain from the UPN.

The Identity Provider (IdP) server can use any unique Active Directory (AD) field as the NameID for an SSO configuration. If you use SSO and you change the email address for an active user, change the mapping for the NameID field on the IdP server.

You can deploy Cisco Webex Meetings Server without SAML 2.0 SSO and after the deployment, turn on SSO. Doing so has the following important effects on the user authentication, auto account creation, and auto account update features:

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is not turned on. User accounts were created in the CWMS system.	Users sign in by using their email addresses and unique passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Turn on SSO. Users with existing accounts sign in to their Webex site, Webex Meetings Desktop Application, or to the Cisco Webex Meetings applications on their mobile devices.	Users are redirected to the SAML 2.0 IdP authentication website and sign in by using their corporate credentials, instead of unique passwords. If they are not valid users, they are informed by the SAML 2.0 IdP that they cannot use Cisco Webex or that they are invalid users.	N/A	N/A	N/A	N/A
SSO is turned on. Users do not have existing accounts in the system.	Same as the previous scenario.	User accounts for Cisco Webex Meetings are created "on-demand" after users sign in. Prerequisite: The SAML Assertion contains a valid email address in the NameID field.	Users that do not have accounts in the system can sign in, cannot access but Cisco Webex. To remedy this situation: • Leave AAC on. • Manually create user accounts.	N/A	N/A
SSO is turned on. Users previously signed in are using SSO and are signing in again.	Same as the "Turn on SSO" scenario.	N/A	N/A	Existing user accounts are automatically updated with any changes to the user credentials as long as the NameID remains unchanged.	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
You turn off SSO. (This is an uncommon scenario.) Users previously signed in by using SSO and are now signing in again.	If users enter their corporate credentials, they cannot sign in because Cisco Webex expects their email addresses and unique passwords. In this situation, educate the users about resetting the unique passwords in their Cisco Webex accounts and allow them enough time to act before you turn off SSO. After resetting their passwords, users can sign in by using their email addresses and unique passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Special case: A user is also a system administrator. Scenario A: The user signs in to the Webex Site. Scenario B: The user signs in to Webex Site Administration.	Scenario A: Same results as the previous scenario. Scenario B: When the user signs in to Webex Site Administration, he or she is always prompted to enter their email address and unique password; SSO has no effect when a user signs into Webex Site Administration. This is a security measure built into the product. It ensures that systems administrators can always sign in to Webex Site Administration. If Webex Site Administration were to support SSO, malfunctions in the SAML 2.0 IdP or a loss of network connectivity between Cisco Webex Meetings Server and the SAML 2.0 IdP could prevent administrators from signing in.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.

SAML Assertion Attributes

The following tables list the SAML assertion attributes supported by Cisco Webex Meetings Server. Make sure to configure the `lastname`, `firstname`, `email`, and `updatetimestamp` attributes. Automatic update does not work unless the `updatetimestamp` attribute is configured.

Supported SAML Assertion Attributes

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
lastname		Yes		
firstname		Yes		
email		Yes	Valid email format	Always mandatory, even if Auto Account Creation and update are disabled in the SSO configuration.
updatetimestamp	The user information update time	No	Support format **long format:** sample: System.currentTimeMillis() **LDIF format:** yyyyMMddHHmmss yyyy-MM-dd HH:mm:ss sample: 20090115213256 **UTC format** ("2009-10-09T06:00:32Z")	If the updateTimeStamp is missing, you cannot perform an auto update user, normally mapped to the whenChanged item if the IdP is linked to AD.
optionalparams		No		See Optional Parameters, on page 135.
OPhoneCountry		No		Office phone country code
OPhoneArea		No		Office phone area

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
OPhoneLocal		No	Enter numerical characters only. For example, 5551212. Do not enter non-numerical characters such as dashes or parentheses.	Office phone local
OPhoneExt		No		Office phone extension
FPhoneCountry		No		Alternate phone country code
FPhoneArea		No		Alternate phone area
FPhoneLocal		No		Alternate phone local
FPhoneExt		No		Alternate phone extension
PPhoneCountry		No		Alternate phone 2 country code
PPhoneArea		No		Alternate phone 2 area
PPhoneLocal		No		Alternate phone 2 local
PPhoneExt		No		Alternate phone 2 extension
MPhoneCountry		No		Mobile phone country code
MPhoneArea		No		Mobile phone area
MPhoneLocal		No		Mobile phone local
MPhoneExt		No		Mobile phone extension
TimeZone		No		See Time Zone Values, on page 135.
Address1		No		Address1
Address2		No		Address2

