Cisco WebEx Meetings Server Planning Guide

First Published: October 21, 2012

Last Modified: October 21, 2012

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

Introduction and Datacenter Topology For Your System

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

Introducing Cisco WebEx Meetings Server

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

Cisco WebEx Meetings Server addresses the needs of today's companies by presenting a comprehensive conferencing solution with all the tools needed for effective and engaging collaboration. It delivers an interactive and productive experience for users.

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 5.0. It features a rapid virtual deployment and powerful tools for administrators to configure and manage the system and see key system metrics.

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.

In addition, mobile users can attend and participate in meetings from their iPhone and iPad.

Important Considerations For Your System

Note the following:

- Forward proxies—not recommended, though you may use forward proxies with restrictions.

  For complete details, see the *Cisco WebEx Meetings Server Troubleshooting Guide*.
- Reverse proxies—only the Internet Reverse Proxy 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, on page 49.
- Multiple datacenters—only a deployment within a single datacenter is supported for this release.

  For complete details, see Deploying Your System in a Single Datacenter, on page 2.

⚠ **Caution** If you disregard our recommendations and requirements when deploying your system, Cisco is not responsible for any problems you may encounter as a result of not following our guidance.

Information for Cisco Unified MeetingPlace Customers

If you are a former or existing Cisco Unified MeetingPlace customer, see the *Cisco WebEx Meetings Server Release Notes* for information about the transition to this new product.

Important 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 may ease the transition for your users by continuing to support both Cisco Unified MeetingPlace and Cisco WebEx Meetings Server for a period of time while encouraging your users to switch to the new system. To help with user training during this transition, Cisco provides training videos that may be accessed from the end user Help page.

Deploying Your System in a Single Datacenter

The current system design, with an optional HA system, is designed for a single data center deployment.

The HA system comprises redundant virtual machines for each virtual machine type in your deployment. For example:

- A primary 250 user system comprises an Admin virtual machine, a Media virtual machine, and an Internet Reverse Proxy (for public access). If you add a HA system, the combined 250 user system comprises two Admin virtual machines, two Media virtual machines, and two Internet Reverse Proxy virtual machines.
- A primary 2000 user system comprises an Admin virtual machine, three Media virtual machines, two Web virtual machines, and an Internet Reverse Proxy (for public access). If you add a HA 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 Internet Reverse Proxy virtual machines.

In an HA system, the public VIP address and private VIP address are shared. When one virtual machine is down, the other virtual machine uses the same VIP address. Because of this behavior, a virtual machine failure is almost completely transparent to end users (as meetings will 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. From our experience, splitting a VLAN across two datacenters creates a variety of problems.

We require highly available connectivity between the internal virtual machines, greatly reducing the problem of distinguishing between a virtual machine failure and a network failure. Allowing a split network may result in split meetings and conflicting database updates. It is more practical to construct a true highly available network segment within a single datacenter than between two datacenters.

Cisco believes 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 that connection results in delays for end users, particularly when scheduling or joining meetings. Latency between media service components directly increases audio and video latency for some users during meetings.

Using VMware vSphere With Your System

VMware vSphere

This product only installs on a VMware vSphere virtualization platform. (For complete details on VMware requirements, see the *Cisco WebEx Meetings Server System Requirements*).

Cisco mandates the deployment of the product in a single datacenter only. Except for the smallest configuration, all installations deploy multiple virtual machines.

- To save you time, Cisco recommends standard Cisco UCS servers with specific configurations of hardware and VMware products.
- However, Cisco WebEx Meetings Server is designed to work on any equivalent Cisco UCS Server that meets or exceeds these specifications.

  For complete details on the hardware and VMware requirements, see the *Cisco WebEx Meetings Server System Requirements*.
- You must purchase VMware vSphere 5.0 for use as the hypervisor platform for Cisco WebEx Meetings Server by completing one of the following:
  - Buy vSphere 5.0 directly from Cisco on the GPL (Global Price List). Cisco is an approved VMware partner and distributor.

    This is convenient for those who "want everything from a single vendor".
  - Purchase vSphere 5.0 directly from VMware, through enterprise agreements you have directly with VMware.

Advantages of Deploying on Your 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 5.0 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.
- Cisco WebEx Meetings Server requires customers to run VMware ESXi 5.0, ESXi 5.0 Update 1, or the VMware ESXi 5.0 installable Cisco ISO Image. Both these editions contain the necessary drivers required to support the Cisco UCS Servers that are required by Cisco WebEx Meetings Server. For more information, see http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf.

Easy Recovery From System Errors

- By using VMware Data Recovery, you have the ability to revert system-impacting changes rapidly, if the change does not meet your expectations. This helps prevent the system from going down with possibly a painful system redeployment.

vSphere Considerations

Note the following considerations:

- You may move your virtual machine to another ESXi host. However, you must retain the layout of the virtual machines on the 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 legacy ESXi host.

- Although you may move your virtual machines, you may not do so using either VMotion or Storage VMotion, as they are not supported in this release.
- VMware Distributed Resource Schedule (DRS) is not supported.
- vSphere High Availability (HA) is not supported.
- vSphere clustering and resource sharing are not supported.

vSphere Best Practices For This Product

- Cisco recommends against using virtual machine snapshots. If you decide to use snapshots, then after confirming your system changes, as applicable either commit the snapshots or remove them as soon as possible. Keeping a snapshot for any period of time will result in performance degradation.
- For SAN environments, deploy disk images to a SAN with high IOPS numbers.
- Make sure there's 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.
- Keep all virtual machines managed by the same vCenter. This allows for an easier recovery should you need to recover your system.

vCenter Server Requirements

In addition to vSphere 5.0, vCenter Server 5.0 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.
- Although the vSphere Standard Edition is required for a 50 or 250 user system, you may consider the alternative of purchasing the vSphere 5.0 Essentials Plus kit. Note that the vSphere 5.0 Essentials Plus kit is useful primarily for budget-conscious customers deploying the 50 user system. However, the Essentials Plus kit does not provide several advanced capabilities that typical enterprise customers require.

vSphere 5.0 Enterprise Plus 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.
- At minimum, you must purchase the vSphere 5.0 Enterprise Plus edition as the lower-end vSphere editions do not support the number of required vCPUs.

vSphere 5.1 Is Not Supported For This Release of Cisco WebEx Meetings Server

- Cisco WebEx Meetings Server 1.0 only supports vSphere releases 5.0 and 5.0 Update 1. It does not currently support vSphere 5.1.
- As VMware no longer sells vSphere 5.0, you should purchase vSphere 5.1 from VMware or directly from Cisco. Then "downgrade" to vSphere 5.0 to host Cisco WebEx Meetings Server. Your vSphere 5.1 license gives you the right to downgrade to vSphere release 5.0.

General Concepts For Your System Deployment

System Sizes

- 50 concurrent users system
    - Typically supports a company between 500 and 1000 employees
    - Primary system (without HA) comprises an Admin virtual machine and an optional Internet Reverse Proxy (for public access)
- 250 concurrent users system
    - Typically supports a company between 2500 and 5000 employees
    - Primary system (without HA) comprises an Admin virtual machine, a media virtual machine, and an optional Internet Reverse Proxy (for public access)
- 800 concurrent users system
    - Typically supports a company between 8000 and 16,000 employees
    - Primary system (without HA) comprises an Admin virtual machine, a media virtual machine, and an optional Internet Reverse Proxy (for public access)
- 2000 concurrent users system
    - Typically supports a company between 20,000 and 40,000 employees
    - Primary system (without HA) comprises an Admin virtual machine, 3 media virtual machines, 2 web machines, and an optional Internet Reverse Proxy (for public access)

Terms Used During the Deployment

Field Name	Description
WebEx Site URL	Secure http URL for users to host and attend meetings.
WebEx Administration URL	Secure http URL for administrators to configure, monitor, and manage the system.
Public VIP	IP address for the WebEx site URL
Private VIP	• IP address for the Administration site URL • IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).

Joining Meetings

Users can join meetings through a browser or through a client on their desktops.

For complete details on the end user experience, see the end user online help for this product. Sign in to the WebEx site and select **Help**.

Windows Users

- For Microsoft Internet Explorer 8 and 9, 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 client software is downloaded and automatically installed the first time the user joins a meeting.
- For 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.
- The preceding bulleted items assume a user has Windows Administrator privileges on their PCs to join WebEx meetings. If this is not true, then system administrators may push the WebEx Meetings application client to user desktops by using standard desktop management software such as IBM Tivoli. See Downloading and Mass Deploying Applications, on page 75.
- There are no specific administrator settings for ActiveX, Java plug-in, WebEx Meetings application installer or TFS with this product.

Mac Users

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

CHAPTER 2

Networking Topology For Your System

End user experience with Cisco WebEx Meetings Server is of a web site, that users access to schedule and join meetings. A special aspect of this web site is real-time conferencing elements that facilitate online meetings.

This chapter describes the different networking topologies supported for this product, including the advantages and disadvantages of each. Select the one that best meets your needs and your network deployment. However, if you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine that enables public access.

Recommended Network Topology

Cisco WebEx Meetings Server comprises two groups of virtual machines: the internal virtual machines and the Internet Reverse Proxy virtual machines. All systems must comprise one or more internal virtual machines. The Internet Reverse Proxy is required only for systems where external users can host or attend meetings from the Internet and mobile devices. Without an Internet Reverse Proxy, only internal and VPN users can host or join meetings.

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 HA virtual machines, are connected together on a local LAN, offering high bandwidth, negligible packet loss, and latency under 1 ms, between these virtual machines. The Cisco WebEx Meetings Server system is not designed to be split between multiple data centers.

- Cisco recommends placing all the internal virtual machines on the same Ethernet switch (usually on the same rack as the virtual machines) with a minimum throughput of
  - 1 Gbps for 50 user and 250 user systems
  - 10 Gbps for 800 user and 2000 user systems

  for links between the edge and core switches. Network latency must be less than 1 ms.

  Note On the Internet Reverse Proxy, the NIC sees double the network traffic of other devices because the connections go through it twice, inbound and outbound.

  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.

- If you decide instead to place the virtual machines on different Ethernet switches within the same datacenter, then your network *must meet* the requirements listed in this section. 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 Redundant Network in HA Deployments, on page 10.

Internet Reverse Proxy Virtual Machines

- 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.
- Because it is common to separate the internal virtual machines from the Internet Reverse Proxy virtual machines on different racks, servers, and ESXi hosts, Cisco recommends:
  - 50 and 250 user systems—dual redundant 1 Gigabit Ethernet links between the DMZ switches and the switches used by the internal virtual machines.
  - 800 and 2000 user systems—dual redundant 10 Gigabit Ethernet links between the DMZ switches and the switches used by the internal virtual machines.

Redundant Network in HA Deployments

- The redundant (HA) virtual machines must be co-located in the same data center with 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.

