



## **Cisco WebEx Meetings Server Planning Guide Release 1.5**

**First Published:** August 14, 2013

**Last Modified:** March 20, 2014

### **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 NON-INFRINGEMENT 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.

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

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)

© 2013-2014 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### **Introduction and Datacenter Topology For Your System 1**

- Introducing Cisco WebEx Meetings Server 1
- Information for Cisco Unified MeetingPlace Customers 2
- General Concepts For Your System Deployment 3
- Deploying Your System in a Single Datacenter 4
- Using VMware vSphere With Your System 5
- Advantages of Deploying Your System on VMware vSphere 5
- Installing VMware vSphere ESXi and Configuring Storage 7
- Joining Meetings 8

---

### CHAPTER 2

#### **Networking Topology For Your System 9**

- Virtual Machine Layout in Your Network 9
- Different Types of Network Topology For Your System 10
- Internal Internet Reverse Proxy Network Topology 11
- Non-Split-Horizon Network Topology 12
- All Internal Network Topology 13
- Split-Horizon Network Topology 14
- Redundant Network in HA Deployments 15
- Network Considerations for the Internet Reverse Proxy 16
- Network Bandwidth Requirements 17
- NIC Teaming for Bandwidth Aggregation 21

---

### CHAPTER 3

#### **Choosing the System Size 23**

- Users 23
- Deployment Sizes For Your System 23
- Requirements for vCenter Co-residency 24
- Virtual Machines In Your System 24
- 50 User System 25

250 User System	26
800 User System	26
2000 User System	27

---

**CHAPTER 4****Networking Changes Required For Your Deployment 29**

Networking Checklist For Your System	30
Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines	31
Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines	33
Networking Checklist for an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS	36
Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS	39
Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS	42
Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS	44
Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access	47
Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access	49
WebEx Site and WebEx Administration URLs	51
Port Access When All the Virtual Machines Are in the Internal Network	53
Port Access With an Internet Reverse Proxy in the DMZ Network	53
VMware vCenter Ports	60
Cisco WebEx Meeting Center Ports	61
Using NAT With Your System	61
Forward Proxies	63

---

**CHAPTER 5****System Capacity Quick Reference Tables 65**

Maximum System Capacity and Scalability for Each System Size	65
--------------------------------------------------------------	----

---

**CHAPTER 6****Best Practices 67**

Cisco WebEx Meetings Server Best Practices	67
--------------------------------------------	----

---

**CHAPTER 7****Configuring Cisco Unified Communications Manager (CUCM) 69**

- Cisco Unified Communications Manager (CUCM) Configuration Summary 69
- Configuration Checklist 70
- Configuring CUCM for High-Availability and Non-High-Availability Systems 71
  - Configuring CUCM on 50-, 250-, and 800-User Systems with No High Availability 71
  - Configuring CUCM on 50-, 250-, and 800-User Systems with High Availability 72
  - Configuring CUCM on 2000-User Systems with No High Availability 73
  - Configuring CUCM on 2000-User Systems with High Availability 74
- Configuring a SIP Trunk Security Profile 75
  - Configuring a SIP Trunk Security Profile for a Load Balance Point 75
  - Configuring a SIP Trunk Security Profile for an Application Point 76
- Configuring a SIP Profile 77
  - Configuring a Standard SIP Profile 77
  - Configuring a TLS SIP Profile 78
  - Configuring an IPv6 SIP Profile 78
- Certificate Management 79
  - Uploading Cisco WebEx Meetings Server Certificates 79
  - Installing a Third-Party CUCM Certificate 80
  - Downloading CUCM Certificates 81
- Configuring a SIP Trunk 81
  - Configuring a SIP Trunk on a Load Balance Point 81
  - Configuring a SIP Trunk for an Application Point 83
- Configuring a Route Group 84
- Configuring a Route List 85
- Configuring a Route Pattern 85
- Configuring a SIP Route Pattern 86
- CUCM Feature Compatibility and Support 86

---

**CHAPTER 8****Downloading and Mass Deploying Applications 91**

- Downloading Applications from the Administration Site 92
- Contents of the Application ZIP Files 93
- Mass Deployment of Cisco WebEx Productivity Tools 95
  - Silent Installation by the Administrator Using the Command Line 96
  - Silent Uninstallation by the Administrator Using the Command Line 96

Silent Installation Using SMS	97
Advertising Cisco WebEx Productivity Tools Using the SMS Per-System Unattended Program	97
Removing Productivity Tools Components by Using the SMS Per-System Unattended Program	98
Adding Productivity Tools Components by Using the SMS Per-System Unattended Program	99
Uninstalling Productivity Tools Using the SMS Per-System Uninstall Program	100
Advertising the Program to Update the New Version of WebEx Productivity Tools	101
Creating a Package from a Definition	101
Mass Deployment of the Meetings Application	102
Installing Cisco WebEx Meetings	102
Uninstall Cisco WebEx Meetings Locally	103
Silent Installation by the Administrator Using the Command Line	103
Silent Uninstallation by the Administrator Using the Command Line	104
Silent Installation Using SMS	104
Advertising Cisco WebEx Meetings Application Using the SMS Per-System Unattended Program	104
Uninstalling the Cisco WebEx Meetings Application Using the SMS Per-System Uninstall Program	106
Mass Deployment of the Network Recording Player	106
Installing Network Recording Player	106
Silent Installation by the Administrator Using the Command Line	107
Silent Uninstallation by the Administrator Using the Command Line	107
Silent Installation Using SMS	107
Advertising Cisco WebEx Network Recording Player Using the SMS Per-System Unattended Program	108
Uninstalling the Cisco WebEx Network Recording Player Using the SMS Per-System Uninstall Program	109
Reconfiguring Your Settings After Performing an Update	109

---

**CHAPTER 9**
**License Management 111**

About Licenses 111

---

**CHAPTER 10**
**SAML SSO Configuration 119**

Overview of Single Sign-On	119
Benefits of Single Sign-On	120
Overview of Setting Up SAML 2.0 Single Sign-On	121
SAML SSO for End-User and Administration Sign In	121
SAML 2.0 Single Sign-On Differences Between Cloud-Based WebEx Meeting Services and WebEx Meetings Server	122
SAML Assertion Attributes	128

---

**CHAPTER 11****Meeting Recordings 145**

About Meeting Recordings	145
--------------------------	-----

---

**CHAPTER 12****SNMP MIBs and Traps Supported 147**

Supported SNMP MIBs	147
Supported SNMP Traps	151







# 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, page 1](#)
- [Information for Cisco Unified MeetingPlace Customers, page 2](#)
- [General Concepts For Your System Deployment, page 3](#)
- [Deploying Your System in a Single Datacenter, page 4](#)
- [Using VMware vSphere With Your System, page 5](#)
- [Advantages of Deploying Your System on VMware vSphere, page 5](#)
- [Installing VMware vSphere ESXi and Configuring Storage, page 7](#)
- [Joining Meetings, page 8](#)

## 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 vSphere. (For specific requirements, see the *Cisco WebEx Meetings Server System Requirements*.) 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. For supported devices, see the *Cisco WebEx Meetings Server System Requirements*.

### Important Considerations For Your System

Note the following:

- Forward proxies—not recommended, though you may use forward proxies with restrictions. For complete details, refer to the *Cisco WebEx Meetings Server Troubleshooting Guide*.
- Reverse proxies—only the Internet Reverse Proxy 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](#).
- 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](#).



---

**Caution**

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

---

### New and Changed Features for Cisco WebEx Meetings Server

For a list of new and changed features, see the section titled "New and Changed Features for Cisco WebEx Meetings Server" in the *Release Notes for Cisco WebEx Meetings Server* at [Release Notes](#).

## Information for Cisco Unified MeetingPlace Customers



---

**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.

# 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	<ul style="list-style-type: none"> <li>• IP address for the Administration site URL</li> <li>• IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).</li> </ul>

# 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 50 user system comprises an Admin virtual machine and an Internet Reverse Proxy (for public access). If you add a HA system, the combined 50 user system comprises two Admin virtual machines and two Internet Reverse Proxy virtual machines.
- A primary 250 or 800 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 or 800 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.



---

**Important**

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

---



---

**Note**

For a description of each type of virtual machine, see [Virtual Machines In Your System](#), on page 24.

---



In an HA system, the public VIP address and private VIP address are shared with the primary system. (The public VIP address and the private VIP address are different and are not 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. (For Cisco WebEx Meetings Server, 4 ms of network latency is acceptable between the internal virtual machines. For more details, see [Virtual Machine Layout in Your Network](#), on page 9.)

# Using VMware vSphere With Your System

## VMware vSphere

	<b>Important</b> This product only installs on a VMware vSphere virtualization platform. (For complete details on VMware requirements, see the <i>Cisco WebEx Meetings Server System Requirements</i> ).
	<b>Restriction</b> 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, 5.0 Update 1, or 5.1 for use as the hypervisor platform for Cisco WebEx Meetings Server by completing one of the following:
  - Buy vSphere 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 directly from VMware, through enterprise agreements you have directly with VMware.

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

**Note**


---

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

---

- Cisco WebEx Meetings Server requires customers to run VMware ESXi or the corresponding VMware ESXi installable Cisco ISO Image. Both these editions contain the necessary drivers required to support the Cisco UCS Servers that are required by Cisco WebEx Meetings Server. For more information, see [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/release/notes/OL\\_26617.pdf](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 source ESXi host.

---

The following VMware features are not supported with Cisco WebEx Meetings Server:

- 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, either commit the snapshots or remove them as soon as possible. Keeping a snapshot for any period of time will result in severe performance degradation.
- For SAN environments, deploy disk images to a SAN with high IOPS numbers.

For an 800 user system, the average IOPS for an OVA deployment is 506 (max IOPS is 855) for the Admin virtual machine and 475 (max IOPS is 652) for a Media virtual machine. Once these virtual machines are created and powered on, then you can enter the case-sensitive URL and continue the system

deployment in a web browser. The average IOPS for a primary system is 108 (max IOPS is 1558) and 163 (max IOPS is 1736) for a secondary system.

- 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.

For more information on network bandwidth, see [Network Bandwidth Requirements](#), on page 17.

### vCenter Server Requirements

In addition to vSphere, vCenter Server is also required.

- To deploy this virtual appliance, you must also use vCenter to deploy and manage the virtual machines in your system. This product will not work without vCenter Server.
- Cisco recommends backups and snapshots of the system ahead of important system-impacting operations. Creating backups permits you to roll back the changes in case the update does not meet your expectation. You may automate backups and snapshots using vCenter.
- Although the vSphere Standard Edition is required for a 50 or 250 user system, you may consider the alternative of purchasing the vSphere Essentials Plus kit. However, the vSphere Essentials Plus kit is useful primarily for budget-conscious customers deploying the 50 user system and does not provide several advanced capabilities that typical enterprise customers require. Consult with your VMware representative for the most cost effective way to meet the system requirements.