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
City		No		City
State		No		State
ZIP code		No		ZIP code
Country		No		See Country Code Values, on page 138.
Region		No		See Region Values, on page 146.
Language		No		See Language Values, on page 147.
TC1	String	No	Tracking Code Group 1 entered by user on the Administration site	Index 1
TC2	String	No	Tracking Code Group 2 entered by user on the Administration site	Index 2
TC3	String	No	Tracking Code Group 3 entered by user on the Administration site	Index 3
TC4	String	No	Tracking Code Group 4 entered by user on the Administration site	Index 4
TC5	String	No	Tracking Code Group 5 entered by user on the Administration site	Index 5
TC6	String	No	Tracking Code Group 6 entered by user on the Administration site	Index 6
TC7	String	No	Tracking Code Group 7 entered by user on the Administration site	Index 7

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
TC8	String	No	Tracking Code Group 8 entered by user on the Administration site	Index 8
TC9	String	No	Tracking Code Group 9 entered by user on the Administration site	Index 9
TC10	String	No	Tracking Code Group 10 entered by user on the Administration site	Index 10

Optional Parameters

You can set the **optionalparams** setting as follows:

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">City=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=OFF</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">Toronto</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">OFF</saml:AttributeValue>

Time Zone Values

Time Zone	Value
Marshall Islands (Dateline Time, GMT-12:00)	0
Samoa (Samoa Time, GMT-11:00)	1
Honolulu (Hawaii Time, GMT-10:00)	2
Anchorage (Alaska Daylight Time, GMT-08:00)	3
San Francisco (Pacific Daylight Time, GMT-07:00)	4
Arizona (Mountain Time, GMT-07:00)	5

Time Zone	Value
Denver (Mountain Daylight Time, GMT-06:00)	6
Chicago (Central Daylight Time, GMT-05:00)	7
Mexico City (Mexico Daylight Time, GMT-05:00)	8
Saskatchewan (Central Time, GMT-06:00)	9
Bogota (S. America Pacific Time, GMT-05:00)	10
New York (Eastern Daylight Time, GMT-04:00)	11
Indiana (Eastern Daylight Time, GMT-04:00)	12
Halifax (Atlantic Daylight Time, GMT-03:00)	13
La Paz (S. America Western Time, GMT-04:00)	14
Newfoundland (Newfoundland Daylight Time, GMT-02:30)	15
Brasilia (S. America Eastern Standard Time, GMT-03:00)	16
Buenos Aires (S. America Eastern Time, GMT-03:00)	17
Mid-Atlantic (Mid-Atlantic Time, GMT-02:00)	18
Azores (Azores Summer Time, GMT)	19
Reykjavik (Greenwich Time, GMT)	20
London (GMT Summer Time, GMT+01:00)	21
Amsterdam (Europe Summer Time, GMT+02:00)	22
Paris (Europe Summer Time, GMT+02:00)	23
Berlin (Europe Summer Time, GMT+02:00)	25
Athens (Greece Summer Time, GMT+03:00)	26
Cairo (Egypt Time, GMT+02:00)	28
Pretoria (South Africa Time, GMT+02:00)	29
Helsinki (Northern Europe Summer Time, GMT+03:00)	30
Tel Aviv (Israel Daylight Time, GMT+03:00)	31
Riyadh (Saudi Arabia Time, GMT+03:00)	32
Moscow (Russian Time, GMT+04:00)	33

Time Zone	Value
Nairobi (Nairobi Time, GMT+03:00)	34
Tehran (Iran Daylight Time, GMT+04:30)	35
Abu Dhabi, Muscat (Arabian Time, GMT+04:00)	36
Baku (Baku Daylight Time, GMT+05:00)	37
Kabul (Afghanistan Time, GMT+04:30)	38
Ekaterinburg (West Asia Time, GMT+06:00)	39
Islamabad (West Asia Time, GMT+05:00)	40
Mumbai (India Time, GMT+05:30)	41
Colombo (Colombo Time, GMT+05:30)	42
Almaty (Central Asia Time, GMT+06:00)	43
Bangkok (Bangkok Time, GMT+07:00)	44
Beijing (China Time, GMT+08:00)	45
Perth (Australia Western Time, GMT+08:00)	46
Singapore (Singapore Time, GMT+08:00)	47
Taipei (Taipei Time, GMT+08:00)	48
Tokyo (Japan Time, GMT+09:00)	49
Seoul (Korea Time, GMT+09:00)	50
Yakutsk (Yakutsk Time, GMT+10:00)	51
Adelaide (Australia Central Standard Time, GMT+09:30)	52
Darwin (Australia Central Time, GMT+09:30)	53
Brisbane (Australia Eastern Time, GMT+10:00)	54
Sydney (Australia Eastern Standard Time, GMT+10:00)	55
Guam (West Pacific Time, GMT+10:00)	56
Hobart (Tasmania Standard Time, GMT+10:00)	57
Vladivostok (Vladivostok Time, GMT+11:00)	58
Solomon Is (Central Pacific Time, GMT+11:00)	59