Important Cisco does not recommend splitting the primary and redundant (HA) components of the system between data centers.

- Connectivity between all the internal virtual machines, both primary and HA, must be fully redundant, so that the failure of a switch or network link will not sever the connectivity between the primary and HA components. To achieve this redundancy, each host server should have dual redundant connections to a pair of Ethernet switches (that is, a connection to switch A plus a connection to switch B).
- The primary and redundant (HA) Internet Reverse Proxy virtual machines must be on a common VLAN or subnet (typically not the same subnet as the internal virtual machines). Connectivity between these two Internet Reverse Proxy virtual machines should be fully redundant, in the same manner as the internal virtual machines.

Different Types of Network Topology For Your System

This product supports the following network topologies:

- Internal Internet Reverse Proxy Network Topology, on page 11
- Non-Split-Horizon Network Topology, on page 12
- All Internal Network Topology, on page 13
- Split-Horizon Network Topology, on page 14

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 Network Topology

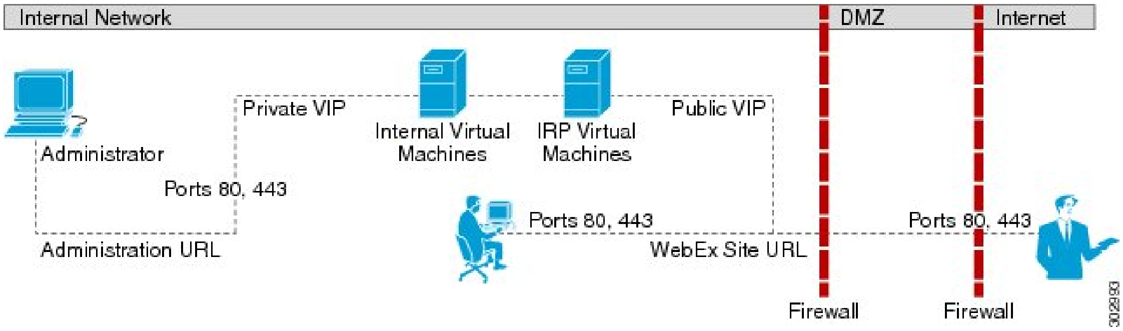
This section describes the network topology when all the virtual machines in your system, including the Internet Reverse Proxy, are in the same internal network.

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

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

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 an all internal Internet Reverse Proxy network topology.



Note 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 44.

Advantages of an All Internal Internet Reverse Proxy Network Topology

- Provides lower latency as there are fewer network hops between the virtual machines.
- Compared with the non-split-horizon network topology, there are no virtual machines in the DMZ.
- Compared with the non-split-horizon network topology, the network traffic for internal users will not connect through the DMZ to host or attend meetings.

Disadvantages of an All Internal Internet Reverse Proxy 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.

Non-Split-Horizon Network Topology

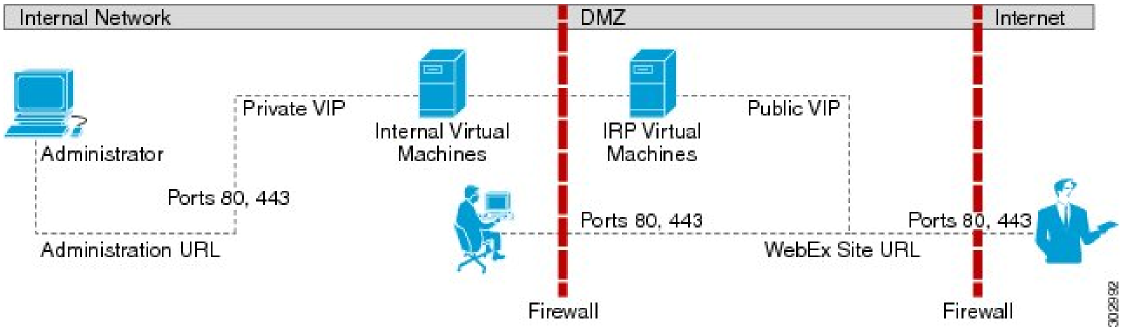
This section describes the network topology when you have a non-split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

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

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 45.

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) will go to the Internet Reverse Proxy in the DMZ network, then come 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.

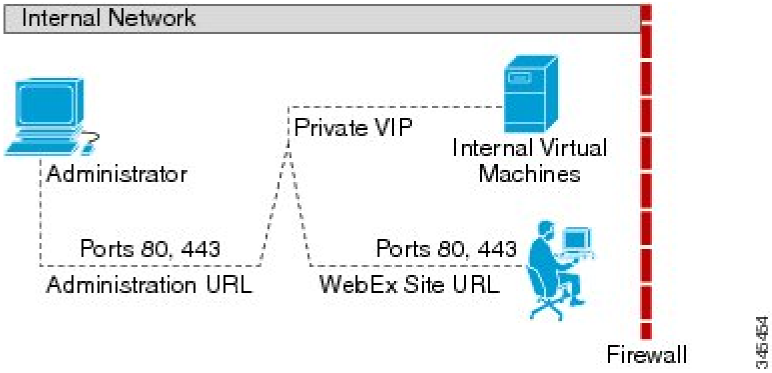
All Internal Network Topology

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.

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

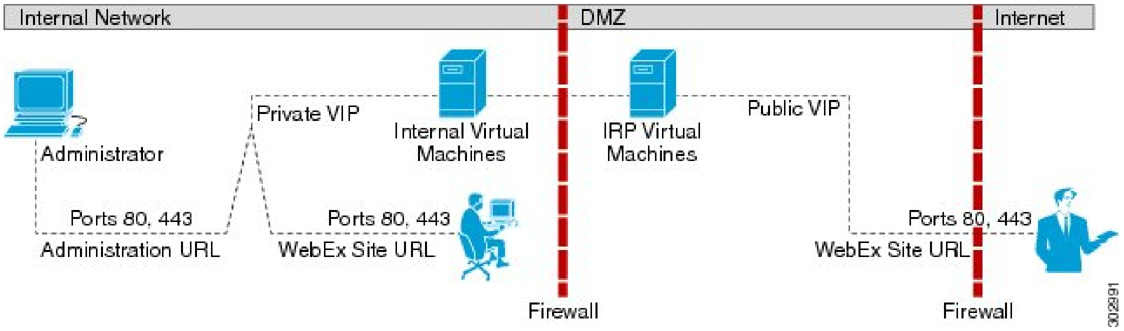
This section describes the network topology when you have a split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

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

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 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 45.

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 will go to the Internet Reverse Proxy. The traffic coming from the internal (private network) will go 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 as well as the Media virtual machines.

CHAPTER 3

Choosing the System Size

This chapter describes the different system sizes, and provides guidance to help you determine the correct size for your company.

Users

- Users cannot be deleted from the system. However, you may deactivate a user from the system.

  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.

- 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.

Deployment Sizes For Your System

Determining the System Size

When determining the size for your system, consider how many users you expect to be using the system at any given time. For a 50 user system, the maximum number of users concurrently attending meetings is 50.

If more than 50 users attempt to start or attend a meeting, they may see error messages stating that they cannot start or attend a meeting at that time.

- Determine the number of users that will be concurrently attending meetings at any given time. You want to select a system size that will accommodate your users in most cases, excepting rare or unusual occurrences.
- Once you select a system size, you can always expand the system later, to a larger size. However, your hardware must meet or exceed the minimum requirements for the larger size or you must purchase additional hardware.
- If you are planning to add high availability for your system, you will deploy both a primary system and a HA system, then "combine" them into a single system, with high availability. Be sure to include the additional virtual machines for the HA system in your hardware purchases.

  Note Adding an HA system does not increase "port" or system capacity. It simply provides some protection against virtual machines failures in your system.

Note Once you determine the system size for your company, be sure to purchase the appropriate hardware and enough VMware licenses to support the minimum requirements for that system size.

- 50 User System, on page 19
- 250 User System, on page 20
- 800 User System, on page 20
- 2000 User System, on page 21

Requirements for vCenter Co-residency

VMware vCenter co-location (co-residency) is only supported with the 50 and 250 concurrent user system configurations.

Note If you plan to place VMware vCenter on the same host as a 50 or 250 concurrent users system, then you must order additional RAM with your UCS server. For the exact amount of RAM required, see the requirements for that system size in the *Cisco WebEx Meetings Server System 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. Although this is optional, Cisco encourages its use as it provides a better user experience for your mobile workforce.

  Note Only the Internet Reverse Proxy 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 Internet Reverse Proxy 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, and if applicable, the media and web virtual machines.

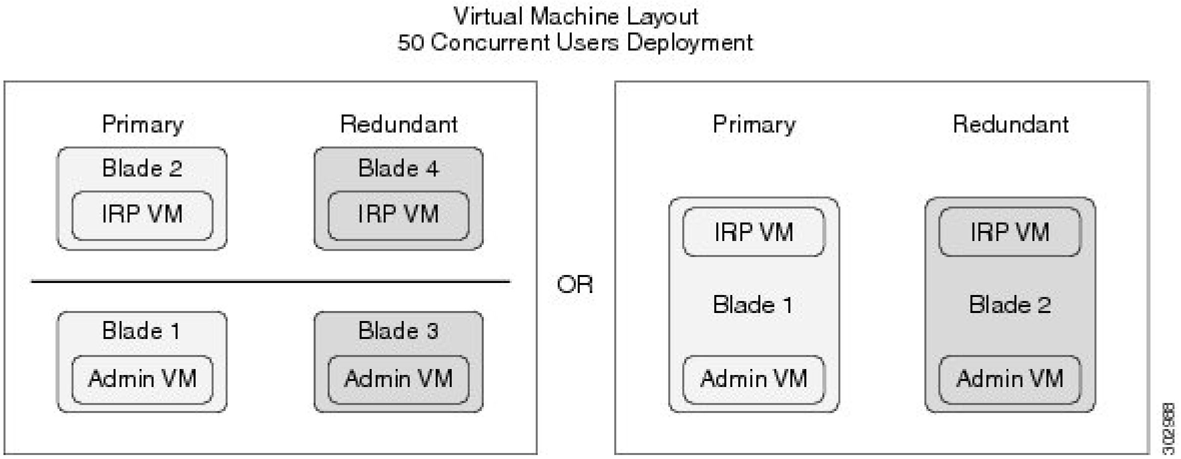
The Internet Reverse Proxy is situated in the DMZ network (non-split-horizon and split-horizon network topologies) or in the internal network (all internal network toplogy.)

- Non-Split-Horizon Network Topology, on page 12
- Split-Horizon Network Topology, on page 14
- Internal Internet Reverse Proxy Network Topology, on page 11

50 User System

This is a schematic diagram of a 50 user system. The diagram illustrates two versions of a 50 user deployment. If you plan to add a HA system, those virtual machines are shown as the "redundant" virtual machines. If you do not want HA, then only deploy the primary system.