### vSphere Edition For the 800 and 2000 User Systems

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

For complete information on vCPU requirements, see the *Cisco WebEx Meetings Server System Requirements*.

- At minimum, you must purchase the vSphere 5.0 Enterprise Plus edition or the vSphere 5.1 Enterprise edition, as the lower-end vSphere editions do not support the number of required vCPUs.

## Installing VMware vSphere ESXi and Configuring Storage

Cisco WebEx Meetings Server is a software-based solution. It is not a combination hardware/software package. You have choices on how to purchase and provision your hardware platforms as long as the hardware meets or exceeds CPU, memory, and storage requirements.

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

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

However, since Cisco WebEx Meetings Server is deployed on Cisco UCS Servers, refer to the *Cisco UCS Servers RAID Guide* at [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/c/sw/raid/configuration/guide/RAID\\_GUIDE.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.html).

- To install VMware vSphere ESXi on a UCS B-Series Back Server, see [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/os-install-guides/vmware/b\\_B-Series\\_VMware\\_Install.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.html).
- To install VMware vSphere ESXi on a UCS C-Series Rack Server, see [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/os-install-guides/vmware/b\\_C-Series\\_VMware\\_Install.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.html).

## Joining Meetings

End user experience with Cisco WebEx Meetings Server is of a web site that users access to schedule and join meetings. This web site includes real-time conferencing elements that facilitate online meetings. Users can join meetings through a browser or through a client on their desktops.

For complete details on the end user experience, sign in to the WebEx site and select **Help**.

### Windows Users

The following assumes that a user has Windows Administrator privileges on their PC sufficient to allow them to join WebEx meetings. If this is not true, system administrators can push the WebEx Meetings application client to a user by using desktop management software such as IBM Tivoli. See [Downloading and Mass Deploying Applications](#).

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

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

### Mac Users

- If Java is enabled (Java is turned off by default in Mac OS X Lion (version 10.7) and OS X Mountain Lion (version 10.8), 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.





## Networking Topology For Your System

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.



### Important

If you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine. You must deploy the Internet Reverse Proxy regardless of how the mobile user attends a meeting.

When using a cellular data network, mobile users join the meeting through the Internet to the Internet Reverse Proxy. When using a local Wi-Fi connection, mobile users join the meeting through the Internet Reverse Proxy (non-split-horizon network topology) or directly to the internal virtual machines (split-horizon network topology).

- [Virtual Machine Layout in Your Network, page 9](#)
- [Different Types of Network Topology For Your System, page 10](#)
- [Internal Internet Reverse Proxy Network Topology, page 11](#)
- [Non-Split-Horizon Network Topology, page 12](#)
- [All Internal Network Topology, page 13](#)
- [Split-Horizon Network Topology, page 14](#)
- [Redundant Network in HA Deployments, page 15](#)
- [Network Considerations for the Internet Reverse Proxy, page 16](#)
- [Network Bandwidth Requirements, page 17](#)
- [NIC Teaming for Bandwidth Aggregation, page 21](#)

## Virtual Machine Layout in Your Network

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.

**Important**

If you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine. You must deploy the Internet Reverse Proxy regardless of how the mobile user attends a meeting.

For more information about using an Internet Reverse Proxy, see [Network Considerations for the Internet Reverse Proxy](#), on page 16.

**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 4 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. However, when provisioning highly available systems you should deploy two Ethernet switches to ensure network level redundancy.

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 specific bandwidth and network latency requirements as described in [Network Bandwidth Requirements](#), on page 17. 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 15.

## 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.



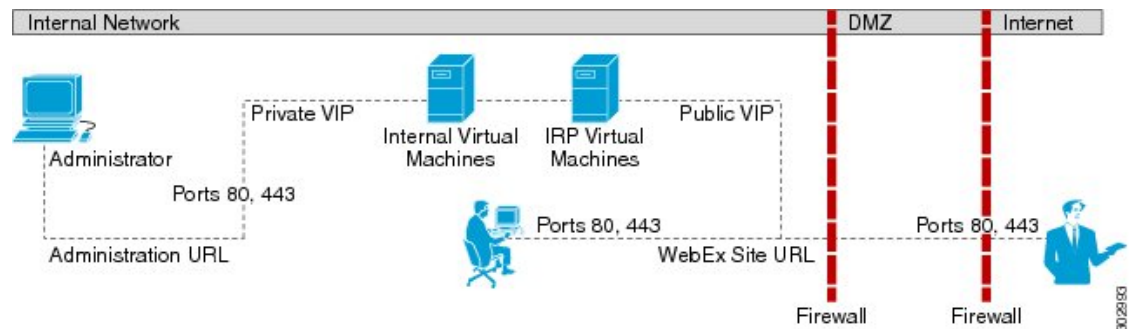
**Note** This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.



**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 53.

### Advantages of an All Internal Internet Reverse Proxy Network Topology

- 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.

For more information about Internet Reverse Proxies, see [Network Considerations for the Internet Reverse Proxy](#), on page 16.

## 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.



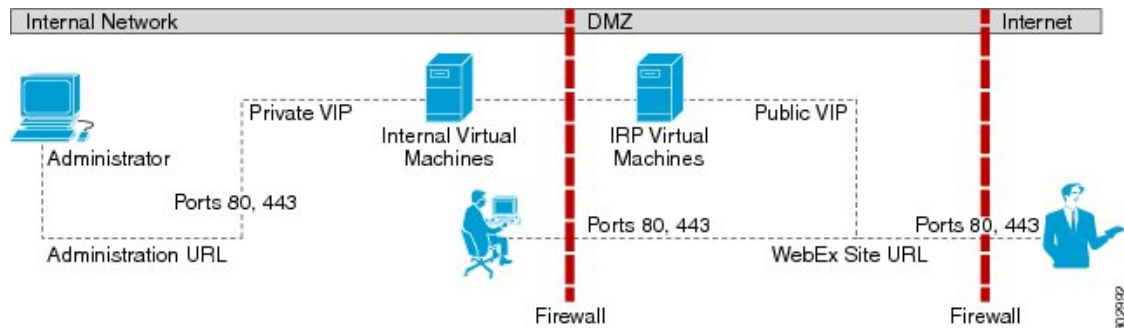
#### Note

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 53.

### Advantages of a Non-Split-Horizon Network Topology

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

### Disadvantages of a Non-Split-Horizon Topology

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



#### Note

Refer to [Network Bandwidth Requirements, on page 17](#) for details about NIC speed requirements for non-split-horizon DNS deployments.

## All Internal Network Topology

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

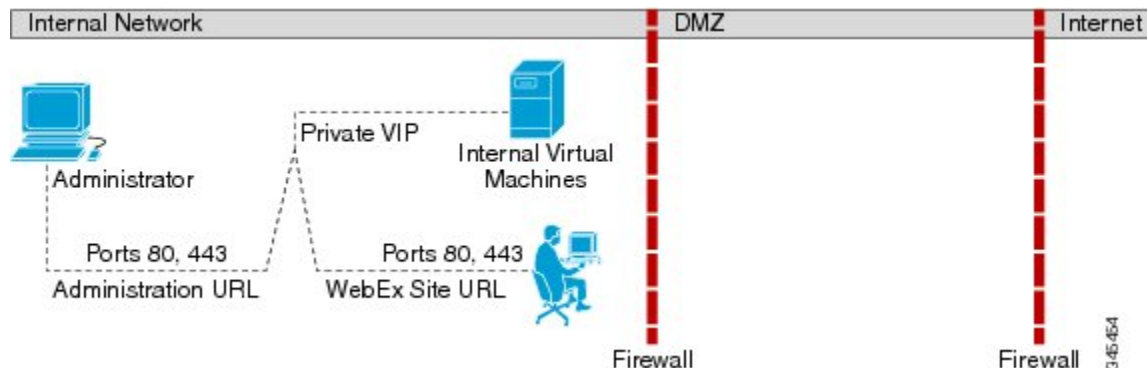


#### Note

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

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**

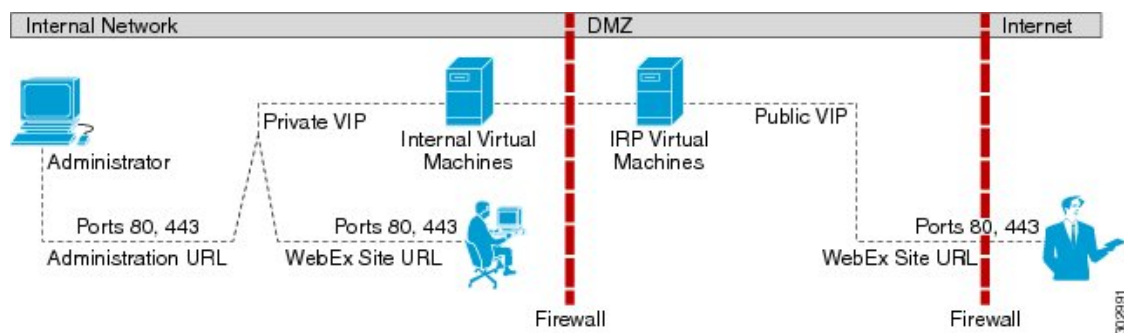
This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

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

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the WebEx site URL using the private 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 53.

### 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.

Refer to [Network Bandwidth Requirements](#), on page 17 for details about NIC speed requirements for split-horizon DNS deployments.

## Redundant Network in HA Deployments

Cisco WebEx Meetings Server does not implement High Availability (HA) in the traditional sense where you deploy a primary system, then deploy a second HA system, and then join both into a HA pair. Instead, Cisco WebEx Meetings Server combines the primary system and the HA system into one single system. For details on each system size, see [Deploying Your System in a Single Datacenter](#), on page 4.

- 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 support 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.