Time Zone	Value
Wellington (New Zealand Standard Time, GMT+12:00)	60
Fiji (Fiji Time, GMT+12:00)	61
Stockholm (Sweden Summer Time, GMT+02:00)	130
Tijuana (Mexico Pacific Daylight Time, GMT-07:00)	131
Chihuahua (Mexico Mountain Daylight Time, GMT-06:00)	132
Caracas (S. America Western Time, GMT-04:30)	133
Kuala Lumpur (Malaysia Time, GMT+08:00)	134
Recife (S. America Eastern Time, GMT-03:00)	135
Casablanca (Morocco Daylight Time, GMT+01:00)	136
Tegucigalpa (Honduras Time, GMT-06:00)	137
Nuuk (Greenland Daylight Time, GMT-02:00)	138
Amman (Jordan Daylight Time, GMT+03:00)	139
Istanbul (Eastern Europe Summer Time, GMT+03:00)	140
Kathmandu (Nepal Time, GMT+05:45)	141
Rome (Europe Summer Time, GMT+02:00)	142
West Africa (West Africa Time, GMT+01:00)	143
Madrid (Europe Summer Time, GMT+02:00)	144

Country Code Values

Country	Code
Afghanistan	93
Albania	355
Algeria	213
American Samoa	1684
Andorra	376
Angola	244
Anguilla	1264

Country	Code
Antarctica	672_1
Antigua (including Barbuda)	1268
Argentina	54
Armenia	374
Aruba	297
Ascension Islands	247
Australia	61
Austria	43
Azerbaijan	994
Bahamas	1242
Bahrain	973
Bangladesh	880
Barbados	1246
Belarus	375
Belgium	32
Belize	501
Benin	229
Bermuda	1441
Bhutan	975
Bolivia	591
Bosnia_Herzegovina	387
Botswana	267
Brazil	55
British Virgin Islands	1284
Brunei	673
Bulgaria	359
Burkina Faso	226
Burundi	257

Country	Code
Cambodia	855
Cameroon	237
Canada	1_1
Cape Verde Island	238
Cayman Islands	1_9
Central African Republic	236
Chad Republic	235
Chile	56
China	86
Colombia	57
Comoros	269_1
Cook Islands	682
Costa Rica	506
Croatia	385
Cuba	53
Cyprus	357
Czech Republic	420
Denmark	45
Diego Garcia	246
Djibouti	253
Dominica	1767
Dominican Republic	1809
Ecuador	593
Egypt outside Cairo	20
El Salvador	503
Equatorial Guinea	240
Eritrea	291
Estonia	372

Country	Code
Ethiopia	251
Faeroe Islands	298
Falkland Islands	500
Fiji Islands	679
Finland	358
France	33
French Depts. (Indian Ocean)	262
French Guiana	594
French Polynesia	689
Gabon Republic	241
Gambia	220
Georgia	995
Germany	49
Ghana	233
Gibraltar	350
Greece	30
Greenland	299
Grenada	1473
Guadeloupe	590
Guantanamo (U.S. Naval Base)	53_1
Guatemala	502
Guinea	224
Guinea-Bisau	245
Guyana	592
Haiti	509
Honduras	504
Hong Kong	852
Hungary	36

Country	Code
Iceland	354
India	91
Indonesia	62
Iran	98
Iraq	964
Ireland	353
Israel	972
Italy	39_1
Ivory Coast	225
Jamaica	1876
Japan	81
Jordan	962
Kazakhstan	7_1
Kenya	254
Kiribati	686
Korea (North)	850
Korea (South)	82
Kuwait	965
Kyrgyzstan	996
Laos	856
Latvia	371
Lebanon	961
Lesotho	266
Liberia	231
Libya	218
Liechtenstein	423
Lithuania	370
Luxembourg	352

Country	Code
Macao	853
Macedonia	389
Madagascar	261
Malawi	265
Malaysia	60
Maldives	960
Mali	223
Malta	356
Marshall Islands	692
Mauritania	222
Mauritius	230
Mayotte Island	269
Mexico	52
Micronesia	691
Moldova	373
Monaco	377
Mongolia	976
Montserrat	1664
Morocco	212
Mozambique	258
Myanmar	95
Namibia	264
Nauru	674
Nepal	977
Netherlands	31
Netherlands Antilles	599_2
New Caledonia	687
New Zealand	64

Country	Code
Nicaragua	505
Niger	227
Niue	683
Norfolk Island	672
Northern Mariana Islands	1670
Norway	47
Oman	968
Pakistan	92
Palau	680
Panama	507
Papua New Guinea	675
Paraguay	595
Peru	51
Philippines	63
Poland	48
Portugal	351
Puerto Rico	1787
Qatar	974
Romania	40
Russia	7
Rwanda	250
San Marino	378
Sao Tome	239
Saudi Arabia	966
Senegal Republic	221
Serbia	381
Seychelles Islands	248
Sierra Leone	232