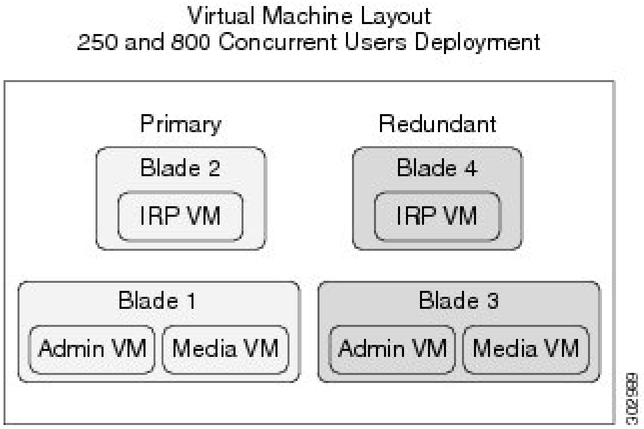
Note For brevity, we use the acronym IRP for the Internet Reverse Proxy in the following diagram.



250 User System

This is a schematic diagram of a 250 user system. If you plan to add a HA system, those virtual machines are shown as the "redundant" virtual machines. If you do not want HA, then only deploy the primary system.

Note For brevity, we use the acronym IRP for the Internet Reverse Proxy in the following diagram.

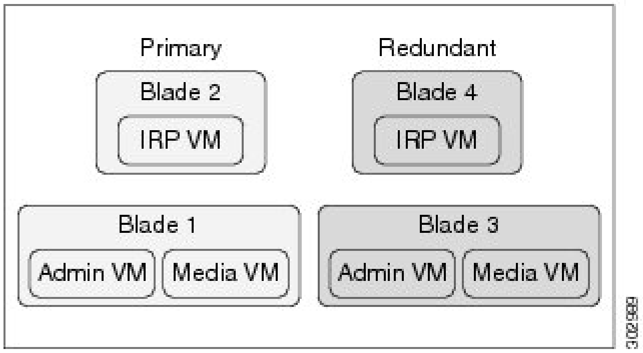


800 User System

This is a schematic diagram of a 800 user system. If you plan to add a HA system, those virtual machines are shown as the "redundant" virtual machines. If you do not want HA, then only deploy the primary system.

Note For brevity, we use the acronym IRP for the Internet Reverse Proxy in the following diagram.

Virtual Machine Layout
250 and 800 Concurrent Users Deployment



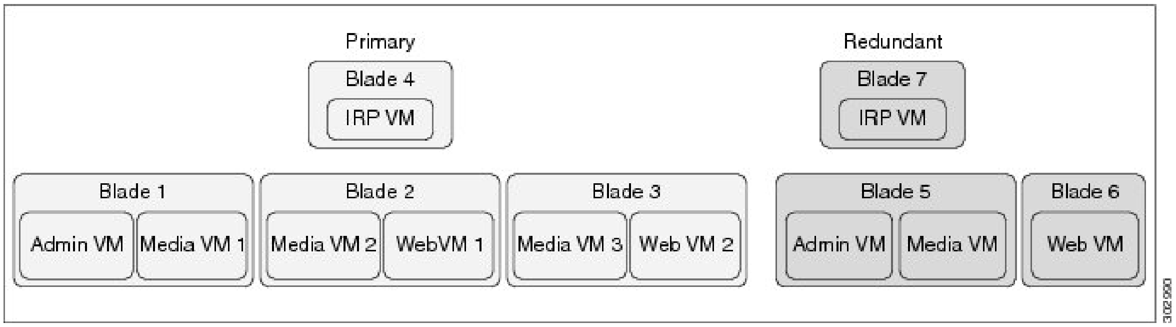
2000 User System

This is a schematic diagram of a 2000 user system. If you plan to add a HA system, those virtual machines are shown as the "redundant" virtual machines. If you do not want HA, then only deploy the primary system.

Note For brevity, we use the acronym IRP for the Internet Reverse Proxy in the following diagram.

Important Be sure to deploy the virtual machines as shown in the following diagram. By deploying different types of virtual machines on a physical server, you can better avoid a system shutdown in case 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.)

Virtual Machine Layout
2000 Concurrent Users Deployment



CHAPTER 4

Networking Changes Required For Your Deployment

This chapter provides a list of the changes you need to make for your system deployment:

- IP addresses required for your system
- DNS configuration changes
- Firewall configuration and port access
- Network routing changes

- Using NAT With Your System, page 49
- Forward Proxies, page 52

Networking Checklist For Your System

The networking checklist lists the networking changes required for your system, depending on your company's DNS configuration and whether or not you enable public access (users can host or attend meetings from the Internet or mobile devices).

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 for your system)
    - Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines, on page 25
    - Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines, on page 27
- Non-split-horizon DNS (the most common DNS configuration for companies)
    - Networking Checklist for an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS, on page 30
    - Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS, on page 32
- Split-horizon DNS
    - Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS, on page 35
    - Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS, on page 37
- Systems without public access
    - Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access, on page 40
    - Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access, on page 42

Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines

Virtual Machine Deployment

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

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

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 virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-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, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, 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 44.

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	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
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>

Task	Compare These IP Addresses
Ensure 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)	

Description	Network Location	IP Address
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.

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>

Task	Example
Update your DNS server with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends 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 44.

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. **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>

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 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. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is 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 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)	

Description	Network Location	IP Address
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 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.

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 virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-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, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 45.

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	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
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>
Ensure 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.

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>

Task	Example
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, Cisco recommends 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 45.

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. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is 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 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)	

Description	Network Location	IP Address
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 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.

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 virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
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, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 45.

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	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
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>
Ensure 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)	
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.

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 (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, Cisco recommends 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 45.

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>
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. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure 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)	
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)	

DNS Configuration

Make the following changes to your DNS configuration.

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 virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-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 virtual machine, and Media virtual machine, if applicable) 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)	

Description	Network Location	IP Address
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.

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>

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.

Port Access in the External Firewall

If you have enabled public access, then the following ports are open inbound directly from the Internet to the Internet Reverse Proxy virtual machines in the internal network:

Important 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

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 in the DMZ network.

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

Port Access in the External Firewall

If you have enabled public access, then the following ports are open inbound from the Internet to the Internet Reverse Proxy virtual machines in the DMZ:

Important 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.

Note Cisco strongly recommends that you open port 80 (http) in addition to port 443 (https), to simplify the end user experience (in a browser, users enter the WebEx site URL without having to remember whether it is http or https. However, for this product, the actual network traffic always flows over port 443 (SSL encrypted https).

Protocol	Port	Source	Destination	Why It Is Needed
TCP	443	Any external clients	Public VIP (Eth1) of the Internet Reverse Proxy	External clients accessing the WebEx site URL using https. TCP connections are initiated from the external client machines to the Internet Reverse Proxy virtual machines.
TCP	80	Any external clients	Public VIP (Eth1) of the Internet Reverse Proxy	External clients accessing the WebEx site URL using http. TCP connections are initiated from the external client machines to the Internet Reverse Proxy virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
UDP	53	Real IP (Eth0) of the Internet Reverse Proxy	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

The following ports must be open when the Internet Reverse Proxy is in the DMZ network. If you have restrictions on connections from the internal network to the DMZ network, then the following table applies. Allow TCP connections *outbound* from the internal network to the DMZ network segment on the following ports.

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

Note UDP port 10162 is the only port that is open inbound from the DMZ to the internal virtual machines. This port is required for monitoring of the Internet Reverse Proxy by the system.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64001	All internal virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed by the internal virtual machines for establishing reverse connections to the Internet Reverse Proxy. TCP connections are established from the internal virtual machines to the Internet Reverse Proxy virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	7001	All internal virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed by the internal virtual machines for establishing reverse connections to the Internet Reverse Proxy. TCP connections are initiated from the internal virtual machines to the Internet Reverse Proxy virtual machines.
TCP	64616	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed for bootstrapping the Internet Reverse Proxy. TCP connections are initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines.
TCP	873	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed to collect logs from the Internet Reverse Proxy. TCP connections are initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines.
TCP	22	Any internal client machines	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed for troubleshooting the Internet Reverse Proxy virtual machines using a Remote Support Account.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	443	Any internal client machines	Private VIP (Eth1) of the Admin virtual machines	Internal users accessing the WebEx site URL using https. TCP connections are established from the internal client machine to the Admin virtual machine.
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.
TCP	10200	Any internal client machines	Real IP (Eth0) of the Admin virtual machines	This is needed for the initial system deployment. TCP connections are established from the internal client machines to the Admin virtual machines.
UDP	161	Real IP (Eth0) of the Admin virtual machines	Real IP (Eth0) of the Internet Reverse Proxy	Needed to allow SNMP GET requests to be sent from the Admin virtual machines to the Internet Reverse Proxy virtual machines. The UDP connection is initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
UDP	10162	Real IP (Eth0) of the Internet Reverse Proxy	Real IP (Eth0) of the Admin virtual machines	Needed to allow SNMP traps and information to be sent from the Internet Reverse Proxy virtual machines to the Admin virtual machines. The UDP connection is initiated inbound from the Internet Reverse Proxy to the Admin virtual machines.
UDP	53	All internal virtual machines (Eth0 IP)	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.

VMware vCenter Ports

These ports are only 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.

- 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
- TCP Port 443 from vCenter to the ESXi hosts for secure https 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

Using NAT With Your System

Cisco supports Network Address Translation (NAT) traversal with this product for virtual machine IP addresses and for the virtual IP addresses (Public and Private VIPs) that are used in your system.