## Network Considerations for the Internet Reverse Proxy

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



### Restriction

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

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

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

### Latency Between Internal Virtual Machines and the Internet Reverse Proxy

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



### Note

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



### Note

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

### Network Traffic Isolation

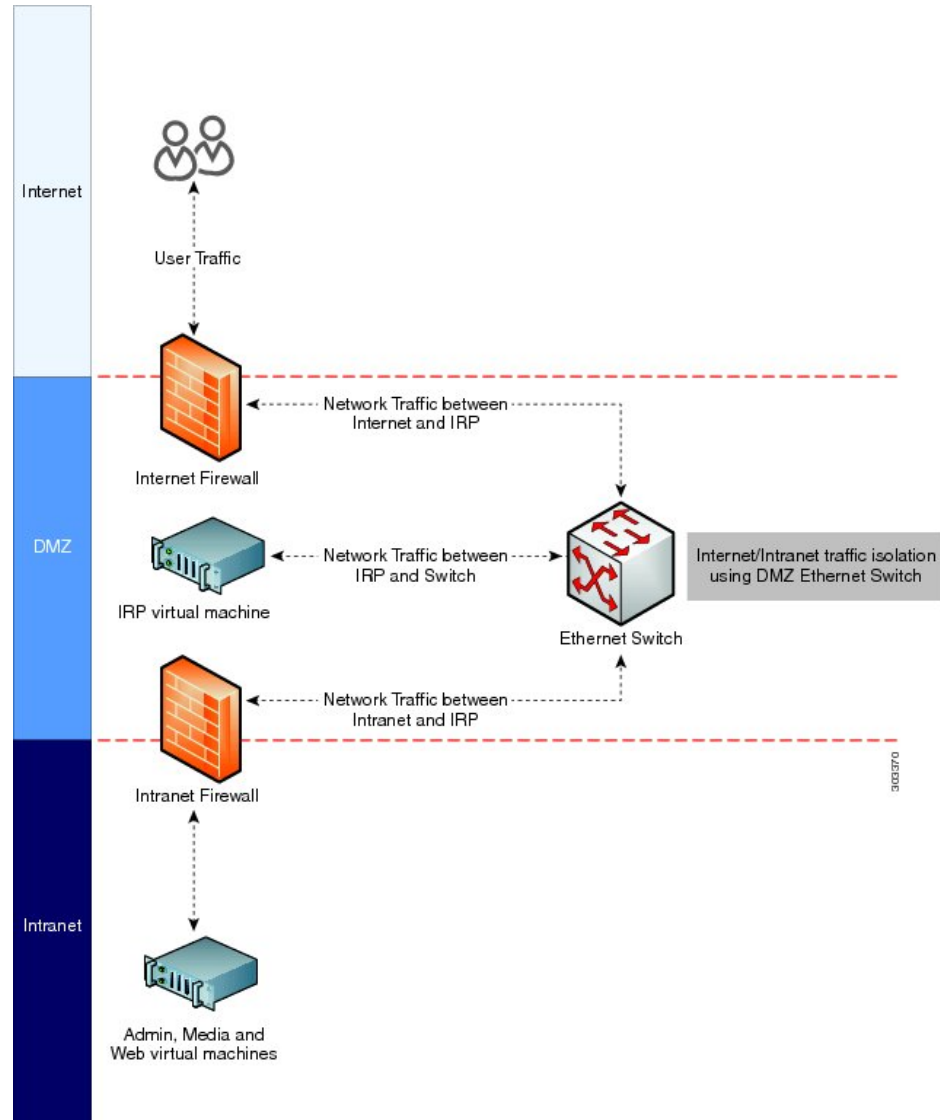
You may set up network traffic isolation between the Internet and your internal network by using a DMZ Ethernet switch. The following procedure and diagram illustrate one example:

- 1 Connect the Internet Reverse Proxy to a head-end switch or router and use that switch or router to split the Internet and Intranet traffic.



- Once the switch or router splits the traffic, then you can pipe those two traffic patterns to two separate physical ports on the switch or router. One port points to the Internet and other port points to the Intranet.

Here is a diagram of a sample network topology:



For information about network bandwidth requirements, see [Network Bandwidth Requirements](#), on page 17.

## Network Bandwidth Requirements

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

### Estimating Bandwidth for End User Sessions

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

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

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

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

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

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

### Bandwidth on Network Paths

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

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

Scenario examples:

- If you expect a maximum of 100 users to connect concurrently from the Internet, you will probably need  $1.5 \text{ Mb/s} \times 100 = 150 \text{ Mb/s}$  of available bandwidth on your ISP connection and through your external firewall to the Internet Reverse Proxy. For mor details about Internet Reverse Proxy, see [Network Considerations for the Internet Reverse Proxy, on page 16](#)

- Assume you have a 2000 user system with all connections going through the Internet Reverse Proxy. In this scenario, you need to assume traffic for all 2000 users will connect to the Internet Reverse Proxy, and then from the Internet Reverse Proxy to the internal virtual machines. The aggregate bandwidth coming into the Internet Reverse Proxy from other parts of the network will be  $2000 \times 1.5 \text{ Mb/s} = 3 \text{ Gb/s}$ . For more details about non-split-horizon, see [Non-Split-Horizon Network Topology](#), on page 12.




---

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

---

- Assume you have 2000 user system in a split-horizon DNS deployment. In this scenario, your Internet users will connect to the Internet Reverse Proxy while intranet users connect directly to the internal virtual machines. Assume ten percent of your users connect to a meeting using the Internet versus 90 percent of users connect to their meetings through the Intranet. The result is the aggregate bandwidth coming into the Internet Reverse Proxy will now be approximately 300 Mb/s (10 percent of 2000 users times 1.5 Mb/s equals 300 Mb/s). If that same 300 Mb/s of traffic passes from the Internet Reverse Proxy, the NIC on the Internet Reverse Proxy may be required to handle 600 Mb/s of user traffic. This is a dramatically lower bandwidth requirement than with a non-split-horizon DNS deployment described in the previous scenario. The reduction in network traffic has direct bearing on the recommendations for NIC or switch interface speed (see next section) which can result in you being able to deploy less expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network. For more details about split-horizon, see [Split-Horizon Network Topology](#), on page 14.




---

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

---

See [NIC Teaming for Bandwidth Aggregation](#), on page 21 for more details.

### Bandwidth on Cisco WebEx Meetings Server Network Interfaces

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

System Capacity	NIC or Switch Interface Speed
50 user system	1 Gb/s
250 user system	1 Gb/s
800 user system	10 Gb/s <sup>1</sup>
2000 user system	10 Gb/s <sup>2</sup>

- <sup>1</sup> You may optionally choose to reduce network infrastructure costs by deploying NIC Teaming using two or more Gigabit Ethernet NICs on the UCS Server and NIC Teaming on the head-end switch.
- <sup>2</sup> If you have a non-split-horizon DNS deployment, the 10 Gb/s requirement pertains to the IRP and internal virtual machines. If you have a split-horizon DNS deployment, you may be able to reduce the network infrastructure demands on your IRP (and DMZ network), which can result in you being able to deploy less expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network, as described in the "Bandwidth on Network Paths" section. However the 10 Gb/s speed requirement holds true for the internal virtual machines (and internal network).

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

#### Assumptions for NIC Speed Calculations:

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

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



#### **Note**

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

### **Bandwidth Considerations for Split-Horizon DNS Deployments**

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

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



---

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

---

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

## NIC Teaming for Bandwidth Aggregation

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



---

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

---

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



---

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

---

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

- Set up an Ethernet switch which supports IEEE 802.3ad/IEEE 802.1ax Link Aggregation Control Protocol (LACP).
- Using vCenter, connect the virtual machine port group associated with the Cisco WebEx Meetings Server virtual machines to both physical adapters.

- Connect both physical adapters to the switch.
- Provision the switch to statically provision the two ports as a team.
- Using VMware vSphere, set NIC Teaming to Active/Active to allow throughput on both NIC interfaces.

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

**Note**

---

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

---



## 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, page 23](#)
- [Deployment Sizes For Your System, page 23](#)
- [Requirements for vCenter Co-residency , page 24](#)
- [Virtual Machines In Your System, page 24](#)
- [50 User System, page 25](#)
- [250 User System, page 26](#)
- [800 User System, page 26](#)
- [2000 User System, page 27](#)

### 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 25](#)
- [250 User System, on page 26](#)
- [800 User System, on page 26](#)
- [2000 User System, on page 27](#)

## 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. The Internet Reverse Proxy is required for your mobile workforce to attend meetings.




---

**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 topology.)

- [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.

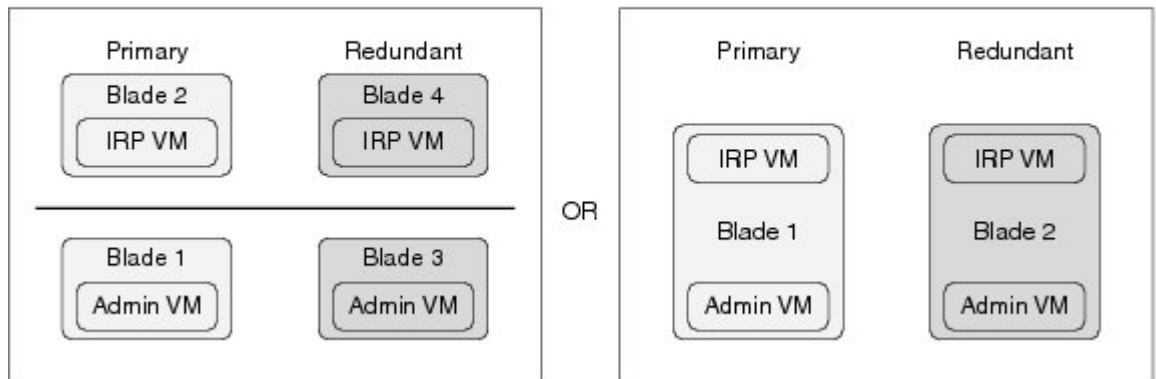



---

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

---

Virtual Machine Layout  
50 Concurrent Users Deployment



3102988

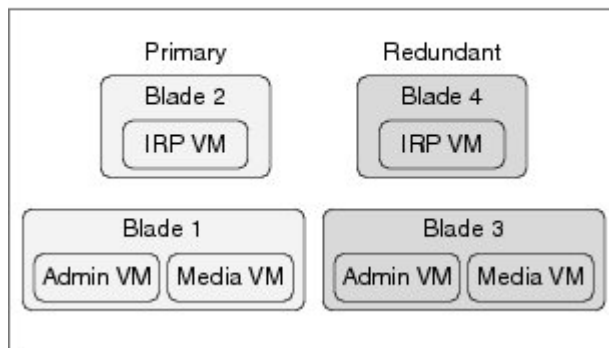
## 250 User System

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.