Country	Code
Singapore	65
Slovakia	421
Slovenia	386
Solomon Islands	677
Somalia	252
South Africa	27
Spain	34
Sri Lanka	94
St. Helena	290
St. Kitts and Nevis	1869
St. Lucia	1758
St. Pierre and Miguelon	508
St. Vincent	1784
Sudan	249
Suriname	597
Swaziland	268
Sweden	46
Switzerland	41
Syria	963
Taiwan	886
Tajikistan	992
Tanzania	255
Thailand	66
Togo	228
Tonga Islands	676
Trinidad and Tobago	1868
Tunisia	216
Turkey	90

Country	Code
Turkmenistan	993
Turks and Caicos	1649
Tuvalu	688
Uganda	256
Ukraine	380
United Arab Emirates	971
United Kingdom	41
United States of America	1
Uruguay	598
Uzbekistan	998
Vanuatu	678
Vatican City	39
Venezuela	58
Vietnam	84
Wallis and Futuna Islands	681
Western Samoa	685
Yemen	967
Zambia	260
Zimbabwe	263

Region Values

Region	Value
United States	2
Australia	3
Canada	4
French Canada	5
China	6
France	7

Region	Value
Germany	8
Hong Kong	9
Italy	10
Japan	11
Korea	12
New Zealand	13
Spain	14
Switzerland	15
Taiwan	16
United Kingdom	17
Mexico	18
Argentina	19
Chile	20
Colombia	21
Venezuela	22
Brazil	23
Portugal	24
Belgium	25
Netherlands	26
Russia	28
India	29

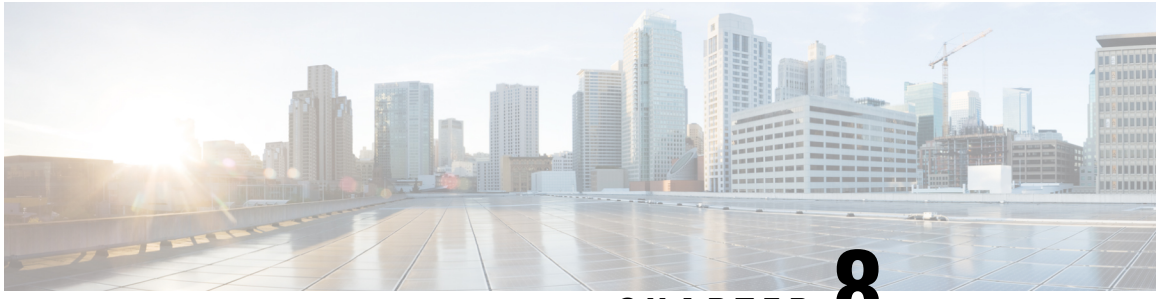
Language Values

Language	Value
Castellon Spanish	11
Dutch	14
English	1
French	7

Language	Value
German	9
Italian	10
Japanese	5
Korean	6
Latin American Spanish	12
Portuguese	15
Russian	16
Simplified Chinese	3
Traditional Chinese	4

Language Codes

Language	Country Code
Castellon Spanish	34
Chinese	852, 853, 886
Dutch	31, 32
French	33, 242, 243
German	41, 43, 49
Italian	39
Japanese	81
Korean	82
Latin American Spanish	52, 54, 56, 57, 58
Mandarin	86
Portuguese	55, 351
Russian	7
U.K. English	44, 61, 64, 91
U.S. English	1



CHAPTER 8

Storage Requirements

Storage Requirements for Meeting Recordings

You can configure a storage server of any capacity. The number of Cisco Webex recordings saved is dependent upon the amount of storage space.

When a user marks a recording for deletion, immediately it is no longer available from the user interface. It is maintained in storage for three to six months. Therefore, recordings can be copied, backed up, or used for up to six months despite being marked for deletion by the user. (If a user inadvertently deletes a recording from the Cisco Webex Meeting Recordings page, but the recording is saved on the Network File System (NFS) storage server, you must contact the Cisco Technical Assistance Center (TAC) to recover the recording.)

If the recordings on your system do not consume over 75 percent of the allocated space in a three-month period, recordings are deleted after six months. If the recordings consume over 75 percent of the allocated space at any point in a three-month period, the system automatically deletes the first 10 files that have been set for deletion by a user.

For example, a user identifies two files for deletion today, and then five files tomorrow, and then nine files the day after tomorrow. If the storage usage exceeds the 75 percent threshold, the system deletes the first two files after three months, the next five files the next day, and then it deletes the first three of the nine files marked for deletion the day after that.

If your organization requires you to store more than six months of meeting recording, periodically archive the recordings to other media.

The following table provides an estimate of the amount of storage space needed for one hour of recording. Use these values to help you estimate the amount of storage space required by your system for six months of meeting recordings.