Note For more information about NAT, see http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

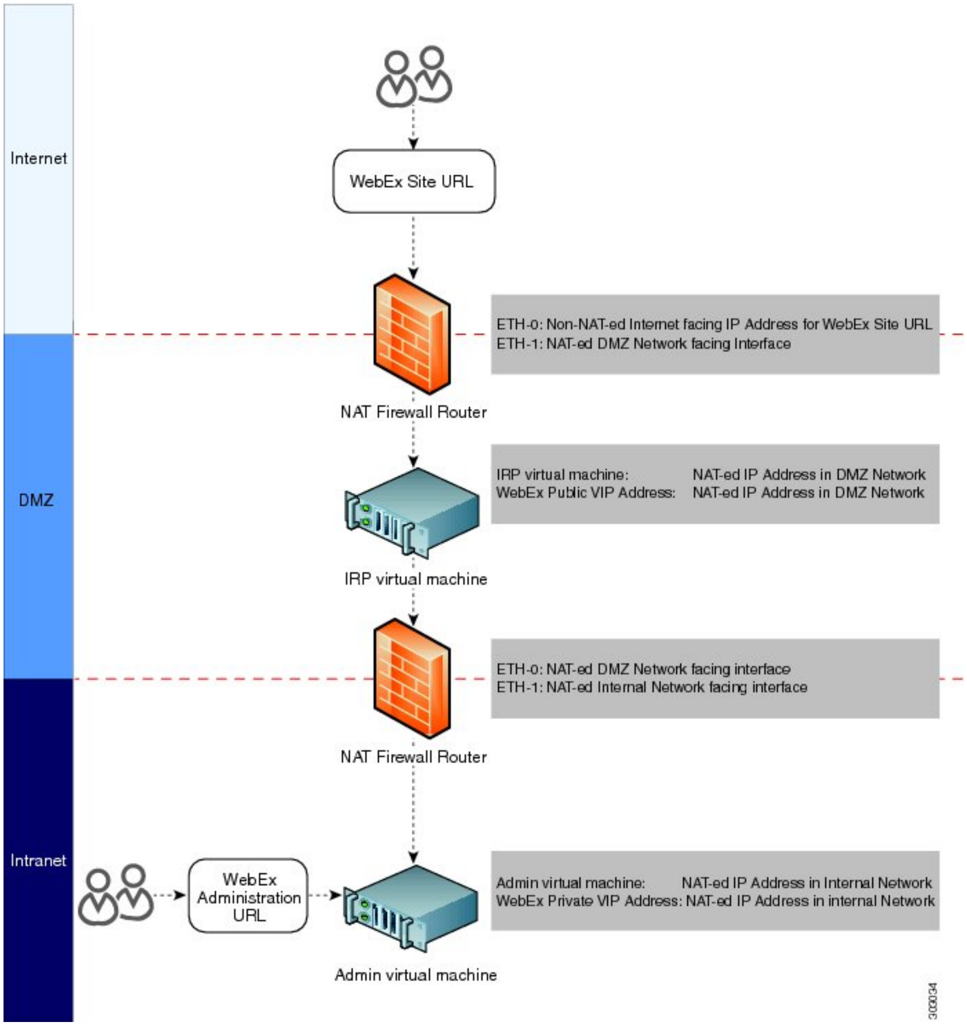
The following schematic diagram illustrates a typical NAT traversal for a 50 user system without HA. By using NAT, you can reduce the number of *public IP addresses* required for the product to just one IP address, instead of two (or three if you deploy HA). You may also deploy similar NAT deployments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

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

Important When using multiple NAT domains, then routing between these various NAT domains may be challenging. However, you may use NAT-ed IP addresses as long as the following requirements are met:

- All the virtual machines in the system may use NAT-ed IP addresses.
- The Internet Reverse Proxy virtual machine IP address must be reachable by the Admin virtual machine in 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 may 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.


Internet
DMZ
Intranet
WebEx Site URL
ETH-0: Non-NAT-ed Internet facing IP Address for WebEx Site URL
ETH-1: NAT-ed DMZ Network facing Interface
NAT Firewall Router
IRP virtual machine: NAT-ed IP Address in DMZ Network
WebEx Public VIP Address: NAT-ed IP Address in DMZ Network
IRP virtual machine
ETH-0: NAT-ed DMZ Network facing interface
ETH-1: NAT-ed Internal Network facing interface
NAT Firewall Router
WebEx Administration URL
Admin virtual machine: NAT-ed IP Address in Internal Network
WebEx Private VIP Address: NAT-ed IP Address in internal Network
Admin virtual machine
303034

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 may 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 may use NAT IP addresses for the private VIP address and the Admin virtual machine IP addresses.

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

System Capacity Quick Reference Tables

This module contains the system capacity tables for the system.

Maximum System Capacity and Scalability for Each System Size

The following table lists the maximum capacity for each system size.

Maximum Number	50 Concurrent Users	250 Concurrent Users	800 Concurrent Users	2000 Concurrent Users
Audio and web users (combined)	50	250	800	2000
Concurrent high-quality video users and video file sharing (combined)	25	125	400	1000
Participants in a meeting	50	100	100	100
Playback recordings of meetings that have ended	13	63	200	500
Recordings of meetings in progress	5	25	80	200
Calls per second	1	3	8	20
Conferences (assuming 2 participants per meeting)	25	125	400	1000

The maximum aggregate bandwidth utilization requirements are:

- 50 concurrent users—125 Mbps

- 250 concurrent users—625 Mbps
- 800 concurrent users—2 Gbps
- 2000 concurrent users—5 Gbps

This list is calculated based on the assumption that the worst case bandwidth usage is 1.8 Mbps, *per user connection*, on an aggregate basis. This value includes the limitation that only one-half of the maximum number of users can be using video at any time, and that users will typically not be in "theater mode" when slides are flipping or a video share is running. The average usage is less than one-half this value, but you should exercise caution when provisioning lower bandwidth as the user experience degrades rapidly when network links are saturated. This traffic is seen on the network links coming in to and out of the data center.

Note The bandwidth requirements for this product are fundamentally the same as for Cisco WebEx cloud services. If you wish to optimize your network provisioning, see http://www.webex.com/pdf/wp_bandwidth.pdf.

For complete details on system capacity, see the *Cisco WebEx Meetings Server System Requirements*.

CHAPTER 6

Configuring Cisco Unified Communications Manager (CUCM)

Configuring Cisco Unified Communications Manager (CUCM)

Configure call control settings with CUCM. You must configure one CUCM system to manage call control but you can optionally configure a second CUCM system for audio high availability.

Cisco WebEx Meetings Server supports CUCM 7.1, 8.6, and 9.0.

Configuring a single CUCM system (no audio high availability) requires the following:

- To call in to your Cisco WebEx Meetings Server system from CUCM, you must configure a call-in route pattern on your conferencing load balancer servers and several SIP route patterns on your conferencing application servers. A call-in route pattern enables CUCM to route calls based on a dial-in phone number that you configure. SIP route patterns are telephony call route patterns that enable CUCM to route calls based on the SIP URL in the SIP messages of calls that are placed.

Note The call-in route pattern number is also the number you use as your call-in access number when you configure your audio features in the Administration site. Make sure to configure your port numbers as described in the following sections.

  - Configure several SIP trunks pointing to your Cisco WebEx Meetings Server conferencing load balancers and configure a route group, a route list, and a route pattern.
  - Configure several SIP trunks pointing to your Cisco WebEx Meetings Server conferencing application servers and configure several SIP route patterns.

- To call out to CUCM from Cisco WebEx Meetings Server:
  - Sign in to the Administration site and configure your CUCM settings. Refer to "Configuring Your Audio Settings for the First Time" in the Administration Guide for more information.

    Note CUCM requires that the conference application server is configured on CUCM as a SIP trunk. Otherwise it will reject messages from the application server.

CUCM Feature Compatibility and Support

The following tables provide feature compatibility information for the supported versions of CUCM.

CUCM Feature Compatibility

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 Cisco WebEx Meetings Server does not support any unlisted CUCM versions or other third-party SIP proxy management applications.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0	Pre-Conditions/Remarks
Call out (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0	Pre-Conditions/Remarks
Call in (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.
TLS/SRTP	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with security certificates.
RFC2833	Yes	Yes	Yes	Select this option during CUCM SIP trunk configuration.
KPML	Yes	Yes	Yes	Select this option during CUCM SIP trunk configuration.
Keepalive—Cisco WebEx Meetings Server sending	Yes	Yes	Yes	Performed using the SIP OPTIONS message.
Keepalive—Cisco WebEx Meetings Server receiving	No	Yes	Yes	Performed using the SIP OPTIONS message.
Quality of Service	Yes	Yes	Yes	For control packets.
TCP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balancer servers; 5062 for conferencing application servers.
TLS	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5061 for conferencing load balancer servers; 5063 for conferencing application servers.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0	Pre-Conditions/Remarks
UDP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balancer servers; 5062 for conferencing application servers.
Self-signed certificates	Yes	Yes	Yes	n/a
Third-party certificates	Yes	Yes	Yes	n/a

Telephony Call Features

Cisco WebEx Meetings Server supports the following CUCM call features.

Note The CUCM 9.0 software that is part of the BE6K (Business Edition 6000) product is also supported by Cisco WebEx Meetings Server.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0
Call hold	Yes	Yes	Yes
Call un-hold	Yes	Yes	Yes
Caller ID display on EP	Yes	Yes	Yes
Calling name display on EP	Yes	Yes	Yes
Call transfer (IPv4 to IPv4)	Yes	Yes	Yes
Call transfer (IPv6 to IPv4)	Yes	Yes	Yes
Call transfer (IPv4 to IPv6)	No	No	Yes
Call transfer (IPv6 to IPv6)	No	No	Yes

Telephony Media Features

Cisco WebEx Meetings Server supports participants with G.711/G.722/G.729 codecs at the same time. Changing your codec configuration does not affect system performance.

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

CUCM Base Configuration

You must create some base CUCM configurations to manage calls for your Cisco WebEx Meetings Server system. Multiple systems can share the same base configuration. Your base configuration consists of the following:

- SIP trunk security profile
- SIP profile

Configuration Checklist

The configuration checklist displays the number of each CUCM configuration type that you must configure for your system.

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[1]	1
50 users with high availability	2	1	4	1	1	N	2
250 users	2	1	2	1	1	N	1
250 users with high availability	2	1	4	1	1	N	2
800 users	2	1	2	1	1	N	1
800 users with high availability	2	1	4	1	1	N	2

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)
2000 users	2	1	5	1	1	N	3
2000 users with high availability	2	1	6	1	1	N	4

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

Configuring a SIP Trunk Security Profile

Configuring a SIP Trunk Security Profile for a Load Balancer Server

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 Administration Guide.

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 using UDP/TCP. Select **Encrypted** if you want CUCM communicate Cisco WebEx Meetings Server using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.

  Note If you want CUCM to communicate with Cisco WebEx Meetings Server 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 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 them with their default settings.

Step 6 Select **Save**.

Configuring a SIP Trunk Security Profile for an Application Server

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 Administration Guide.

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 using UDP/TCP. Select **Encrypted** if you want CUCM communicate Cisco WebEx Meetings Server using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.

  Note If you want CUCM to communicate with Cisco WebEx Meetings Server 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 Cisco WebEx Meetings Server using UDP/TCP. Enter 5063 if you want CUCM communicates Cisco WebEx Meetings Server using TLS.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

Configuring a SIP Profile

Configuring a Standard SIP Profile

The standard 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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields:

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

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.
- Enable ENAT—Select the check box.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

CUCM Specific Configuration

The following CUCM configurations must be made for individual Cisco WebEx Meetings Server systems. These configurations cannot be shared by multiple systems.

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

Certificate Management

If you want CUCM to communicate with Cisco WebEx Meetings Server using TLS, you must perform the following actions:

- Obtain a Cisco WebEx Meetings Server certificate from the Administration site and then upload it to CUCM.
- Download your CUCM certificate and then upload it to Cisco WebEx Meeting Server Administration site.

Refer to "Managing Certificates" in the online help and *Administration Guide* for more information.