Virtual Machine Layout  
250 and 800 Concurrent Users Deployment



3102988

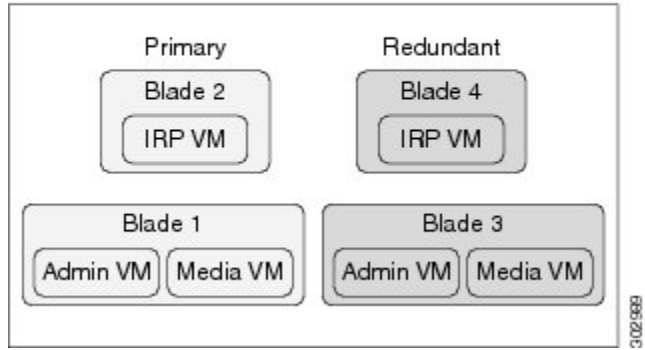
## 800 User System

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



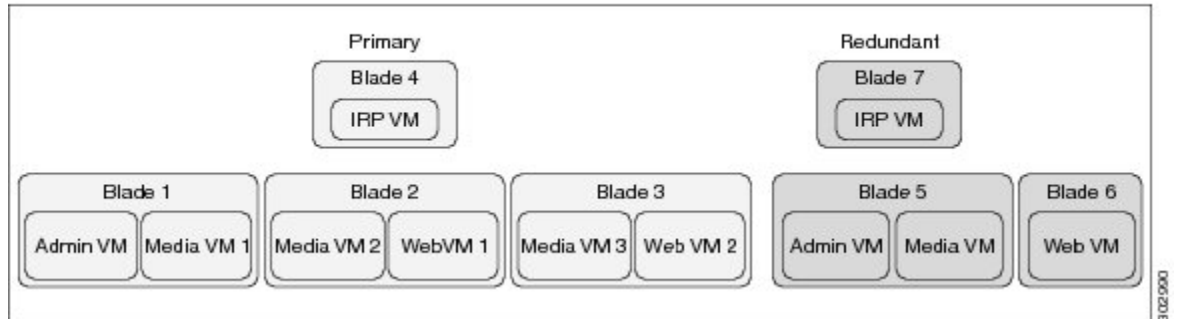
## 2000 User System

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.

Virtual Machine Layout  
2000 Concurrent Users Deployment



**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.)





# 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
  
- [Networking Checklist For Your System, page 30](#)
- [Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines, page 31](#)
- [Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines, page 33](#)
- [Networking Checklist for an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS, page 36](#)
- [Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS, page 39](#)
- [Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS, page 42](#)
- [Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS, page 44](#)
- [Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access, page 47](#)
- [Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access, page 49](#)
- [WebEx Site and WebEx Administration URLs, page 51](#)
- [Port Access When All the Virtual Machines Are in the Internal Network, page 53](#)

- [Port Access With an Internet Reverse Proxy in the DMZ Network](#), page 53
- [VMware vCenter Ports](#), page 60
- [Cisco WebEx Meeting Center Ports](#), page 61
- [Using NAT With Your System](#), page 61
- [Forward Proxies](#), page 63

## 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 31
  - [Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines](#), on page 33
- 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 36
  - [Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS](#), on page 39
- Split-horizon DNS
  - [Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS](#), on page 42
  - [Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS](#), on page 44
- Systems without public access
  - [Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access](#), on page 47
  - [Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access](#), on page 49

# 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) <b>Note</b> 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.

**Note**

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Update your DNS server with Administration site URL and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt; &lt;Public-VIP-address&gt;</li> </ul>

**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 53](#).

**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	<ul style="list-style-type: none"> <li>• Internal Subnet &lt;internal-subnet&gt;/24</li> <li>• DMZ Subnet &lt;DMZ-subnet&gt;/24</li> </ul>



Task	Compare These IP Addresses
<p>Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.</p> <p><b>Note</b> 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.</p>	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
<p>Ensure that the Private VIP address and internal virtual machines are on the same subnet.</p>	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>

## 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)	

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

### DNS Configuration

Make the following changes to your DNS configuration.



#### Note

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Update your DNS server with Administration site URL and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt; &lt;Public-VIP-address&gt;</li> </ul>

### 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 53.

### 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	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet. <b>Note</b> 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.	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>

## 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)	
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.

**Note**

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>

Task	Example
Update your DNS server with Administration site URL and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt; &lt;Public-VIP-address&gt;</li> </ul>

### 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 53.

### 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	<ul style="list-style-type: none"> <li>• Internal Subnet &lt;internal-subnet&gt;/24</li> <li>• DMZ Subnet &lt;DMZ-subnet&gt;/24</li> </ul>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Ensure that the Private VIP address and internal virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>

# 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)	
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)	

Description	Network Location	IP Address
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

### DNS Configuration

Make the following changes to your DNS configuration.



#### Note

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt;   &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt;   &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt;   &lt;web-vm-IP-address&gt;</li> </ul>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt;   &lt;IRP-vm-IP-address&gt;</li> </ul>
Update your DNS server with Administration site URL and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt;   &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt;   &lt;Public-VIP-address&gt;</li> </ul>



**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 53.

**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	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt;   &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt;   &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt;   &lt;web-vm-IP-address&gt;</li> </ul>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt;   &lt;IRP-vm-IP-address&gt;</li> </ul>
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt;   &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt;   &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt;   &lt;web-vm-IP-address&gt;</li> </ul>

# 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)	
WebEx site URL (used exclusively by the system. Maps to two VIP addresses) <ul style="list-style-type: none"> <li>• internal users—private VIP address</li> <li>• external users—public VIP address</li> </ul>	<ul style="list-style-type: none"> <li>• Internal users—Internal (same subnet as Admin virtual machine)</li> <li>• External users—DMZ (same subnet as the Internet Reverse Proxy)</li> </ul>	
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.

**Note**

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs](#), on page 51.

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>
Update your DNS server (that enables internal lookup) with the hostname and IP address for the DMZ virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Update your DNS server (that enables internal lookup) with WebEx site URL, Administration site URL, and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> <li>• &lt;WebEx-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server (that enables external lookup) with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt; &lt;Public-VIP-address&gt;</li> </ul>

**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 53.

**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	<ul style="list-style-type: none"> <li>• Internal Subnet &lt;internal-subnet&gt;/24</li> <li>• DMZ Subnet &lt;DMZ-subnet&gt;/24</li> </ul>

Task	Compare These IP Addresses
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Ensure that the Private VIP address and internal virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>

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

### Virtual Machine Deployment

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

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

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

### Required IP Addresses

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

Description	Network Location	IP Address
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to two VIP addresses) <ul style="list-style-type: none"> <li>• internal users—private VIP address</li> <li>• external users—public VIP address</li> </ul>	<ul style="list-style-type: none"> <li>• Internal users—Internal (same subnet as Admin virtual machine)</li> <li>• External users—DMZ (same subnet as the Internet Reverse Proxy)</li> </ul>	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

### DNS Configuration

Make the following changes to your DNS configuration.



#### Note

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>
Update your DNS server (that enables internal lookup) with the hostname and IP address for the DMZ virtual machine.	<ul style="list-style-type: none"> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
Update your DNS server (that enables internal lookup) with WebEx site URL, Administration site URL, and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> <li>• &lt;WebEx-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>
Update your DNS server (that enables external lookup) with WebEx site URL and Public VIP address information.	<ul style="list-style-type: none"> <li>• &lt;WebEx-site-URL&gt; &lt;Public-VIP-address&gt;</li> </ul>

### 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 53.

### 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	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	<ul style="list-style-type: none"> <li>• &lt;Public-VIP-address&gt;</li> <li>• &lt;IRP-vm-FQDN&gt; &lt;IRP-vm-IP-address&gt;</li> </ul>
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.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>

## 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.

**Note**

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>
Update your DNS server with Administration site URL, WebEx site URL, and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> <li>• &lt;WebEx-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>

**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.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> </ul>

## 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)	

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

### DNS Configuration

Make the following changes to your DNS configuration.



#### Note

There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see [WebEx Site and WebEx Administration URLs, on page 51](#).

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.	<ul style="list-style-type: none"> <li>• &lt;admin-vm-FQDN&gt;   &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt;   &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt;   &lt;web-vm-IP-address&gt;</li> </ul>

Task	Example
Update your DNS server with Administration site URL, WebEx site URL, and Private VIP address information.	<ul style="list-style-type: none"> <li>• &lt;Administration-site-URL&gt; &lt;Private-VIP-address&gt;</li> <li>• &lt;WebEx-site-URL&gt; &lt;Private-VIP-address&gt;</li> </ul>

### 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.	<ul style="list-style-type: none"> <li>• HTTP &lt;Private-VIP-address&gt;:80</li> <li>• HTTPS &lt;Private-VIP-address&gt;:443</li> </ul>

### 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.	<ul style="list-style-type: none"> <li>• &lt;Private-VIP-address&gt;</li> <li>• &lt;admin-vm-FQDN&gt; &lt;admin-vm-IP-address&gt;</li> <li>• &lt;media-vm-FQDN&gt; &lt;media-vm-IP-address&gt;</li> <li>• &lt;web-vm-FQDN&gt; &lt;web-vm-IP-address&gt;</li> </ul>

## WebEx Site and WebEx Administration URLs

### WebEx Site URL

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

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

### **WebEx Administration URL**

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

### **Names for the WebEx Site and WebEx Administration URLs**

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

- the same name as the hostnames for any of the virtual machines comprising the system
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version

- WBXService
- webex

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

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

**Note**

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

### 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).

**Restriction**

Configure TCP port 64700 on the Internet Reverse Proxy to deny any requests that come to the public VIP address. In the external firewall, you will limit access to this port for requests only from the Admin virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	443	Any external clients	Public VIP (Eth1) of the 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.
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.

---



---

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

---



---

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

---



---

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

---

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64001	All internal virtual machines (Eth0 IP)	Real IP (Eth0) of the 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.
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.



Protocol	Port	Source	Destination	Why It Is Needed
TCP	64616	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	<p>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.</p> <p><b>Note</b> Using iptables or access control lists (ACLs), configure the firewall so that connections to port 64616 only come from the Admin virtual machine.</p>

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64700	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	<p>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.</p> <p><b>Note</b> Limit access to this port on all Cisco WebEx Meetings Server virtual machines only to other Cisco WebEx Meetings Server virtual machines with firewall rules.</p>
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.
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.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	65002	Any internal client machines	Any internal client machines	Controls network traffic between internal virtual machines
TCP	65102	Any internal client machines	Any internal client machines	Controls network traffic between internal virtual machines
TCP	80	Any internal client machines	Private VIP (Eth1) of the Admin virtual machines	Internal users accessing the WebEx site URL using http. TCP connections are established from the internal client machine to the Admin virtual machine.
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 are some of the ports that are used during the deployment of Cisco WebEx Meetings Server. Once the deployment completes, you may optionally close any ports that were opened solely for the deployment.

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

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

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

# Cisco WebEx Meeting Center Ports

These ports are used for communication between Cisco WebEx Meeting Center and Cisco WebEx Meetings Server.