Meeting Content	Approximate Storage Space Needed for a One Hour Meeting Recording
Application sharing	36 MB
Voice	30 MB
180p video	104 MB
360p video	337 MB

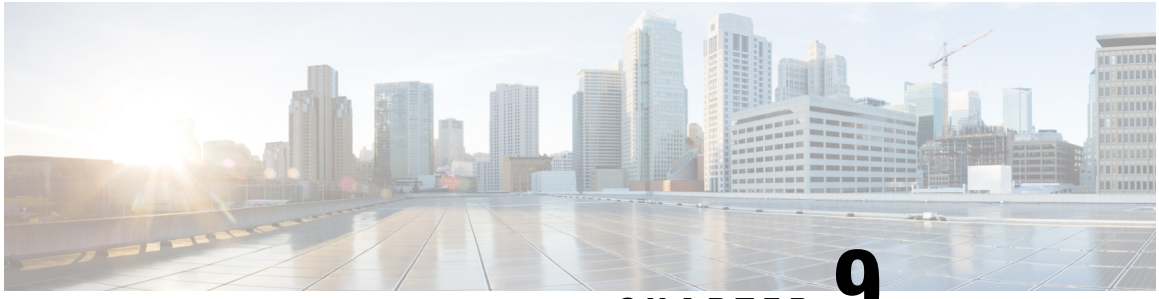
Webcam videos are stored at the original resolution for the meeting recording. However, during playback the video resolution is restricted to 180p.

Storage Requirements for System Backup Files

Considerations when determining the storage space required for backups:

- The number of users
- The average number of meetings held each day
- The size of your database, which will increase over time
- With HA deployments, there can be lags in transaction journal transport due to network latency or a high system load during the replication of data. This can increase the size of a backup file.

The Dashboard shows the approximate storage requirements for a system backup. Allow enough space on the storage server for at least three times the indicated backup size.



CHAPTER 9

SNMP MIBs and Traps Support

This section describes the MIBs available on your system. When you access your MIB data you will expose additional MIBs not listed in this section. The additional MIBs you expose through the process are primarily used internally for things like inter-virtual machine management. Cisco does not support customer-side SNMP monitoring that uses these MIBs, nor is there any guarantee that these MIBs will be used in future releases of Cisco Webex Meetings Server.

Supported SNMP MIBs

The SNMP MIB ftp://ftp.cisco.com/pub/mibs/v2/CISCO-WBX-MEETING-MIB.my is supported by Cisco Webex Meetings Server. Not all MIB variables are applicable to Cisco Webex Meetings Server or to all Cisco Webex Meetings Server deployment types. For example, data center related MIBs do not apply to Cisco Webex Meetings Server systems.

CWMS System Information MIBS

Object[20]	OID	Description
cwCommSystemVersion Type: String	.1.3.6.1.4.1.9.9.809.1.1.1	Cisco Webex system version.
cwCommSystemObjectID Type: Autonomous	.1.3.6.1.4.1.9.9.809.1.1.2	The sysObjectID as defined in SNMPv2-MIB.

[20] All objects in this table are read only (RO).

CPU-Related MIBs

Object	Read/Write Privilege	OID	Description
cwCommCPUTotalUsage Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.1	Percentage of CPU usage by a host component. The total CPU usage contains CPU user usage, CPU system usage, and CPU nice usage. The CPU user time: CPU time spent in user space. The CPU system time: CPU time spent in kernel space. The CPU nice time: CPU time spent on low priority processes.
cwCommCPUUsageWindow Type: Gauge32	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	Duration (in seconds) before a notification (trap) is sent indicating a CPU usage has crossed a normal/minor/major threshold and remains at the new threshold.
cwCommCPUTotalNumber Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	Number of CPUs on the system.
cwCommCPUUsageTable Type: n/a	Not-accessible	.1.3.6.1.4.1.9.9.809.1.2.1.4	A list of CPU usage registers on the device.
cwCommCPUIndex Type: Unsigned	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.1	Unique CPU identifier. Each CPU has its own usage and breakdown values.
cwCommCPUName Type: String	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.2	CPU name. For example, Intel® Xeon™ CPU 3.00GHz.

Object	Read/Write Privilege	OID	Description
cwCommCPUUsage Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	Percentage of total CPU resources used. Usually GHz is used for measuring CPU power. Since GHz is too large for measuring some CPU usage categories, KHz is used as the measuring unit. The system speed multiplies by the fraction of each CPU section (for example, idle, nice, user) to get the CPU KHz for each category. KHz is used as the unit of measure for all the CPU categories in this table.
cwCommCPUUsageUser Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	CPU power executed in user mode.
cwCommCPUUsageNice Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.5	CPU power executed on low priority processes. Nice is a program found on UNIX and Linux. It directly maps to a kernel call of the same name. Nice is used to invoke a utility or shell script with a particular priority, thus giving a process more or less CPU time than other processes.
cwCommCPUUsageSystem Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.6	CPU power executed in kernel mode.
cwCommCPUUsageIdle Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	CPU power in idle status.
cwCommCPUUsageIOWait Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	CPU power used when waiting for disk I/O to complete.
cwCommCPUUsageIRQ Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	CPU power used when handling an interrupt request.