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 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 certificate that you saved to your local hard drive.

Step 8 Select **Upload File**.
Wait for your system to indicate "Success: Certificate Uploaded."

Step 9 Select **Close**.

Downloading CUCM Certificates

Refer to your CUCM documentation for more information on generating CUCM certificates.

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 OS Administration**.

Step 3 Select **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 Select **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 online help and *Administration Guide*.

Configuring a SIP Trunk

Configuring a SIP Trunk on a Load Balancer Server

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 **Device** > **Trunk**.

Step 4 Select **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 them at their default settings.

Step 6 Select **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 your load balancer server IPv4 address.
- Destination Address IPv6—Enter your load balancer server 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 your load balancer server's security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM communicates 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.

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

Step 8 Select **Save**.

Step 9 Select **Reset** and then select **Reset and Restart** in the pop-up window.
You must reset the SIP trunk to complete your configuration.

Configuring a SIP Trunk for an Application Server

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 **Device** > **Trunk**.

Step 4 Select **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 them at their default settings.

Step 6 Select **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 your load balancer server IPv4 address.
- Destination Address IPv6—Enter your load balancer server IPv6 address if you want 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 using UDP/TCP. Enter 5063 if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- SIP Trunk Security Profile—Select your load balancer server's security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM communicates 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.

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

Step 8 Select **Save**.

Step 9 Select **Reset** and then select **Reset and Restart** in the pop-up window.
You must reset the SIP trunk to complete your 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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Route Group Name—Enter a name for your route group.
- Distribution Algorithm. Select **Circular** in 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 Balancer Server** in the Available Devices list. Then select **Add to Route Group**.

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

Step 6 Select **Save**.

What to Do Next

Create a route list for your route group. Proceed to Configuring a Route List, on page 67.

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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Name—Enter a name for your route list.
- Cisco Unified Communications Manager Group—Select **Default** in drop-down menu.

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

Step 6 Select **Save**.

Step 7 Select **Add Route Group**.
The **Route List Detail Configuration** page appears.

Step 8 Select the previously configured route group from **Route Group** drop-down menu and select **Save**.
The **Route List Configuration** page appears.

Step 9 Select **Save**.

What to Do Next

Configure a route pattern for your route list. Proceed to Configuring a Route Pattern, on page 68.

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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Route Pattern—Enter a name for your route pattern.
- 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 them at their default settings.

Step 6 Select **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 Select **Cisco Unified CM Administration**.

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

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Pattern Usage—Select **IP Address Routing**.
- IPv4 Pattern—Enter the application server IP address.
- SIP Trunk—Select the previously configured SIP trunk for the application server from the drop-down menu.

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

Step 6 Select **Save**.

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 with No High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 50-, 250-, and 800-user systems without high availability.

Information Required

- One load balancer server's IP address
- One application server's IP address
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps in the order presented:

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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60 and Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
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 62.
3	Configure one SIP trunk for your load balancer server.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60.
4	Configure one SIP trunk for your application server.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 67.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 67.
7	Configure *N* route patterns 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, on page 68.
8	Configure one SIP route pattern for your application server.	See Configuring a SIP Route Pattern, on page 69.

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

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

Information Required

- Two load balancer servers' IP addresses
- Two application servers' IP addresses
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps in the order presented:

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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60 and Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
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 62.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60.
4	Configure two SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 67.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 67.
7	Configure *N* route patterns 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, on page 68.
8	Configure two SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 69.

Configuring CUCM on 2000-User Systems with No High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 2000-user systems without high availability.

Information Required

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

Configuration Procedure

Perform the following steps in the order presented:

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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60 and Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
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 62.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60.
4	Configure three SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 67.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 67.
7	Configure *N* route patterns 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, on page 68.
8	Configure three SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 69.

Configuring CUCM on 2000-User Systems with High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 2000-user systems with high availability.

Information Required

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

Configuration Procedure

Perform the following steps in the order presented:

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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60 and Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
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 62.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 60.
4	Configure four SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 61.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 67.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 67.
7	Configure *N* route patterns 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, on page 68.
8	Configure four SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 69.

CHAPTER 7

Downloading and Mass Deploying Applications

Use of this product requires additional applications that must be downloaded to your users' computers. You can download and mass deploy these applications using tools available to you on the Administration site. These applications include the following:

- Cisco WebEx Meetings (Windows and Mac)
- Cisco WebEx Productivity Tools (Windows)
- Cisco WebEx Network Recording Player (Windows and Mac)

To get these applications installed on your users' computers, you can use the Administration site to configure automatic downloads, enable users to download the applications themselves, push applications to your users' computers, or download the installation files and manually install them on your users' computers.

This product can be used on computers whose users have administrator privileges and on those that do not. Automatic downloads, user-enabled download and installation, and pushing applications to your users' computers works when your users have administrator privileges. If your company does not give your users administrator privileges then you must use an alternative approach to install the applications on their computers.

On PCs with administrator privileges:

- Users can download and install the Cisco WebEx Meetings application, Productivity Tools, and Network Recording Player from the end-user download pages. No additional administrator action is required.
- Users are advised to install the Productivity Tools the first time they sign in.
- The Cisco WebEx Meetings application is downloaded on-demand the first time a user joins a meeting and is installed silently on the user's PC.

On PCs without administrator privileges:

- We recommend that you push the Cisco WebEx Meetings application and Productivity Tools to end-user desktops offline before you inform end-users that user accounts have been created for them. This ensures that your users can start and join meetings from their web browsers and Windows desktops the first time they sign in.
- You can acquire the .MSI installers for each from the **Admin** > **Settings** > **Downloads** page. See Configuring Your Download Settings for more information.

- If you decide against pushing the applications to your users, they can still access these applications from the end-user download pages. However, if their PCs prohibit installation of downloaded applications, they will not be able to complete the installation process.
- When users join meetings by using their web browser (the Cisco WebEx Meetings application can still be downloaded on demand) they can join meetings successfully. In addition, the Cisco WebEx Meetings application attempts to perform an installation to speed up the process of starting or joining future meetings. This fails because their PCs do not have administrator privileges.

Downloading Applications from the Administration Site

You can configure your system so that administrators can manually download Cisco WebEx desktop applications to users or you can enable users to perform their own downloads.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Downloads**.

Step 3 Select the **Auto update WebEx Productivity Tools** check box to configure periodic automatic updates. (**Default**: checked.)

Step 4 Select your download method:

- Permit users to download WebEx desktop applications
- Manually push WebEx desktop applications to user's desktop

If you select **Permit users to download WebEx desktop applications**, you can select **Save** to finish your Download configuration. No further action is necessary. If you select **Manually push WebEx desktop applications to user’s desktop**, proceed to the next step.

Use the **Manually push WebEx desktop applications to user’s desktop** option to enable conferencing for users who do not have administrator permissions.

If you select **Manually push WebEx desktop applications to user’s desktop**, the Cisco WebEx Meetings, Productivity Tools, and Network Recording Player sections appear on the page.

Step 5 In the WebEx Meetings section select **Download** and then select **Save** to save the ZIP file to your system. The ZIP file contains installers for both Windows and Mac platforms in all available languages. After you open the ZIP file, select the installer for your platform and language. The installer for Windows systems is an MSI file. The installer for Mac systems is a DMG file.

Step 6 In the Productivity Tools section, select **Download** and then select **Save** to save the ZIP file to your system.

The ZIP file contains installers for all available languages. After you open the ZIP file, select the installer for your language. The installer is an MSI file.

Step 7 In the WebEx Network Recording Player section select **Download** and then select **Save** to save the ZIP file to your system.
The ZIP file contains installers for both Windows and Mac platforms in all available languages. After you open the ZIP file, select the installer for your platform and language. The installer for Windows systems is an MSI file. The installer for Mac systems is a DMG file.

Step 8 Select **Save** to save your download settings.

What to Do Next

Unzip the MSI or DMG files and deploys these clients to end-user desktops with the mass deployment software used by your enterprise. This ensures that the clients are ready for operation when the user attempts to schedule or join meetings or view recordings. For more information on deploying the clients in Windows environments, refer to the following sections:

- Mass Deployment of Cisco WebEx Productivity Tools, on page 80
- Mass Deployment of the Meetings Application, on page 86
- Mass Deployment of the Network Recording Player, on page 89

Each ZIP file contains the application installer for all 13 supported languages. See Contents of the Application ZIP Files, on page 77 for information on determining which installer to use in each ZIP file.

Contents of the Application ZIP Files

This section describes the installer applications contained in each of the ZIP files that you download from the Administration site. The ZIP files contain one installer application per language. This section also provides a key to help you determine the language of each installer. Windows installer applications are provided in 13 languages. Mac installer applications are only provided in English.

Application Language Key

The English application installer file in each ZIP file is titled without a language suffix. For example, the WebEx Meetings client is titled onpremmc.msi (Windows) and webexmc_onprem.dmg (Mac). The application installer file for each of the other 12 languages contains an abbreviation in its title that indicates the language of the application it contains. See the following table for the abbreviation used for each language:

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

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

Note Swedish (SV) and Telephony Service Provider (TSP) files are also included in the application ZIP files. These files are not supported and should be disregarded for the purposes of installing applications for use with Cisco WebEx Meetings Server.

Productivity Tools ZIP File Contents

The Productivity Tools ZIP file contains the following files. Use the key in the table above to determine the language of each file. Note that there is no Mac version of the Productivity Tools.

- ptools.msi
- ptools_B5.msi
- ptools_DE.msi
- ptools_ES.msi
- ptools_FR.msi
- ptools_GB.msi
- ptools_IT.msi
- ptools_JP.msi
- ptools_KO.msi
- ptools_NL.msi
- ptools_PT.msi
- ptools_RU.msi
- ptools_SP.msi
- ptools_SV.msi
- ptools_TSP.msi

WebEx Meetings Client ZIP File Contents

The WebEx Meetings client ZIP file contains the following files. Use the key in the table above to determine the language of each file.

- onpremmc.msi
- onpremmc_B5.msi
- onpremmc_DE.msi
- onpremmc_ES.msi
- onpremmc_FR.msi
- onpremmc_GB.msi
- onpremmc_IT.msi
- onpremmc_JP.msi
- onpremmc_KO.msi
- onpremmc_NL.msi
- onpremmc_PT.msi
- onpremmc_RU.msi
- onpremmc_SP.msi
- onpremmc_SV.msi
- onpremmc_TSP.msi
- webexmc_onprem.dmg

Network Recording Player ZIP File Contents

The Network Recording Player ZIP file contains the following files. Use the key in the table above to determine the language of each file.