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

## 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](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.

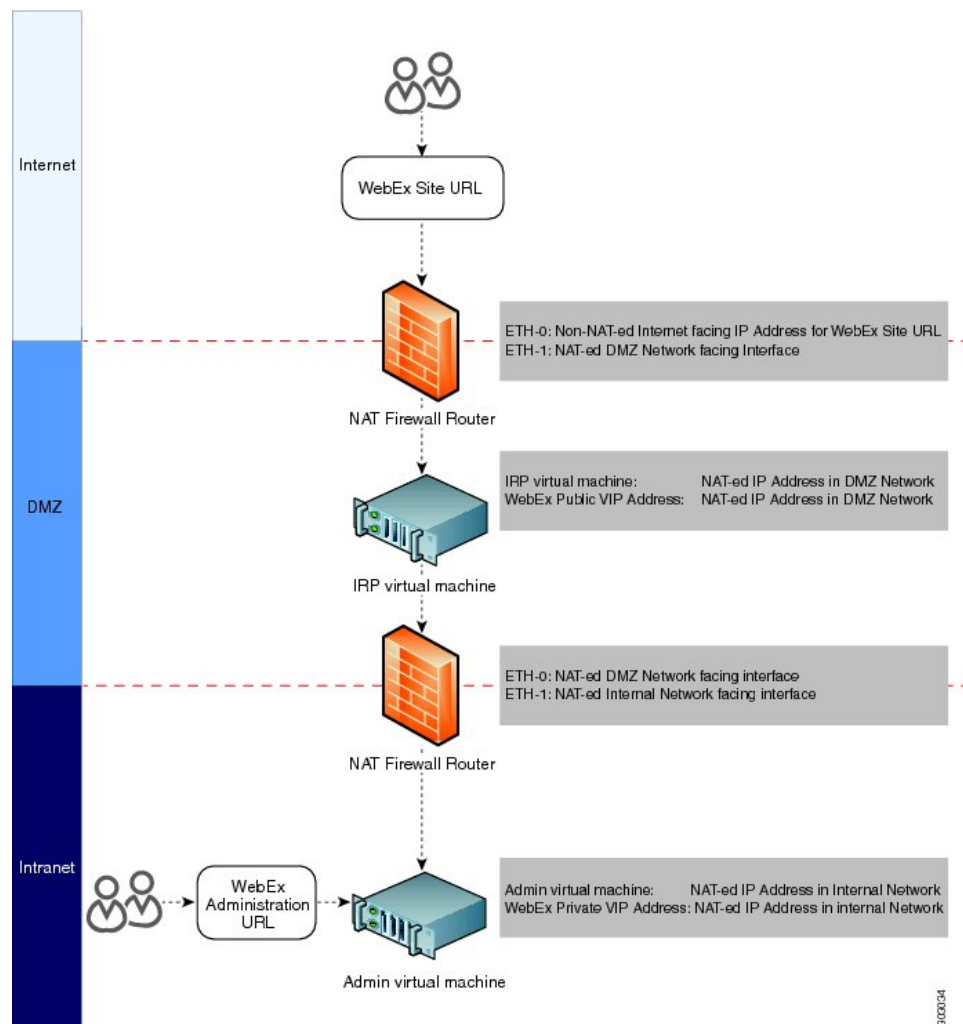
---

**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.



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, page 65](#)

### 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 video and video file sharing (users sharing or receiving video combined)	25	125	400	1000
Participants in a meeting	50	100	100	100
Playback recordings of meetings that have ended	12	63	200	500
Recordings of meetings in progress	3	13	40	100
Calls per second	1	3	8	20
Conferences (assuming 2 participants per meeting)	25	125	400	1000

**Tip**

---

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

---

**Note**

---

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

---

For information about network bandwidth requirements for the various size user systems, see [Network Bandwidth Requirements](#).



## Best Practices

---

- [Cisco WebEx Meetings Server Best Practices, page 67](#)

### Cisco WebEx Meetings Server Best Practices

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

- Power your virtual machine hosts using UPS to minimize power interruptions. Repeated power failures can damage host systems and virtual machines.
- Make sure you always put your system into maintenance mode before shutting down a guest operating system.
- For scheduled events and other situations that require a system shutdown, make sure you gracefully shut down your virtual machines by shutting down the guest operating system.
- The system is designed to repair itself when necessary and rebooting can interrupt this process. We do not recommend that you reboot your system to fix it. If your system is in an unhealthy state, contact the Cisco TAC. Power off your system only when instructed to do so or during scheduled events such as data center maintenance.
- Configure network redundancy to minimize network failures. Refer to "Adding a High Availability System" in the *Cisco WebEx Meetings Server Administration Guide* for more information.
- Configure NIC teaming on your system. NIC teaming improves performance and provides redundancy in the event of a NIC failure.
- If your organization has expertise in managing a storage area network (SAN), we recommend SAN over direct attached storage (DAS). SANs can be more reliable than local disk arrays. Refer to the *Cisco WebEx Meetings Server System Requirements* for more information on SAN storage requirements.
- Using snapshots on your virtual machines can impair system performance in ways that affect user experience even when the system is otherwise lightly loaded.
- If your system is having problems, make sure you check your VMware VCenter environment to determine if conditions in VCenter or the network are causing the problem.
- Configure high availability to increase the probability that your system can continue to operate if a failure occurs.

- If you have a high-availability system and your secondary system fails, you can repair it by removing the existing secondary system (refer to "Removing a High Availability System" in your *Cisco WebEx Meetings Server Administration Guide*) and adding a new secondary system (refer to "Adding a High Availability System" in your *Cisco WebEx Meetings Server Administration Guide*). If the primary system on a high-availability system fails, you cannot repair it using this procedure. We recommend that you restore your primary system using the disaster recovery procedure and then add a new secondary system. Until you add a new secondary system your deployment will be operating without full redundancy. This procedure helps prevent unplanned outages if any of your secondary virtual machines fails. Refer to "Using the Disaster Recovery Feature" in the *Cisco WebEx Meetings Server Administration Guide* for more information.
- Provision a network file system (NFS) and make sure that it has enough storage capacity to store regular automatic backups of your database and meeting recordings.
- Since your system only keeps the latest system backup on the NFS and removes previous ones every day, we recommend that you keep several recent backups on other media.
- Use your dashboard to monitor the health status of the NFS, CPU, and storage. Ensure that dashboard alarms for storage and CPU are enabled.
- If you plan to use directory integration, refer to the Configuring Directory Integration section in the "Managing Users" chapter of the *Cisco WebEx Meetings Server Configuration Guide* for more information.
- When using Cisco WebEx Meetings Server, the related SIP trunk on CUCM in the Call Manager interface should have the **Media Termination Point Required** check box deselected on the **Trunk Configuration** page. See [Configuring a SIP Trunk on a Load Balance Point, on page 81](#) and [Configuring a SIP Trunk for an Application Point, on page 83](#) for more details.



# Configuring Cisco Unified Communications Manager (CUCM)

---

- [Cisco Unified Communications Manager \(CUCM\) Configuration Summary, page 69](#)
- [Configuration Checklist, page 70](#)
- [Configuring CUCM for High-Availability and Non-High-Availability Systems, page 71](#)
- [Configuring a SIP Trunk Security Profile, page 75](#)
- [Configuring a SIP Profile, page 77](#)
- [Certificate Management, page 79](#)
- [Configuring a SIP Trunk, page 81](#)
- [Configuring a Route Group, page 84](#)
- [Configuring a Route List, page 85](#)
- [Configuring a Route Pattern, page 85](#)
- [Configuring a SIP Route Pattern, page 86](#)
- [CUCM Feature Compatibility and Support, page 86](#)

## Cisco Unified Communications Manager (CUCM) Configuration Summary

To enable teleconferencing on Cisco WebEx Meetings Server you must configure one CUCM system to manage call control but you can optionally configure a second CUCM system for audio high availability.

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

- Size (50/250/800/2000)

- High availability
- Transport type

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

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

- Base configuration



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

- SIP trunk security profile
- SIP profile

- Specific configuration



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

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

## 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 <sup>3</sup>	1
50 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)
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
2000 users	2	1	5	1	1	N	3
2000 users with high availability	2	1	6	1	1	N	4

<sup>3</sup> N is the number of Call-In Access Numbers that you configure in Cisco WebEx Meetings Server.

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

#### Configuration Procedure

Perform the following steps:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point</a> , on page 75 and <a href="#">Configuring a SIP Trunk Security Profile for an Application Point</a> , on page 76.
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 <a href="#">Configuring a TLS SIP Profile</a> or <a href="#">Configuring an IPv6 SIP Profile</a> , on page 78.
3	Configure one SIP trunk for your load balance point.	See <a href="#">Configuring a SIP Trunk on a Load Balance Point</a> .
4	Configure one SIP trunk for your application point.	See <a href="#">Configuring a SIP Trunk for an Application Point</a> .
5	Configure one route group by using the SIP trunk that you configured for your load balance point in Task 3, above.	See <a href="#">Configuring a Route Group</a> .
6	Configure one route list using the route group that you configured in Task 5, above.	See <a href="#">Configuring a Route List</a> .
7	Configure <i>N</i> route patterns by using the above route list. <i>N</i> is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See <a href="#">Configuring a Route Pattern</a> .
8	Configure one SIP route pattern for your application point.	See <a href="#">Configuring a SIP Route Pattern</a> .

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

### Configuration Procedure

Perform the following steps:



Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point</a> , on page 75 and <a href="#">Configuring a SIP Trunk Security Profile for an Application Point</a> , on page 76.
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 <a href="#">Configuring a TLS SIP Profile</a> or <a href="#">Configuring an IPv6 SIP Profile</a> , on page 78.
3	Configure two SIP trunks for your load balance points.	See <a href="#">Configuring a SIP Trunk on a Load Balance Point</a> .
4	Configure two SIP trunks for your application points.	See <a href="#">Configuring a SIP Trunk for an Application Point</a> .
5	Configure one route group by using the SIP trunk that you configured for your load balance point in Task 3, above.	See <a href="#">Configuring a Route Group</a> .
6	Configure one route list by using the route group that you configured in Task 5, above.	See <a href="#">Configuring a Route List</a> .
7	Configure <i>N</i> route patterns by using the above route list. <i>N</i> is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See <a href="#">Configuring a Route Pattern</a> .
8	Configure two SIP route patterns for your application points.	See <a href="#">Configuring a SIP Route Pattern</a> .

## 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 balance points' IP addresses
- Three application points' 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 balance point and add a SIP trunk security profile for your application point. See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 75</a> and <a href="#">Configuring a SIP Trunk Security Profile for an Application Point, on page 76</a> .
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 <a href="#">Configuring a TLS SIP Profile</a> or <a href="#">Configuring an IPv6 SIP Profile, on page 78</a> .
3	Configure two SIP trunks for your load balance points.	See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 75</a> .
4	Configure three SIP trunks for your application points.	See <a href="#">Configuring a SIP Trunk Security Profile for an Application Point, on page 76</a> .
5	Configure one route group using the SIP trunk that you configured for your load balance point in Task 3, above.	See <a href="#">Configuring a Route Group, on page 84</a> .
6	Configure one route list using the route group that you configured in Task 5, above.	See <a href="#">Configuring a Route List, on page 85</a> .
7	Configure <i>N</i> route patterns using the above route list. <i>N</i> is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See <a href="#">Configuring a Route Pattern, on page 85</a> .
8	Configure three SIP route patterns for your application points.	See <a href="#">Configuring a SIP Route Pattern, on page 86</a> .