Object	Read/Write Privilege	OID	Description
cwCommCPUUsageSoftIRQ Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	CPU power used when handling a software interrupt request.
cwCommCPUUsageSteal Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	CPU power used on other tasks when running in a virtualized environment.
cwCommCPUUsageCapacitySubTotal Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	Current total CPU power.
cwCommCPUMonitoringStatus Type: String	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	Monitoring status of CPU resources: • closed (0)—Resource not available. • open(1)—Resource is available.
cwCommCPUCapacityTotal Type: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.6	Overall CPU capacity.

CWMS Memory Information

Object[21]	OID	Description
cwCommMEMUsage Type: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.1	Physical memory usage of the virtual machine.
cwCommMEMMonitoringStatus Type: String	.1.3.6.1.4.1.9.9.809.1.2.2.2	Monitoring status of the memory resource: closed (0)—Resource not available. open(1)—Resource is available.
cwCommMEMTotal Type: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.3	Total physical memory size (in KB) of the host.
cwCommMEMSwapUsage Type: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.3.1	Physical memory usage (in percentage) and swap memory usage of the host.

Object[21]	OID	Description
cwCommMEMSwapMonitoringStatus Type: String	.1.3.6.1.4.1.9.9.809.1.2.3.2	This object provides the monitoring status of memory and swap memory. closed (0)—The memory and swap memory status is available. open(1)—The memory and swap memory status is not available.

[21] All objects in this table are read only (RO).

Disk Usage

Object[22]	OID	Description
cwCommDiskUsageCount	.1.3.6.1.4.1.9.9.809.1.2.5.1	Count of how many disks (for example, local disk, remote disk, meeting recording disk) available in the system.
cwCommDiskUsageIndex	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.1	Index of entries in the table that contain management information generic to the disk usage.
cwCommDiskPartitionName	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	Disk partition name. For example, the partition /opt or /dev.
cwCommDiskUsage	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.3	Current disk usage (in percentage) on the host.
cwCommDiskTotal	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.4	Total disk space size (in MB) of this host.
cwCommDiskMonitoringStatus	1.3.6.1.4.1.9.9.809.1.2.5.3	Monitoring status of disk resources. close (0)—The disk usage status is not available. open (1)—The disk usage status is available.

[22] All objects in this table are read only (RO).

Supported SNMP Traps

Cisco Webex Meetings Server supports SNMP traps.

Notification Events

cwCommSystemResourceUsageNormalEvent (.1.3.6.1.4.1.9.9.809.0.1)

Notification when a system resource usage changes from the *normal* status. System can send out this notification in the event:

- The `cwCommCPUUsage` value of one CPU changes to be less than the value of pre-defined CPU Minor Threshold.
- The value of `cwCommMEMUsage` changes to be less than the value of a pre-defined MEM Minor Threshold.
- The value of `cwCommMEMSwapUsage` changes to be less than in the pre-defined MEM SwapMinor Threshold.
- The value of `cwCommFileUsage` changes to be less than the pre-defined File Minor Threshold.
- The value of `cwCommDiskUsage` on one disk changes to be less than the pre-defined Disk Minor Threshold.

cwCommSystemResourceUsageMinorEvent (.1.3.6.1.4.1.9.9.809.0.2)

Notification when a system resource usage changes from the *minor* status. The minor notification means the system has some issues and the system administrator must resolve them. System can send out this notification in the event:

- The `cwCommCPUUsage` value of one CPU changes to be larger than or equal to the value of pre-defined CPU Minor Threshold and be less than cwCommCPUMajorThreshold.
- The `cwCommMEMUsage` value changes to be larger than or equal to the value of the pre-defined MEM Minor Threshold and be less than the pre-defined MEM Major Threshold.
- The `cwCommMEMSwapUsage` value changes to be larger than or equal to the value of pre-defined MEM Swap Minor Threshold and be less than the pre-defined MEM Swap Major Threshold.
- The `cwCommFileUsage` value changes to be larger than or equal to the value of pre-defined File Minor Threshold and be less than the pre-defined File Major Threshold.
- The `cwCommDiskUsage` value of one disk changes to be larger than or equal to the value of pre-defined Disk Minor Threshold and be less than the pre-defined Disk Major Threshold.

cwCommSystemResourceUsageMajorEvent (.1.3.6.1.4.1.9.9.809.0.3)

This notification indicates system resource usage changes to the *major* status. The major notification means the system is in critical state and it required the system administrator to take action immediately. The system can send out this notification in the event:

- The `cwCommCPUUsage` value of one CPU changes to be larger than or equal to the value of pre-defined CPU Major Threshold.
- The `cwCommMEMUsage` value changes to be larger than or equal to the value of pre-defined MEM Major Threshold.
- The `cwCommMEMSwapUsage` value changes to be larger than or equal to the value of pre-defined MEM Swap Major Threshold.
- The `cwCommFileUsage` value changes to be larger than or equal to the value of pre-defined File Major Threshold.