- nbr2player_onprem.msi
- nbr2player_onprem_B5.msi
- nbr2player_onprem_DE.msi
- nbr2player_onprem_ES.msi
- nbr2player_onprem_FR.msi
- nbr2player_onprem_GB.msi
- nbr2player_onprem_IT.msi
- nbr2player_onprem_JP.msi
- nbr2player_onprem_KO.msi
- nbr2player_onprem_NL.msi
- nbr2player_onprem_PT.msi
- nbr2player_onprem_RU.msi

- nbr2player_onprem_SP.msi
- nbr2player_onprem_SV.msi
- nbr2player_onprem_TSP.msi
- webexnbrplayer_onprem.dmg

Mass Deployment of Cisco WebEx Productivity Tools

This section is designed to help your organization understand the tasks involved in installing Cisco WebEx Productivity Tools. This section is a comprehensive guide that covers various types of installations, including a single-computer installation and large-scale installations using Microsoft Systems Management Server 2003 (SMS). Cisco WebEx Meetings Server supports integration for Outlook which is contained in the ptools.msi package.

Silent Installation by the Administrator Using the Command Line

Administrators can sign in to a user's computer and install Cisco WebEx Productivity Tools using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer's hard drive and then open the Windows Command Prompt.

Note On Windows 7 and Windows Vista, you must use "run as administrator" to open it.

Step 3 Run the MSI command to install Cisco WebEx Productivity Tools silently.

Example:

```
msiexec.exe /q /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1
```

Parameter Name	Value	Description
OI	1	Enable Outlook Integration
	0 (default)	Disable Outlook Integration

Step 4 Restart the computer.

Silent Uninstallation by the Administrator Using the Command Line

Administrators can sign in to a user's computer and uninstall Cisco WebEx Productivity Tools using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to some location and then open the Windows Command Prompt.

Example:

Note On Windows 7 and Windows Vista, you must use “run as administrator” to open it.

Step 3 Uninstall all components of the MSI package ptools.msi by entering the following command:

Example:

```
msiexec.exe /q /x "ptools.msi"
```

Silent Installation Using SMS

The following limitations apply when you perform a silent installation using SMS:

- SMS per-user mode cannot be supported.
- If the SMS administrator wants to add a feature for WebEx Productivity Tools, the administrator must run the **REMOVE** command first and then run the **ADDSOURCE** command, even though the feature has not been installed before.
- If a user logs on to a computer with remote desktop while their administrator advertises the package, he must restart the computer to make sure WebEx Productivity Tools will work normally.

Advertising Cisco WebEx Productivity Tools Using the SMS Per-System Unattended Program

If you are the SMS administrator, perform the following procedure to advertise the Cisco WebEx Productivity Tools using the SMS per-system unattended program.

Before You Begin

Sign in to the Administration site and manually push the Productivity Tools to the user's desktop.. Refer to the "Configuring Your Download Settings" section of the *Cisco WebEx Meetings Server Administration Guide* for more information.

Procedure

Step 1 Create a package from the definition. See Creating a Package from a Definition, on page 85 for more information.

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

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **Programs**.
b) Right-click the **Per-system unattended** option and then select **Properties** to open the **Per-system unattended Program Properties** dialog box.
c) 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**.)

d) Select the **General** tab.
e) Append an additional parameter to the command line option to specify some options for Cisco WebEx Productivity Tools:

- Append SITEURL=″http://sample.webex.com″ to specify the WebEx Site URL used by your company.
- Append Productivity Tools flags to specify which component is enabled for WebEx Productivity Tools. The 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 "ptools.msi".
- Append Productivity Tools flags and parameters to the command line: msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1.

Note See the parameters table in Silent Installation by the Administrator Using the Command Line, on page 80 for parameter definitions.

Step 3 Now you can advertise the program.

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **Programs**.
b) Right-click **Per-system unattended**.
c) Select **All Tasks** > **Distribute Software**.
d) Select **Next** in the **Distribute Program Wizard**.
e) Select the SMS Server and select **Next**.
f) Select the collection and select **Next**.
g) Enter the advertisement name in the **Name** field and select **Next**.
h) Specify whether the advertisement should apply to subcollections and select **Next**.
i) Specify when the program will be advertised and select **Next**.
j) Specify whether to assign the program and select **Next**.
k) Select **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 will see a message indicating that the assigned program is going to run after the program has been advertised. The assigned program will run silently.

Removing Productivity Tools Components by Using the SMS Per-System Unattended Program

Perform the following procedure to remove Productivity Tools:

Procedure

Step 1 Create a new program and copy all the options from the “per-system unattended program” as described in Advertising Cisco WebEx Productivity Tools Using the SMS Per-System Unattended Program, on page 81, and then update the command line:

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **Programs**.
b) Right-click the blank area and then select **New** > **Program**.
c) Enter the program name and default command line.
d) In 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) Update the command-line on the **General** tab.
f) Append REMOVE to the command line and specify the features that need to be removed.

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

Step 2 Advertise the program to the specified collection of work machines in the domain. See Silent Installation Using SMS, on page 81 for more information.
Cisco WebEx Productivity Tools will be updated on these machines silently.

Adding Productivity Tools Components by Using the SMS Per-System Unattended Program

For an administrator to add a component to the Productivity Tools, he must run REMOVE first and then run ADDSOURCE, even though the component has not been installed before.

Procedure

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

a) Open the SMS administrator console and navigate to **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **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 and 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) Append REMOVE to the command line and specify the features that need to be added.

Example:
If you want to add OI, you must REMOVE them first, even if they are not already installed: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"

Step 2 Advertise the program to the specified collection of work machines in the domain. See Silent Installation Using SMS, on page 81 for more information.

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 navigate to **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **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 that need to be added.

Example:
If you want to add OI, you must REMOVE them first, even if they are not already installed: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI" OI=1

Step 4 Advertise the program to the specified collection of work machines in the domain. See Silent Installation Using SMS, on page 81 for more information.
Cisco WebEx Productivity Tools will be updated on these machines silently.

Uninstalling Productivity Tools Using the SMS Per-System Uninstall Program

The SMS administrator can uninstall Cisco WebEx Productivity Tools using the SMS per-system uninstall program by performing the following procedure.

Procedure

Step 1 Use the SMS Installation package created in Creating a Package from a Definition, on page 85.

Step 2 Advertise the per-system uninstall program to uninstall Cisco WebEx Productivity Tools.
Cisco WebEx Productivity Tools will be uninstalled on these machines silently.

Advertising the Program to Update the New Version of WebEx Productivity Tools

Perform the following procedure to advertise the program to update to the new version of Cisco WebEx Productivity Tools.

Before You Begin

Sign in to the Administration site, select **Settings** > **Downloads** and disable the following settings:

- **Auto update Cisco WebEx Productivity Tools**
- **Permit users to download WebEx desktop applications**

Procedure

Step 1 Create a new SMS installation package using the WebEx Productivity Tools MSI package. See Creating a Package from a Definition, on page 85 for more information.

Step 2 Change the program options for **Per-system unattended** before advertisement. See Adding Productivity Tools Components by Using the SMS Per-System Unattended Program, on page 83 for more information.

Step 3 Advertise the program. See Adding Productivity Tools Components by Using the SMS Per-System Unattended Program, on page 83 for more information.
The old Cisco WebEx Productivity Tools are removed and the new Cisco WebEx Productivity Tools are installed silently.

Creating a Package from a Definition

Perform the following procedure to create a package from a definition.

Procedure

Step 1 Open the SMS Administrator Console and select **Site Database** > **Package**.

Step 2 Right-click **Package**.

Step 3 Select **New** > **Package From Definition**.

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

Step 5 Select **Browse** to locate and select the WebEx Productivity Tools MSI package and then select **Next**.

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

Step 7 Select Source directory location. The directory path is the folder where contains the install package. Then select **Next**.

Step 8 Select **Finish**.

Step 9 Select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Productivity Tools 2.80 English** > **Programs**. There are six default programs available.

Mass Deployment of the Meetings Application

This section is designed to help your organization understand the tasks involved in installing Cisco WebEx Meetings application. This section is a comprehensive guide that covers various types of installations, including a single-computer installation and large-scale installations using Microsoft Systems Management Server 2003 (SMS).

Installing Cisco WebEx Meetings

Before You Begin

The following pre-requisites apply to the Cisco WebEx Meetings installer:

- Installing the Cisco WebEx MSI package requires administrator privileges. The MSI package is installed to the default OS Programs folder which requires administrator privileges to access.
- The Cisco WebEx MSI package is developed for Windows Installer Service 2.0 or higher. If the local machine is configured with an older version, an error message will be displayed informing the user that in order to install this MSI package, a newer version of the Windows Installer Service is required. Upon executing the MSI package, the user will be prompted with a basic MSI interface.

Procedure

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

The installation wizard appears with an introductory message.

Step 2 Select **Next** on the following few dialogue boxes until you reach the installation dialogue box.

Step 3 Select **Install**.

Step 4 Select **Finish** after the installation is complete.

Silent Installation by the Administrator Using the Command Line

You can sign in to a user's computer and install the Cisco WebEx Meetings application using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer's hard drive and then open the Windows Command Prompt.

Note On Windows 7 and Windows Vista, you must use "run as administrator" to open it.

Step 3 Enter the MSI command to install Cisco WebEx Meeting Applications silently.

Example:
Enter msiexec /i onpremmc.msi /qn.

Step 4 Restart the computer.

Silent Uninstallation by the Administrator Using the Command Line

You can sign in to a user's computer and uninstall the Cisco WebEx Meetings application using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to some location and then open the Windows Command Prompt.

Note On Windows 7 and Windows Vista, you must use "run as administrator" to open it.

Step 3 Uninstall all components of the MSI package onpremmc.msi by entering the following command: msiexec/x onpremmc.msi/qn.

Silent Installation Using SMS

Before You Begin

The following limitations apply when you perform a silent installation using SMS:

- SMS per-user mode cannot be supported.
- If a user logs on to a computer with remote desktop while their administrator advertises the package, he must restart the computer to make sure the WebEx Meetings application works normally.

Advertising Cisco WebEx Meetings Application Using the SMS Per-System Unattended Program

If you are the SMS administrator, perform the following procedure to advertise the Cisco WebEx Meetings application using the SMS per-system unattended program.

Before You Begin

Sign in to the Administration site and configure your Download settings to manually push the WebEx desktop applications to the user's desktop. Refer to the "Configuring Your Download Settings" section of the Cisco WebEx Meetings Server Administration Guide for more information.

Procedure

Step 1 Create a package from the definition. See Creating a Package from a Definition, on page 85 for more information.

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

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Meeting Application English** > **Programs**.

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

c) 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 select **Allow users to interact with this program**.

d) Select 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 "onpremmc.msi" /qn

Step 3 Now you can advertise the program.