## 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 balance points' IP addresses
- Four application points' 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 balance point and add a SIP trunk security profile for your application point. See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 75</a> and <a href="#">Configuring a SIP Trunk Security Profile for an Application Point, on page 76</a> .
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 <a href="#">Configuring a TLS SIP Profile</a> or <a href="#">Configuring an IPv6 SIP Profile, on page 78</a> .
3	Configure two SIP trunks for your load balance points.	See <a href="#">Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 75</a> .
4	Configure four SIP trunks for your application points.	See <a href="#">Configuring a SIP Trunk Security Profile for an Application Point, on page 76</a> .
5	Configure one route group using the SIP trunk that you configured for your load balance point in Task 3, above.	See <a href="#">Configuring a Route Group, on page 84</a> .
6	Configure one route list using the route group that you configured in Task 5, above.	See <a href="#">Configuring a Route List, on page 85</a> .
7	Configure <i>N</i> route patterns using the above route list. <i>N</i> is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See <a href="#">Configuring a Route Pattern, on page 85</a> .
8	Configure four SIP route patterns for your application points.	See <a href="#">Configuring a SIP Route Pattern, on page 86</a> .

## Configuring a SIP Trunk Security Profile

### Configuring a SIP Trunk Security Profile for a Load Balance Point

#### Before You Begin

If your Cisco WebEx Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the 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 to communicate with 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 with Cisco WebEx Meetings Server using UDP/TCP. Enter 5061 if you want CUCM communicates Cisco WebEx Meetings Server using TLS.
- Note** Do not configure any of the other fields on the page. Leave them with their default settings.
- Step 6** Select **Save**.
- 

## Configuring a SIP Trunk Security Profile for an Application Point

### Before You Begin

If your Cisco WebEx Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the *Administration Guide*.

## Procedure

---

- Step 1** Sign in to `http://cucm-server/`, where *cucm-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 to communicate with 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 with Cisco WebEx Meetings Server using UDP/TCP. Enter 5063 if you want CUCM to communicate with 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**.
-

# 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.



---

**Note** If Cisco WebEx Meetings Server uses third-party certificates, then all certificates in the certificate chain need to be uploaded to CUCM.

---

- Download your CUCM certificate and then upload it to Cisco WebEx Meeting Server Administration site.



---

**Note** If CUCM uses third-party certificates, then only the last certificate in the certificate chain (Root Certificate Authority (CA) certificate) needs to be uploaded to Cisco WebEx Meetings Server.

---

Refer to "Managing Certificates" in the *Administration Guide* for more information. See [http://www.cisco.com/en/US/products/ps12732/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html) for more details.

## Uploading Cisco WebEx Meetings Server Certificates

### Procedure

---

- Step 1** Download and export your Cisco WebEx Meetings Server certificate.
- a) Sign in to the Cisco WebEx Meetings Server Administration site.
  - b) Select **Settings > Security > Certificates**.
  - c) Copy the certificate name from the SSL Certificate section.
  - d) Select **More Options > Export SSL certificate**.
  - e) Save your certificate to your local hard drive.
- Step 2** Sign in to `http://ccm-server/`, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
- Step 3** 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**.

---

## Installing a Third-Party CUCM Certificate

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

### Before You Begin

- Generate a Certificate Signing Request (CSR) and send it to a third part certificate authority to apply for certificates. See [Generating a Certificate Signing Request \(CSR\)](#) for instructions.
- The certificate authority will send you a certificate chain which can have the following:
  - Certificate 1 (end user) - issued to an end-user entity by an intermediate certificate authority.
  - Certificate 2 (intermediate) - issued to an intermediate certificate authority by a root certificate authority.
  - Certificate 3 (Root CA) - issued by the root certificate authority.
- When you receive multiple certificates in a certificate chain, you should concatenate the three certificates into one file, with the end user certificate first.

### Procedure

---

**Step 1** Import your third-party certificate file into you Cisco WebEx Meetings Server. See [Importing a SSL Certificate](#) for instructions.

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

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

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

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

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

**Step 7** Select **Browse** button and select the Root Certificate Authority (CA) certificate that you saved to your local hard drive.  
This is the last, self-signed certificate from the verification chain, which is used to verify the CallManager.pem certificate.

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

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

**Step 9** Select **Close**.

---



### What to Do Next

For more information about certificates, refer to the "Managing Certificates" section in the *Administration Guide* at [http://www.cisco.com/en/US/products/ps12732/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html).

## 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 *Administration Guide*. See [http://www.cisco.com/en/US/products/ps12732/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html) for more details.

## Configuring a SIP Trunk

### Configuring a SIP Trunk on a Load Balance Point

#### Procedure

---

- Step 1** Sign in to <http://ccm-server/>, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
  - Step 2** 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.

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

**Step 6** Select **Next**.

**Step 7** Configure the following fields:

- **Device Name**—Enter a name for the SIP trunk.
- **Device Pool**—Select an appropriate device pool from the drop-down menu.  
To determine which Cisco Unified Communications Manager Group has been configured on that device pool, select **System > Device Pool menu**. To verify which Cisco Unified Communications Managers are part of this group, select **System > Cisco Unified CM Group**.
- **Note** Record the IP addresses of the primary and secondary server. You will enter these IP addresses when you configure your audio settings in Cisco WebEx Meetings Server. See "Configuring Your Audio Settings for the First Time" in the *Administration Guide* for more details. See [Cisco WebEx Meetings Server Install and Upgrade Guides](#).
- **Destination Address**—Enter your load balance point IPv4 address. Refer to the SIP Configuration table on your Administration Site Audio page the IP address.
- **Destination Address IPv6**—Enter your load balance point IPv6 address if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- **Destination Port**—Enter 5060 if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Enter 5061 if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- **SIP Trunk Security Profile**—Select your load balance point's security profile from the drop-down menu.
- **SIP Profile**—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- **Calling Search Space**—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM that you want Cisco WebEx Meetings Server to call out to. Select **Call Routing > Class of Control > Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
- **Rerouting Calling Search Space**—Select a Calling Search Space that contains the route partition that is configured for the SIP route pattern from the section below, "Configuring a SIP Route Pattern." If this is set to **< None >**, then this will only be able to route calls to route patterns with a route partition set to **< None >**, so the SIP route pattern will need to have the route partition set to **< None >**. This configuration is necessary to enter meetings in Cisco WebEx Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide* for more information.

**Note** Do not change any other fields on this page. Leave 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 Point

### Procedure

---

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

**Step 2** 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 the values 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 the application server IPv4 address.
- Destination Address IPv6—Enter your application 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 by using UDP/TCP. Enter 5063 if you want CUCM to communicate with Cisco WebEx Meetings Server by using TLS.
- SIP Trunk Security Profile—Select your application server security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server by using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server by using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- Calling Search Space—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM that you want to enable Cisco WebEx Meetings Server to call. Select **Call Routing > Class of Control > Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. If this is set to **<None >**, this will only be able to call devices or route patterns with a partition set to **<None >**. For more information, refer to *Calling Search Space Configuration* in the *Cisco Unified Communications Manager*

*Administration Guide or Partitions and Calling Search Spaces in the Cisco Unified Communications Manager System Guide.*

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

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

**Step 8** 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 the configuration.

## Configuring a Route Group

### Procedure

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

**Step 2** 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 Balance Point** 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 85.

# 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 85.

# 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.
  - Route Partition—Select a route partition that is accessible by phones or devices that can call Cisco WebEx Meetings Server. If this set to **<None>** any device configured in CUCM would be able to call

Cisco WebEx Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

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

**Note** Do not change any other fields on this page. Leave 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

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

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

**Step 6** Select **Save**.

---

## CUCM Feature Compatibility and Support

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

**CUCM Feature Compatibility**

Cisco WebEx Meetings Server supports CUCM 7.1, 8.6, 9.0, and 9.1.

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 9.0-9.1	Pre-Conditions/Remarks
Call out (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.
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.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1	Pre-Conditions/Remarks
TCP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balance points; 5062 for conferencing application points.
TLS	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5061 for conferencing load balance points; 5063 for conferencing application points.
UDP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balance points; 5062 for conferencing application points.
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 9.0-9.1
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



Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1
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





## 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)
- Cisco WebEx Productivity Tools (Windows)
- Cisco WebEx Network Recording Player (Windows)

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" section in the "Configuring Settings" chapter of the *Cisco WebEx Meetings Server Configuration Guide* 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, page 92](#)
  - [Contents of the Application ZIP Files, page 93](#)
  - [Mass Deployment of Cisco WebEx Productivity Tools, page 95](#)
  - [Mass Deployment of the Meetings Application, page 102](#)
  - [Mass Deployment of the Network Recording Player, page 106](#)
  - [Reconfiguring Your Settings After Performing an Update, page 109](#)

## 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 the Windows platform 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.
- 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 the Windows platform 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.

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

You can unzip the downloaded file and deploy the MSI files to user's desktops with the mass deployment software used by your enterprise. This ensures that the clients are ready for operation when a user wants to schedule or join meetings or view recordings.

**What to Do Next**

For more information about deploying the clients in a Windows environment, refer to the following sections:

- [Mass Deployment of Cisco WebEx Productivity Tools, on page 95](#)
- [Mass Deployment of the Meetings Application, on page 102](#)
- [Mass Deployment of the Network Recording Player, on page 106](#)

Each ZIP file contains the application installer for all 13 supported languages. See [Contents of the Application ZIP Files, on page 93](#) 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.

**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). 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
IT	Italian

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

**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

**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

### Network Recording Player ZIP File Contents

**Note**

Network Recording Player is only available for download and mass deployment if you have selected "Permit users to download WebEx desktop applications" on the Downloads page. Refer to "Configuring Your Download Settings" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

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

## 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.

### Before You Begin

Before you install a maintenance release or upgrade your system to a newer release, your users must uninstall Cisco WebEx Productivity Tools running on their desktops.

### 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.  
**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.
- Mass deployment is possible but each user must enter credential information.

## 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

Before you install a maintenance release or upgrade your system to a newer release, your users must uninstall Cisco WebEx Productivity Tools running on their desktops. After the upgrade, you can use the Administration site to manually push the Productivity Tools to your users or users can download Productivity Tools from the end-user **Downloads** page.

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 101](#) 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 96 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 97, 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: `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 97](#) 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 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) 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 97](#) 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 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) 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, use this sample command: `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 97](#) 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 101](#).
- 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

Before you install a maintenance release or upgrade your system to a newer release, your users must uninstall Cisco WebEx Productivity Tools running on their desktops. After the upgrade, you can use the Administration site to manually push the Productivity Tools to your users or users can download Productivity Tools from the end-user **Downloads** page.

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 101](#) 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 99](#) for more information.
- Step 3** Advertise the program. See [Adding Productivity Tools Components by Using the SMS Per-System Unattended Program, on page 99](#) 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).