- The `cwCommDiskUsage` value of one disk changes to be larger than or equal to the value of pre-defined Disk Major Threshold.

Trap Data

Supported trap data. We recommend that you set your MIB filter to receive only these traps.

Trap Data	Description
Name: cwCommNotificationHostAddressType **OID:** .1.3.6.1.4.1.9.9.809.1.2.4.1 **Textual Convention:** InetAddressType	Type of the network address made availab cwCommNotificationHostAddress.
Name: cwCommNotificationHostAddress **OID:** .1.3.6.1.4.1.9.9.809.1.2.4.2 **Textual Convention:** InetAddress	The host IP address sent with the notifica
Name: cwCommNotificationResName **OID:** .1.3.6.1.4.1.9.9.809.1.2.4.3 **Textual Convention:** CiscoWebexCommSysRes	The system resource name sent with the n named system resource has exceeded pre- 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. open file descriptor (no MIB data) 4. cwCommSocketUsage 5. one of the cwCommDiskTotal
Name: cwCommNotificationResValue **OID:** .1.3.6.1.4.1.9.9.809.1.2.4.4 **Textual Convention:** Unsigned32	System resource percentage usage value v
Name: cwCommNotificationSeqNum **OID:** .1.3.6.1.4.1.9.9.809.1.2.4.5 **Textual Convention:** Counter32	Sequence number that tracks the order of

CHAPTER 10

User System Requirements

The system requirements for end users to host and access meetings.

Common PC System Requirements

The requirements for the administrator PC and the Webex Meetings Desktop Application user PC are the same.

Client and Browser Requirements

- JavaScript and cookies enabled
- Java 6, Java 7, or Java 8 (for web browsers that support Java) enabled
- Cisco Webex plug-ins enabled for Chrome and Firefox
- Plug-ins enabled in Safari
- Active X enabled and unblocked for Microsoft Internet Explorer (recommended)
- **Enable Protected Mode** disabled for all zones, for Microsoft Internet Explorer 64-bit

Note Because of Google and Mozilla policy changes, some users must manually enable the Webex plug-in when using these browsers to join a Webex meeting or to play a Webex recording. For more information and instructions, visit https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm.

If a client is using a browser other than the specified versions of Chrome or Firefox and have Java enabled, the Cisco Webex Meetings application automatically downloads onto the client system the first time that client starts or joins a meeting. We recommend that you direct all clients to install the latest update for your Java version.

TLS Requirements

Configure **Internet settings** on all user computers to use TLS encryption. For example, on a Windows PC select **Control Panel** > **Internet Options** > **Advanced** > **Security** > **Use TLS 1.1** and **Use TLS 1.2**. We recommend selecting both options for maximum compatibility. (**Use TLS 1.0** is not supported in versions 2.7 or higher.)

If your users host meetings for guests, such as people who do not work for your company, tell those meeting guests to manually update their operating systems and browsers that they must match the TLS setting before they join your meetings. If they do not modify their systems, they will experience compatibility issues. We recommend that you include these instructions in your meeting invitations. You can do this by editing the appropriate meeting invitations available on your Administration site at **Settings** > **Email** > **Templates**.

System Requirements—Windows

Supported Windows Operating Systems

- Windows 7 (32-bit/64-bit)
- Windows 8 (32-bit/64-bit)
- Windows 8.1 (32-bit/64-bit)
- Windows 10 (32-bit/64-bit)
- Microsoft Windows 10 Redstone 1—Also known as Windows 10 Anniversary Update (Version 1607)

Windows Hardware Requirements

Intel Core2 Duo or AMD CPU 2.XX GHz or higher processor.

A minimum of 2 GB of RAM is recommended.

Supported Windows Browsers

- Microsoft Edge (Windows 10 only): 42 and 44
- Microsoft Internet Explorer (IE): 11
- Mozilla Firefox: 59–70
- Google Chrome: 65–78

Microsoft Outlook Integration

- Microsoft Outlook 2013
- Microsoft Outlook 2016
- Microsoft Outlook Web App (Microsoft Office 365)

Cisco Jabber for Windows Integration

This release supports Jabber for Windows 12.1.0, 12.1.1, 12.5.0, and 12.6.0.

System Requirements—Mac

Supported Mac Operating Systems

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.1
- macOS Mojave 10.14.2
- macOS Mojave 10.14.3
- macOS Mojave 10.14.4
- macOS 10.15.1 Catalina
- macOS 11.x Big Sur

Mac Hardware Requirements

2.0 GHz or higher CPU.

A minimum of 512 MB of RAM is recommended.