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Meeting Application English** > **Programs**.
b) Right-click **Per-system unattended**.
c) Select **All Tasks** > **Distribute Software**.
d) Select **Next** in the **Distribute Program Wizard**.
e) Select the SMS Server and select **Next**.
f) Select the collection and select **Next**.
g) Enter the advertisement name in the **Name** field and select **Next**.
h) Specify whether the advertisement should apply to subcollections and select **Next**.
i) Specify when the program will be advertised and select **Next**.
j) Specify whether to assign the program and select **Next**.
k) Select **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 will see a message indicating that the assigned program is going to run after the program has been advertised. The assigned program will run silently.

Uninstalling the Cisco WebEx Meetings Application Using the SMS Per-System Uninstall Program

The SMS administrator can uninstall the Cisco WebEx Meetings application using the SMS per-system uninstall program by performing the following procedure.

Procedure

Step 1 Use the SMS Installation package created in Creating a Package from a Definition, on page 85.

Step 2 Advertise the per-system uninstall program to uninstall the Cisco WebEx Meetings application.
The Cisco WebEx Meetings application will be uninstalled on the specified machines silently.

Mass Deployment of the Network Recording Player

This section is designed to help your organization understand the tasks involved in installing Cisco WebEx Network Recording Player. This section is a comprehensive guide that covers various types of installations, including a single-computer installation and large-scale installations using Microsoft Systems Management Server 2003 (SMS).

Installing Network Recording Player

Before You Begin

The following pre-requisites apply to the Cisco WebEx Network Recording Player installer:

- Installing the Cisco WebEx MSI package requires administrator privileges. The MSI package is installed to the default OS Programs folder which requires administrator privileges to access.
- The Cisco WebEx MSI package is developed for Windows Installer Service 2.0 or higher. If the local machine is configured with an older version, an error message will be displayed informing the user that in order to install this MSI package, a newer version of the Windows Installer Service is required. Upon executing the MSI package, the user will be prompted with a basic MSI interface.

Procedure

Step 1 Launch the installer on the user's computer.
The installation wizard appears with an introductory message.

Step 2 Select **Next** on the following few dialogue boxes until you reach the installation dialogue box.

Step 3 Select **Install**.

Step 4 Select **Finish** after the installation is complete.

Silent Installation by the Administrator Using the Command Line

You can sign in to a user's computer and install the Cisco WebEx Network Recording Player using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to the computer's hard drive and then open the Windows Command Prompt.

Note On Windows 7 and Windows Vista, you must use "run as administrator" to open it.

Step 3 Enter the MSI command to install Cisco WebEx Network Recording Player silently.

Example:
Enter msiexec/i nbr2player_onprem.msi/qn.

Step 4 Restart the computer.

Silent Uninstallation by the Administrator Using the Command Line

You can sign in to a user's computer and uninstall the Cisco WebEx Network Recording Player using silent mode.

Procedure

Step 1 Sign in to the user's computer.

Step 2 Download the MSI package to some location and then open the Windows Command Prompt.

Note On Windows 7 and Windows Vista, you must use "run as administrator" to open it.

Step 3 Uninstall all components of the MSI package onpremmc.msi by entering the following command: msiexec/i nbr2player_onprem.msi/qn.

Silent Installation Using SMS

Before You Begin

The following limitations apply when you perform a silent installation using SMS:

- SMS per-user mode cannot be supported.
- If a user logs on to a computer with remote desktop while their administrator advertises the package, he must restart the computer to make sure the WebEx Meetings application works normally.

Advertising Cisco WebEx Network Recording Player Using the SMS Per-System Unattended Program

If you are the SMS administrator, perform the following procedure to advertise the Cisco WebEx Network Recording Player using the SMS per-system unattended program.

Before You Begin

Sign in to the Administration site and configure your Download settings to manually push the WebEx desktop applications to the user's desktop. Refer to the "Configuring Your Download Settings" section of the Cisco WebEx Meetings Server Administration Guide for more information.

Procedure

Step 1 Create a package from the definition. See Creating a Package from a Definition, on page 85 for more information.

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

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Network Recording Player English** > **Programs**.
b) Right click the **Per-system unattended** option and select **Properties** to open the **Per-system unattended Program Properties** dialog box.
c) 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 select **Allow users to interact with this program**.

d) Select 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 Now you can advertise the program.

a) Open the SMS administrator console and select **Site Database** > **Packages** > **Cisco WebEx LLC Cisco WebEx Network Recording Player English** > **Programs**.
b) Right-click **Per-system unattended**.
c) Select **All Tasks** > **Distribute Software**.
d) Select **Next** in the **Distribute Program Wizard**.
e) Select the SMS Server and select **Next**.
f) Select the collection and select **Next**.
g) Enter the advertisement name in the **Name** field and select **Next**.
h) Specify whether the advertisement should apply to subcollections and select **Next**.
i) Specify when the program will be advertised and select **Next**.
j) Specify whether to assign the program and select **Next**.
k) Select **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 will see a message indicating that the assigned program is going to run after the program has been advertised. The assigned program will run silently.

Uninstalling the Cisco WebEx Network Recording Player Using the SMS Per-System Uninstall Program

The SMS administrator can uninstall the Cisco WebEx Network Recording Player using the SMS per-system uninstall program by performing the following procedure.

Procedure

Step 1 Use the SMS Installation package created in Creating a Package from a Definition, on page 85.

Step 2 Advertise the per-system uninstall program to uninstall the Cisco WebEx Network Recording Player.
The Cisco WebEx Network Recording Player will be uninstalled on the specified machines silently.

CHAPTER 8

License Management

About Licenses

This section describes the licensing method used for this product.

This product features user-based licensing which requires that you purchase a license for each user that intends to host meetings. We count licenses as follows:

- If a user hosts at least one meeting per 30-day window, then that user consumes one license. If this user hosts additional meetings in this same 30-day window, the user still only consumes one license, unless this user hosts simultaneous meetings.
- If a user hosts simultaneous meetings (at the same date and time), then the system counts an additional license for each simultaneous meeting hosted by this user in the 30-day window.
- If a user hosts no meetings in the 30-day window, then this user consumes no licenses.

Note There is currently a known issue that causes no licenses to be consumed if a user attends only the teleconference portion of a meeting (and not the web portion). In future versions of this product, attending either the teleconference or web portion of a meeting (or both) will result in a license use.

Note The system counts license use for each user every 30 days, as shown in the following table.

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User A schedules a meeting but does not host it.	January 1	9:00 a.m.	No	0

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User B hosts one meeting.	January 2	9:00 a.m.	No	1
User C hosts two meetings on different dates and times.	January 3 January 4	9:00 a.m. 10:00 a.m.	No	1
User D hosts two meetings on the same date and time.	January 6 January 6	9:00 a.m. 9:00 a.m.	Yes (2)	2
User E hosts two meetings on the same date and time, and another two simultaneous meetings on a different date and time within the month.	January 6 January 6 January 10 January 10	9:00 a.m. 9:00 a.m. 4 p.m. 4 p.m.	Yes (2)	2
User F hosts two meetings on the same date and time neither of which he attends, although the meetings occur.	January 7 January 7	9:00 a.m. 9:00 a.m.	Yes (2)	2
User G hosts a meeting and passes host rights to another participant during the meeting. The user then hosts a 2nd meeting that runs simultaneously with the 1st meeting.	January 8 January 8	9:00 a.m. 9:00 a.m.	Yes (2)	2
User H hosts a meeting but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 9	9:00 a.m.	No	0

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User J hosts two meetings on the same date and time but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 10 January 10	9:00 a.m. 9:00 a.m.	No	0
User K hosts a meeting and passes host rights to another participant during the meeting. The user then hosts a 2nd meeting that runs simultaneously with the 1st meeting but all of the 2nd meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 11 January 11	10:00 a.m. 10:00 a.m.	No	1

180-Day Free-Trial Period

After you sign in to this product for the first time and complete the first-time-experience wizard, your 180-day free-trial begins. During the free trial, administrators can configure the system and your users can schedule, host, and attend meetings. A banner appears at the top of the Administration site indicating how many days remain in your free trial. Thirty days before your free trial ends, you receive an email that informs you that you must purchase and install licenses or your system will be disabled.

At the end of your free trial, your system is disabled. You can sign in to your system but you cannot use any other features until you add licenses. Refer to the *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

Obtaining Licenses

Contact your Cisco sales representative to order licenses for your system. When you contact your sales representative, you will need to specify how many licenses you want. You will need one license for each employee in your organization who will be hosting meetings.

There are several ways you can determine how many licenses you will need. You can use your dashboard to view usage, resource history, and meeting trends to determine how many users are hosting and attending meetings on your system. After you have been using the product for a few months, you can use your monthly summary reports and customized details reports to help you determine how many licenses you need. Your monthly summary reports display statistics on service adoption and user license usage. Service adoption statistics show you the rate at which new users are adopting your system by displaying the rate of adoption for the previous three months and predicting the growth rate over the next three months. User license statistics display license usage over the previous three months and expected growth over the next three months.

After you purchase licenses from your Cisco sales representative, he will send you an email that contains your Product Authorization Key (PAK). Use the licenses tool at the Administration site to enter your PAK and register your licenses. Refer to the *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

License Overages

Once you have purchased and configured licenses on your system, you must make sure you have enough licenses to accommodate all hosts on your system. Your system checks every 30 days if there are enough licenses for each host. If the number of hosts on your system exceeds the number of licenses, an email is sent to the administrator notifying him of the overage. You are given a six-month grace period to increase the number of licenses on your system so that it meets or exceeds the number of hosts. If you do not purchase enough licenses to meet usage before the end of the six-month period, your system will be disabled. The email message informs the administrator of the date when this will occur.

The system checks and adjusts the license numbers displayed on the administration site. The audit manager runs once per day (at 2:00 a.m.) to adjust the overage number as necessary. At the end of each 30-day period, the system checks license usage. If the number of hosts has dropped below the number of licenses, the overage condition ends. If the number of hosts still exceeds the number of licenses, a new email is sent to your administrator each month that notifies him that the overage condition still exists and the date when the system will be disabled.

If you still have an overage condition after six months, your system is disabled and the administrator receives an email notifying him what has occurred. After your system is disabled your users will be unable to schedule, host, or attend meetings on your system. The Administration site will function normally so an administrator can sign in and add licenses. Once an administrator has added licenses to the system, users will regain the ability to schedule, host, and attend meetings.

Temporary Licenses

If you have temporary licenses configured on your system, your temporary license status appears on a banner on each page of the Administration site. The banner informs you of how many temporary licenses you have configured and when those temporary licenses expire. When temporary licenses expire your system returns to its previous license status.

Out-of-Date Licenses

If you upgrade your system, you must also update your licenses. Once you have upgraded your system, an email is sent to your administrator notifying him that he has been given a six-month grace period to update the licenses. If you do not update your licenses before the end of the six-month period, your system will be disabled. The email message informs the administrator of the date when this will occur.