**Note** "Silent installation" means the application can be deployed silently but end-user configuration is necessary.

---

## 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.
- 

## Uninstall Cisco WebEx Meetings Locally

You can sign in to a user's computer and uninstall the Cisco WebEx Meetings application from the Control Panel or the WebEx folder on the local hard drive.

### Before You Begin

The Cisco WebEx Meetings application is installed on a user's computer.

### Procedure

---

- Step 1** Sign in to the user's computer.
- Step 2** Delete the Cisco WebEx Meetings application using one of the following methods:
  - Select **Start > Control Panel > Programs and Features**. From the list of programs, select **Cisco WebEx Meetings** and then **Uninstall/Change**.
  - Select **Start > Computer > System (C:) > ProgramData folder > WebEx folder**. Right-click **atcliun.exe** and select **Delete**.

**Note** When you uninstall **atcliun.exe** from the WebEx folder, both the on-premises and cloud versions of the Cisco WebEx Meetings application are removed, if both versions of the application were saved on the user's local hard drive. However, when you uninstall the application using the Control Panel, only the on-premises version of the application is uninstalled.

The Cisco WebEx Meetings application is uninstalled from the user's computer.

---

## 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** 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 101 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 101.
- 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 101 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 101.
  - 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.
- 

## Reconfiguring Your Settings After Performing an Update

**Note**

Your network recording player application automatically upgrades the first time it is used to play a recording after an update is performed.

---

After you perform an update of your Cisco WebEx Meetings Server software, you must update the paths to your mass-deployed applications.

For Mac systems the path is /Users/(Local User)/Library/Application Support/WebEx Folder/.

For Windows systems, your path depends on the version, download type, and web browser type:

- Windows XP, Windows 2000
  - <SystemDisk>\Windows\Downloaded Program Files\WebEx (general administrative users)
  - <SystemDisk>\Program Files\WebEx (MSI installation of WebEx client)
  - <SystemDisk>\Documents and Settings\<UserName>\ WebEx (general users)
  - <SystemDisk>\Documents and Settings\<UserName>\Application Data\WebEx (for Java downloads)
  - <SystemDisk>\Documents and Settings\<UserName>\Local Settings\Temporary Internet Files\webexmc (.exe solution)

- <SystemDisk>\Documents and Settings\<UserName>\Local Settings\Temp\WebEx (write <Username\WebEx fail)
  - <Folder name registered by ieatgpc.dll>\WebEx (if you have built ieatgpc.dll into your system)
  - <FireFoxDir>\plugins\WebEx (for Mozilla Firefox)
- Windows 7 and Windows Vista: <SystemDisk>\ProgramData\WebEx
  - From Productivity Tools or WebEx Connect, use your Productivity Tools or WebEx Connect path.
  - If you are using MSI installation always use a unique path. Your system will ignore the pre-existing file.
  - If you are using the download type with Windows 7, your system will use a unique path. In Windows XP, if the GPC can find the registered table value, your system will use a pre-existing folder. Otherwise the system will use its own path as described above.

Your client applications on both Windows and Mac systems are automatically updated to maintain compatibility with your updated system.

In a locked down environment, you must perform your updates manually for Windows systems but not for Mac systems.



## License Management

---

- [About Licenses, page 111](#)

### About Licenses

#### About User-Based Licensing

This product has Host-based Licensing. It requires that you purchase a license for each user that intends to host meetings. It is important to understand the following terms:

- **Participant**--An individual that attends meetings, but does not schedule or host meetings, and does not have control over the host features, such as presenting content unless the participant is designated by a host to be the presenter.
- **Meeting Host**--Schedules meetings, attends meetings in the capacity of a host, and is allowed control over selected features, such as identifying a presenter or muting another participant.
- **Alternate Host**--Identified when the meeting is scheduled as someone who can assume the host role in the absence of the meeting host. If the meeting host who scheduled the meeting does not attend, the alternate host is given control over most of the same features as the meeting host. If both the individual identified as an alternate host and the meeting host attend the meeting, the status of the alternate host from a licensing perspective is *participant*.
- **Join Before Host (JBH)**--Allows participants to join a meeting before the arrival of the host or an alternate host.
- **Overlapping Meetings**--Two or more meetings that are scheduled during the same time of day by the same host. When a meeting host or an alternate host starts overlapping meetings, additional licenses might be consumed. An individual can schedule overlapping meetings, but the individual cannot host more than one meeting at a time. An overlapping meeting occurs when the host of one meeting leaves that meeting to start another meeting, and the first meeting continues under the direction of a different individual acting as host.
- **Grace Period**--A 15-minute overlap period. The grace period only applies when JBH is enabled and a meeting is started by an attendee who is not the host.

The license usage calculation occurs once per month, for example, once from January 1 through 31, once from February 1 through 28, and so forth. Licenses are counted as follows:

- Licenses are never consumed by *scheduling* meetings. When scheduling a meeting, the meeting host can identify alternative hosts. Identifying alternative hosts or scheduling a meeting on behalf of others does not consume licenses. When attending a meeting, the individual scheduling a meeting is identified as the meeting host by default.
- Licenses are never consumed by participants. If an individual has attended meetings during the month always as a participant and never acted as a host, zero licenses are consumed by that individual.
- One license is consumed and associated to an individual the first time they start a meeting in a given month and are identified as the host of that meeting. If an individual starts any more non-overlapping meetings during the month, no additional licenses are consumed. If during the next month the same individual does not attend any meetings as a host, zero licenses are consumed by that individual for that month. That individual can attend meetings as a participant without consuming a license.
- One additional license is consumed and associated to an individual for every overlapping meeting attended by that individual as the host of those meetings. The total number of licenses consumed by a single individual is determined by the highest number of overlapping meetings hosted by that individual. An individual who attends two meetings in the capacity of host in the same time period consumes and is associated to two licenses for the month. If that individual starts three meetings that overlap the same time period, three licenses are consumed. And so forth. If the same individual attends a meeting as the host, leaves the first meeting before that meeting ends and attends another meeting in the capacity of a host, two licenses are required for that individual.
- No additional licenses are consumed when an individual identified as an alternate host that has not yet consumed a license that month, starts a meeting and the meeting host joins the meeting.
- One license is consumed and associated with an alternate host when an alternate host that has not yet consumed a license that month attends a meeting in the capacity of the host and the meeting host who scheduled the meeting fails to join that meeting.

If you perform a major upgrade or disaster recovery procedure on your system, you must configure new virtual machines and re-host the licenses. (See [Re-hosting Licenses after a Software Upgrade or System Expansion](#).)

The system counts license use for each user each month, as the example scenarios show in the table. The scenarios in the table assume that in every example, it is the first time that a user has hosted a meeting in that month.

Scenario	Meeting Date	Meeting Time	Licenses Consumed
User A schedules a meeting, but the meeting is never started.	January 1	9:00 a.m. to 10:00 a.m.	0
User B starts a meeting.	January 2	9:00 a.m. to 10:00 a.m.	1
User C hosts two or more meetings that do not overlap.	January 3 January 3 January 4	9:00 a.m. to 10:00 a.m. 2:00 p.m. to 2:30 p.m. 10:00 a.m. to 11:00 a.m.	1
User D attends two meetings that overlap the same date and time.	January 6 January 6	9:00 a.m. to 10:00 a.m. 9:30 a.m. to 10:00 a.m.	2



Scenario	Meeting Date	Meeting Time	Licenses Consumed
User E starts two meetings that overlap the same date and time. The host that started both meetings and an alternate host hosts the second meeting.	January 6 January 6	9:00 a.m. to 10:00 a.m. 9:30 a.m. to 10:00 a.m.	3 One license consumed by the host that started each meeting and one license is consumed by the alternate host.
User F starts two meetings on the same date and leaves both meetings. The meetings are each hosted by an alternate host.	January 7 January 7	9:00 a.m. to 10:00 a.m. 9:00 a.m. to 10:00 a.m.	2 One for each for the original host and one for the alternate hosts that continued one of the meetings.
User G starts a meeting and passes host rights to another participant during the meeting. The host of the first meeting then starts a second meeting that runs simultaneously with the first meeting.	January 8 January 8	9:00 a.m. to 10:00 a.m. 9:30 a.m. to 10:00 a.m.	2 One for each for the original host and one for the alternate hosts that continued one of the meetings.
User H starts a meeting that has <b>Join Before Host</b> enabled. A host joins the meeting. The first user then schedules a second meeting that runs simultaneously with the first meeting, but all of the second meeting participants join the teleconference only (not the web portion) option selected.	January 11 January 11	9:00 a.m. to 10:00 a.m. 9:00 a.m. to 10:00 a.m.	2
User J schedules a meeting. <b>Join Before Host</b> is enabled. Participants join, but neither the meeting host nor an alternate host attends the meeting and all participants leave the meeting.	January 11	9:00 a.m. to 10:00 a.m.	1
User K starts a meeting with <b>Join Before Host</b> enabled. The JBH attendee starts a second meeting on behalf of the host. Before the grace period expires the host leaves and ends the first meeting.	January 12 January 12	9:00 a.m. to 10:00 a.m. 9:10 a.m. to 10:00 a.m.	1

Scenario	Meeting Date	Meeting Time	Licenses Consumed
User L starts three Personal Conferences (not the web portion) with account 1, account 2 and account 3 at the same date but different times.	January 12 January 12 January 12	9:00 a.m. to 10:00 a.m. 10:00 a.m. to 11:00 a.m. 11:00 a.m. to 12:00 p.m.	1
User M starts three Personal Conferences (not the web portion) with account 1, account 2 and account 3 at the same date and time.	January 14	9:00 a.m. to 10:00 a.m.	3
User N starts a meeting with <b>Join Before Host</b> enabled and a Personal Conference (not the web portion) at the same date but at different times.	January 14 January 14	9:00 a.m. to 10:00 a.m. 11:00 a.m. to 12:00 p.m.	1
User P starts a meeting with <b>Join Before Host</b> enabled and a Personal Conference (not the web portion) at the same date and time.	January 15 January 15	9:00 a.m. to 10:00 a.m. 9:00 a.m. to 10:00 a.m.	2
User Q starts a Personal Conference (not the web portion) and shortly thereafter launches the overlapping web portion.	January 16 January 16	9:00 a.m. to 10:00 a.m. (Personal Conference) 9:15 a.m. to 10:00 a.m. (Web Meeting launched in conjunction with the Personal Conference)	1

From the **Reports** page, you can request a report that provides the total number of licenses consumed during the month. In addition, we recommend that you view the PDF Summary Report that shows month-by-month license consumption trends. By viewing the overall license trend, you can plan for future license purchases more effectively, to match the growing adoption of this system within your company.