Supported Mac Browsers

- Apple Safari: 12.0.1, 12.1, and 13
- Google Chrome: 65–78
- Mozilla Firefox: 59–70

Cisco Jabber for Mac Integration

The following Cisco Jabber for Mac integrations are supported for Cisco Webex Meetings Server sites that are configured for SAML 2.0 single sign-on (SSO) or LDAP/Active Directory: Cisco Jabber for Mac Release 12.1.0, 12.1.1, 12.5.0, and 12.6.0.

Operating Systems Requirements for Mobile Devices

Users can install the Cisco Webex application for iOS or Android on their mobile devices. If you enable the Webex mobile feature, users can use the application to attend or start meetings. A user can also access Cisco Webex on a mobile device by using a browser, but it might not provide an optimal user experience.

Cisco Webex Meeting Server version 2.0 and higher supports:

- Apple iPhones and iPads using iOS 6.0 and later.
- Android mobile devices using Android 2.1 and later.
- Jabber for iPhones and for Android 9.6 and later.

Note You cannot play back a recording on mobile device. If you started a meeting by using an Android mobile device, you can start and manage the recording of a meeting. If you started a meeting by using an iOS mobile device, you cannot start or manage the recording of a meeting on the iOS device.

Citrix Virtual Apps and Desktops Support

Cisco Webex Meeting Server supports Citrix Virtual Apps and Desktops 7.6, 7.11, 7.12 and 7.15, with the following operating systems:

- **Host Operating Systems:** Microsoft Windows and Mac
- **Virtual Operating Systems:** Microsoft Windows 7, Windows Server 2012R2, and Windows Server 2016

The host operating system is the operating system installed on the end user's computer. The virtual operating system is the operating system delivered by the server.

About Host Licenses

This product has **Host-based Licensing** requiring that you purchase a license for each user that **hosts** meetings or is manually assigned a license. A user does not consume a Host license by attending or scheduling a meeting on behalf of others. The license usage calculation for reporting purposes occurs once per month, for example, once from January 1 through 31, and once from February 1 through 28, and so forth.

Note When upgrading from a previous version, all licenses that were on the original system are released from their assignment to users. Users can reacquire licenses by hosting meetings or being manually assigned licenses. This is also true when installing a Multi-data Center (MDC) system. Host licenses are lost on the data center joining the MDC system. Those licenses can be re-hosted on the MDC system after the join.

From the **Reports** page, you can request a report that provides the total number of licenses consumed. In addition, we recommend that you view the PDF Summary Report that shows license consumption trends. By viewing the overall license trend, you can plan for future license purchases more effectively, to match the growing adoption of this system within your company.

CHAPTER 11

Cisco Webex Meetings Server Integration and Audio Endpoint Compatibility

CUCM Feature Compatibility and Support

Cisco Webex Meetings Server (CWMS) supports Cisco Unified Call Manager (CUCM) 8.6 or 9.0 without TLS/SRTP, and CUCM 9.1, 10.0, 10.5, 11.0(1a), 11.5, 11.5(1)SU1 and later service updates (SU), and 12.0SU1 and later SUs.

For a list of CUCM releases tested with CWMS, see the *Release Notes for Cisco Webex Meetings Server* for your release.

Important TLS connections between CUCM and CWMS fail with releases of CUCM that do not support certificates that are signed with a signature algorithm SHA256 with RSA encryption.

Upgrade CUCM to a version that supports this signature algorithm or obtain a third-party certificate that is signed with SHA1 with RSA encryption. According to the latest National Institute of Standards and Technology (NIST) recommendation, SHA1 should not be used for digital signature generation because it has a security vulnerability.

Session Manager Edition (SME) Integration

CWMS supports Session Manager Edition (SME).

Unified MP users can choose Cisco Webex as the web conferencing provider when scheduling a Unified MP meeting. Cisco Webex integration is available in Cisco Unified MP 6.0.2 and later releases. Unified MP provides voice and video conferencing. To join a Unified MP meeting, Webex users require the voice and video dial-in information, or they can use the out-dial feature that is available in Webex.

Audio Endpoint Compatibility

You can use any standards-based audio endpoint that connects to Cisco Unified Communications Manager to join a Webex meeting. The supported audio endpoints include the Cisco IP Phones, Telepresence endpoints, and PSTN devices such as mobile phones and land line phones. Many audio endpoints support audio and video connectivity. However, only audio connectivity to the Cisco Webex Meetings Server is supported.

To permit users from outside the organization to join Webex meetings by using PSTN devices, your company must deploy Analog-to-VoIP Gateways, such as Cisco Integrated Service Routers (ISR). The IP phones listed below have been tested with Cisco Webex Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Lifesize video phone
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

Other Cisco UC-compatible endpoints should also operate normally. For a list of Cisco Unified IP Phones supported by Cisco Unified Communications Manager and the Device Packs available for each model, see Cisco Unified IP Phone Feature and Cisco Unified Communications Manager Device Pack Compatibility Matrix .