The system checks and adjusts the license numbers displayed on the administration site. The audit manager runs once per day (at 2:00 a.m.) to adjust the out-of-date licenses number as necessary. At the end of each 30-day period, the system checks to see if the licenses have been updated from the previous period. If the licenses have been updated, the out-of-date license condition ends. If the licenses have not been updated yet, a new email is sent to your administrator each month that notifies him that the out-of-date license condition still exists and the date when the system will be disabled.

If you still have an out-of-date license condition after six months, your system is disabled and the administrator receives an email notifying him what has occurred. After your system is disabled your users will be unable to schedule, host, or attend meetings on your system. The Administration site will function normally so an administrator can sign in and update the licenses. Once an administrator has updated the licenses, users will regain the ability to schedule, host, and attend meetings.

Enterprise License Manager (ELM) Connection Lost

When you purchase licenses, you use an embedded ELM tool to enter your PAK and register your licenses. ELM performs synchronization every 12 hours to update the license status and last compliance time. If two days pass with no connection to ELM, an email is sent to your administrator to inform him that ELM is unable to synchronize with your system. You are given a six-month grace period to reconnect to ELM. If your system does not reconnect with ELM before the end of the six-month period, your system will be disabled. The email message informs the administrator of the date when this will occur.

A new email is sent to your administrator at the end of each month that the system is unable to connect with ELM informing him of the date when the system will be disabled. If your system reconnects with ELM before the six-month grace period passes, this condition ends.

If your system is still unable to connect to ELM after six months, your system is disabled and the administrator receives an email notifying him what has occurred. After your system is disabled your users will be unable to schedule, host, or attend meetings on your system. The Administration site will function normally so an administrator can sign in to the system but the system must reconnect with ELM to end this condition and restore the ability to schedule, host, and attend meetings.

CHAPTER 9

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 web sites 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 web sites 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 usually 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 Active Directory 2010)
- 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 user'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 self-selected passwords specific to the Meetings Server system. Users select their passwords upon activating their Meetings Server accounts. While this approach works well for most small- and mid-sized organizations, larger organizations prefer user authentication using corporate credentials—that is, Active Directory—for enhanced security. You can accomplish this goal by using SAML 2.0 SSO.

  Note One added security benefit of SSO is that the corporate password is never actually sent to or stored in Cisco WebEx Meetings Server after the user authenticates successfully.

- 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

  You can achieve automation for these events by configuring **Auto Account Creation** and **Auto Account Update** in the SSO section of the Cisco WebEx Meetings Server Administration site. 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 successfully, thereby eliminating the need to create users manually using Cisco WebEx Administration. 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 SAML 2.0 IdP user 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 fairly complicated.

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 implies setting up 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—then it is critical to ensure that the SSO authentication website is also accessible from the Internet. This usually implies deploying the SAML 2.0 IdP in your DMZ. Without this extra step, users will 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 using both of these methods:
   - Select **Settings** > **Security** > **Federated SSO** on your Cisco WebEx Meetings Server Administration site.
   - Follow the instructions in your SAML 2.0 IdP documentation. Note that these instructions vary from vendor to vendor and might even change from version to version of the SAML 2.0 IdP. This is another reason to ensure 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 SAML 2.0 IdPs because those instructions are intended for cloud-based Cisco WebEx meeting services and therefore do not work optimally with Cisco WebEx Meetings Server.

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. This has the following important implications for SAML 2.0 single sign-on (SSO):

- It is mandatory for the SAML Assertion to carry the email address in the NameID field. Without this step, user authentication and account creation fail because Cisco WebEx Meetings Server does not permit the creation of user accounts without an associated email address.
- 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 WebEx Meetings Server uses a complete email address to create user accounts, you cannot remove the email domain from the UPN.

In practice, you can initially deploy Cisco WebEx Meetings Server without SAML 2.0 SSO and turn on SSO later. 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
You have not turned on SSO. User accounts were created in the system.	Users sign in using their email addresses and self-selected 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
Next you turn on SSO. Users with existing accounts sign in to their WebEx site, WebEx Productivity Tools, or the Cisco WebEx Meetings app on their mobile devices.	Users are redirected to the SAML 2.0 IdP authentication website and asked to sign in using their corporate credentials, instead of email addresses and self-selected passwords. The users sign in successfully because they are recognized by the SAML 2.0 IdP as valid users. If they are not valid users, they will be informed by the SAML 2.0 IdP that they cannot use WebEx Meetings Server or that they are invalid users.	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
SSO is turned on. Users do not have existing accounts in the system.	Same as the previous scenario.	User accounts in Cisco WebEx Meetings Server are created "on-demand" after users sign in. Prerequisite: The SAML Assertion contains a valid email address in the NameID field.	Users do not have existing accounts in the system. They can sign in but will not be able to use Cisco WebEx Meetings Server. The easiest way to remedy this situation is to do one of the following: • Leave AAC on. • Before users sign in, manually create user accounts using "CSV File Import" or "Create user" from the Cisco WebEx Administration site.	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is turned on. Users previously signed in using SSO and are now signing in again.	Same as the second scenario.	N/A	N/A	Existing user accounts are automatically updated with any changes to the user credentials (usually first name or last name) as long as the NameID remains unchanged.	N/A
Subsequently you turn off SSO. This is an uncommon scenario because customers tend to leave SSO on after turning it on. Users previously signed in using SSO and are now signing in again.	If users enter their corporate credentials, they cannot sign in because WebEx Meetings Server expects them to enter their email addresses and self-selected passwords. In this situation, educate the users about resetting the self-selected passwords in their WebEx accounts and allow them enough time to act before you turn off SSO. After resetting their passwords, users can sign in using their email addresses and self-selected 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 the Cisco WebEx Administration site.		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.

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	Scenario A: Same results as the previous scenario Scenario B: In contrast to the behavior on a WebEx site, when the user signs in to the Cisco WebEx Administration site, he or she is always prompted to enter the email address and self-selected password. In other words, SSO has no effect when you sign in to the Cisco WebEx Administration site. This is a security measure built into the product because of the need to ensure that systems administrators can always sign in to the Cisco WebEx Administration site. If the Cisco WebEx Administration site also supports SSO, then malfunctions in				

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	the SAML 2.0 IdP or a loss of network connectivity between Cisco WebEx Meetings Server and the SAML 2.0 IdP might result in a situation in which systems administrators can no longer sign in and manage the product. This is the reason why SSO is not supported for the Cisco WebEx Administration site.				

CHAPTER 10

Network Management

Network Management Requirements

In addition to the monitoring features available on the dashboard, Cisco WebEx Meetings Server supports Cisco Unified Operations Manager (CUOM) for system operation monitoring, including load monitoring, health checks, and fault reporting.

Note Cisco WebEx Meetings Server does not support CUOM configuration and management features.

Each virtual machine on your system runs an SNMP agent. Each virtual machine is therefore visible to CUOM. The SNMP agent supports the SNMPv3 protocol, including the authentication and encryption mechanisms in SNMPv3.

Each SNMP agent currently supports the following standard MIBs:

- MIB-II (RFC-1213)
- SYSAPPL MIB (RFC-2287)
- SNMPv2-SMI
- SNMPv2-CONF
- SNMPv2-TC
- INET-ADDRESS-MIB
- Host Resources MIB (RFC-2780)
- SNMP-FRAMEWORK-MIB
- Cisco Discovery Protocol (CDP) MIB
- CISCO-SMI

Note You can set the CUOM destination from your Administration site. For more information, refer to the "Configuring Your System" section of the Administration Guide.

In addition, each virtual machine supports one or more application-specific MIBs.

Following is a list of the supported private MIBs:

- CISCO-WBX-COMMON-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 796—This common MIB is used for all registered server components running on each virtual machine.
- CISCO-WBX-DATA-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 795—This MIB is for web-sharing servers.
- CISCO-WBX-MEDIA-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 797—This MIB is for video and Voice Connection Using Computer application servers.
- CISCO-WBX-SSLGW-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 794—This MIB is for the SSL gateway.
- CISCO-WBX-TELEPHONY-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 799—This MIB is for the telephony server that bridges the external voice telephony services with the Cisco WebEx application.
- CISCO-WBX-TELSVR-MIB
    - CANA (Cisco Assigned Numbers Authority) OID 788—This MIB is for the network-based recording server.

Among the private MIBs listed above, the CISCO-WBX-COMMON-MIB provides all the necessary information that we support for each virtual machine in terms of the following:

- System resource utilization
- Common server information
- Process manager information
- Daemon process attributes
- Notification resources

Following are examples of some MIB Objects from CISCO-WBX-COMMON-MIB:

- Common server information
    - cwCommServIndex
    - cwCommServType

  - cwCommServID
  - cwCommServIPAddrType
  - cwCommServIPAddr
  - cwCommServCmdLine
  - cwCommServStatus
  - cwCommServStartTime
  - cwCommServErrorMsg
  - cwCommServVersion
  - cwCommServAction
  - cwCommServMEMUsed
  - cwCommServCPUUsage

- Supported notification events
  - cwCommSystemResourceUsageNormalEvent
  - cwCommSystemResourceUsageMinorEvent
  - cwCommSystemResourceUsageMajorEvent
  - cwCommCPUUsageNormalEvent
  - cwCommCPUUsageMinorEvent
  - cwCommCPUUsageMajorEvent
  - cwCommNodeMgrUpEvent
  - cwCommNodeMgrDownEvent
  - cwCommWBXDScriptStartErrorEvent
  - cwCommDaemonUpStatusEvent
  - cwCommDaemonDownStatusEvent
  - cwCommServMEMUsageNormalEvent
  - cwCommServMEMUsageExceededEvent
  - cwCommServCPUUsageNormalEvent
  - cwCommServCPUUsageExceededEvent

CHAPTER 11

Meeting Recordings

Meeting recordings consume space on your storage server. This section describes storage server thresholds, alarms, meeting recording consumption of storage server space, and the process of purging old recordings.

About Meeting Recordings

You can configure a storage server of any capacity. The number of recordings you can store is dependent upon the amount of storage space you configure. Periodically, you should archive any recordings to other media if your organization requires that you keep recordings for more than six months.

Your system performs two tasks to maintain recording space:

- After six months it deletes recordings set for deletion by your users.
- It deletes recordings set for deletion before six months if your recordings exceed a certain threshold during a three-month period.

When a user deletes a recording, it is no longer available from the user interface but it is maintained in storage for six months. Therefore, you can still access the storage server to copy, back up, or use the recording files for six months after they have set for deletion by the user.

Each meeting recording is approximately 50–100 MB and with 1 TB of space allocated for recording storage, your system should have room for six months of recordings with standard usage. However, if the recordings on your system consume over 75 percent of the allocated space after three months, the system automatically deletes the first 10 files that have been set for deletion by the user.

For example, if a user deletes two files today, and then five files tomorrow, and then nine files the day after tomorrow, and then storage usage surpasses the 75% limit after 3 months, the system deletes the first two files today, the next five files tomorrow, and then the first three files deleted the day after tomorrow.