#### Caution

Your system allows license consumption to exceed the number of licenses installed on your system. Administrators receive **licenses exceeded** emails and dashboard notices informing them that they must either reduce license consumption or purchase more licenses within six months. During this six-month period, your system continues to function normally for your users. If you have not reduced license consumption or purchased more licenses after six months, the system shuts down for all users until an administrator installs more licenses.

When the system is shut down, users cannot schedule, host, or attend meetings, or access meeting recordings. Users see a **Site under maintenance** message on the WebEx site. The Administration site functions normally, so an administrator can sign in and add licenses to address the licenses exceeded condition. Once additional licenses have been installed, users are able to access the WebEx site, host meetings, end meetings, and access recordings.

### Six-Month Free-Trial Period

After you sign in to this product for the first time and complete the first-time-experience wizard, your six-month 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 months remain in your free trial. One month 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 [Managing Licenses](#) section of the *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

### Re-hosting Licenses

After CWMS software has been upgraded or an existing system has been expanded, re-hosting the licenses allows older, valid licenses to be used on a upgraded or expanded system. See [Re-hosting Licenses after a Software Upgrade](#) in the *Cisco WebEx Meetings Server Administration Guide*.

### 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.

Licenses can be obtained by using the embedded Cisco Enterprise License Manager, eFulfillment, or by contacting TAC. Refer to the [Managing Licenses](#) section of *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

### Exceeding Your Licenses

Once you have purchased and configured licenses on your system, you must make sure you have enough licenses to accommodate all active hosts on your system. Your system checks every month to determine if there are enough licenses for each active host. The license count is reset each calendar month. If the number of active hosts on your system exceeds the number of licenses, an email is sent to the administrator notifying him that he has exceeded his licenses. You are given a six-month grace period to reduce your license usage or increase the number of licenses on your system so that it meets or exceeds the number of active hosts. If you do not reduce your license usage or 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 number of licenses used as necessary. At the end of each month the system checks license usage. If the number of hosts has dropped below the number of licenses, the licenses exceeded condition ends. If the number of active hosts still exceeds the number of licenses, a new email is sent to your administrator each month that notifies him that the licenses exceeded condition still exists and the date when the system will be disabled.

If you still have a licenses exceeded condition for straight 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, or access recordings 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, and access recordings.

### 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 month, 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, or access recordings on your system. The Administration site will function normally so an administrator can sign in and update licenses. Once an administrator has updated the licenses, users will regain the ability to schedule, host, and attend meetings, and access recordings.

### Prime License Manager (PLM) Connection Lost

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

If your system is still unable to connect to PLM after six months, your system is disabled and the administrator receives an email notification of what has occurred. When your system is disabled, users are not able to schedule, host, or attend meetings, or access recordings on the system. The Administration site functions normally, so an administrator can sign in to the system but the system must reconnect with PLM to end this condition and restore the ability for users to schedule, host, and attend meetings, and access recordings.

### Actions that Require New Licenses

The following system-altering actions require that you install new licenses:

- Expansion—See [Expanding Your System to a Larger System Size](#) for more information.
- Upgrade—See [Upgrading the System](#) for more information.
- Disaster Recovery—See [Using the Disaster Recovery Feature](#) for more information.





## SAML SSO Configuration

---

- [Overview of Single Sign-On, page 119](#)
- [Benefits of Single Sign-On, page 120](#)
- [Overview of Setting Up SAML 2.0 Single Sign-On, page 121](#)
- [SAML SSO for End-User and Administration Sign In, page 121](#)
- [SAML 2.0 Single Sign-On Differences Between Cloud-Based WebEx Meeting Services and WebEx Meetings Server, page 122](#)
- [SAML Assertion Attributes, page 128](#)

### 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 Windows Server 2008/Windows Server 2008 R2 or AD FS server role in Windows Server 2012)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Because SAML 2.0 is an open standard, other SAML 2.0 IdPs might also operate with Cisco WebEx Meetings Server. However, other SAML 2.0 IdPs have not been tested by Cisco. It is therefore the 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 SSO for End-User and Administration Sign In

SAML SSO is typically configured only for sign-in purposes on the End-User site and not the Administration site. On SAML 2.0 SSO-integrated Cisco WebEx Meetings Server sites the behavior mirrors SaaS WebEx behavior when it comes to user authentication. A Cisco WebEx Meetings Server administrator (and an SaaS

WebEx administrator) can sign in to an end-user account using SAML SSO but must sign in to an administrator account on the same system using a separate password. This ensures that in the event of catastrophic failures on the SAML SSO IdP, an administrator will still be able to access the Administration site. Without this failsafe, you might encounter a situation in which the Administration site becomes inaccessible not because of a product failure but because of a problem with the SAML SSO IdP software. The SAML SSO IdP software is on a server that is external to Cisco WebEx Meetings Server (or SaaS WebEx) and therefore outside of our control.

## SAML 2.0 Single Sign-On Differences Between Cloud-Based WebEx Meeting Services and WebEx Meetings Server

While the cloud-based Cisco WebEx meeting services employ unique user IDs when creating users accounts, Cisco WebEx Meetings Server uses email addresses as the basis for creating user accounts. 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
<p>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.</p>	<p>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.</p> <p>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.</p>	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: <ul style="list-style-type: none"> <li>• Leave AAC on.</li> <li>• Before users sign in, manually create user accounts using "CSV File Import" or "Create user" from the Cisco WebEx Administration site.</li> </ul>	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
<p>Special case: A user is also a system administrator.</p> <p>Scenario A: The user signs in to the WebEx Site.</p> <p>Scenario B: The user signs in to the Cisco WebEx Administration site.</p>		<p>Scenario A: Same results as the previous scenario.</p> <p>Scenario B: N/A.</p>	<p>Scenario A: Same results as the previous scenario.</p> <p>Scenario B: N/A.</p>	<p>Scenario A: Same results as the previous scenario.</p> <p>Scenario B: N/A.</p>	<p>Scenario A: Same results as the previous scenario.</p> <p>Scenario B: N/A.</p>

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	<p>Scenario A: Same results as the previous scenario</p> <p>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.</p> <p>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.</p> <p>If the Cisco WebEx Administration site also supports SSO, then malfunctions in</p>				

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.				

## SAML Assertion Attributes

The following table lists the SAML assertion attributes supported by Cisco WebEx Meetings Server. Make sure to configure the lastname, firstname, email, and updatetimestamp attributes. Automatic update does not work unless the updatetimestamp attribute is configured.

### Supported SAML Assertion Attributes

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
lastname		Yes		
firstname		Yes		
email		Yes	Valid email format	



Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
updateTimestamp	The user information update time	No	Support format <b>long format:</b> sample: System.currentTimeMillis() <b>LDIF format:</b> yyyyMMddHHmmss yyyy-MM-dd HH:mm:ss sample: 20090115213256 <b>UTC format</b> ("2009-10-09T06:00:32Z")	If the updateTimeStamp is missing, you cannot perform an auto update user, normally mapped to the whenChanged item if the IdP is linked to AD.
optionalparams		No		Optional parameters can be set in the formats described in the "Optional Parameters" section below.
OPhoneCountry		No		Office phone country code
OPhoneArea		No		Office phone area
OPhoneLocal		No	Enter numerical characters only. For example, 5551212. Do not enter non-numerical characters such as dashes or parentheses.	Office phone local
OPhoneExt		No		Office phone extension
FPhoneCountry		No		Alternate phone country code
FPhoneArea		No		Alternate phone area
FPhoneLocal		No		Alternate phone local
FPhoneExt		No		Alternate phone extension
PPhoneCountry		No		Alternate phone 2 country code
PPhoneArea		No		Alternate phone 2 area
PPhoneLocal		No		Alternate phone 2 local

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
PPhoneExt		No		Alternate phone 2 extension
MPhoneCountry		No		Mobile phone country code
MPhoneArea		No		Mobile phone area
MPhoneLocal		No		Mobile phone local
MPhoneExt		No		Mobile phone extension
TimeZone		No		Time zone (see the "Time Zones" section below)
Address1		No		Address1
Address2		No		Address2
City		No		City
State		No		State
ZIP Code		No		ZIP code
Country		No		Country (see the "Country Values" section below)
Region		No		Region (see the "Region Values" section below)
Language		No		Language (see the "Language Values" section below)
TC1	String	No	Tracking Code Group 1 entered by user on the Administration site	Index 1
TC2	String	No	Tracking Code Group 2 entered by user on the Administration site	Index 2
TC3	String	No	Tracking Code Group 3 entered by user on the Administration site	Index 3
TC4	String	No	Tracking Code Group 4 entered by user on the Administration site	Index 4

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
TC5	String	No	Tracking Code Group 5 entered by user on the Administration site	Index 5
TC6	String	No	Tracking Code Group 6 entered by user on the Administration site	Index 6
TC7	String	No	Tracking Code Group 7 entered by user on the Administration site	Index 7
TC8	String	No	Tracking Code Group 8 entered by user on the Administration site	Index 8
TC9	String	No	Tracking Code Group 9 entered by user on the Administration site	Index 9
TC10	String	No	Tracking Code Group 10 entered by user on the Administration site	Index 10

### Optional Parameters

You can set the optionalparams setting as follows:

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">City=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=OFF</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="City">
- <saml:AttributeValue xsi:type="xs:string">Toronto</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="AA">
- <saml:AttributeValue xsi:type="xs:string">OFF</saml:AttributeValue>

### Time Zone Values

The following table provides the values for the TimeZone attribute.

Time Zone	Value
Marshall Islands (Dateline Time, GMT-12:00)	0
Samoa (Samoa Time, GMT-11:00)	1

Time Zone	Value
Honolulu (Hawaii Time, GMT-10:00)	2
Anchorage (Alaska Daylight Time, GMT-08:00)	3
San Francisco (Pacific Daylight Time, GMT-07:00)	4
Arizona (Mountain Time, GMT-07:00)	5
Denver (Mountain Daylight Time, GMT-06:00)	6
Chicago (Central Daylight Time, GMT-05:00)	7
Mexico City (Mexico Daylight Time, GMT-05:00)	8
Saskatchewan (Central Time, GMT-06:00)	9
Bogota (S. America Pacific Time, GMT-05:00)	10
New York (Eastern Daylight Time, GMT-04:00)	11
Indiana (Eastern Daylight Time, GMT-04:00)	12
Halifax (Atlantic Daylight Time, GMT-03:00)	13
La Paz (S. America Western Time, GMT-04:00)	14
Newfoundland (Newfoundland Daylight Time, GMT-02:30)	15
Brasilia (S. America Eastern Standard Time, GMT-03:00)	16
Buenos Aires (S. America Eastern Time, GMT-03:00)	17
Mid-Atlantic (Mid-Atlantic Time, GMT-02:00)	18
Azores (Azores Summer Time, GMT)	19
Reykjavik (Greenwich Time, GMT)	20
London (GMT Summer Time, GMT+01:00)	21
Amsterdam (Europe Summer Time, GMT+02:00)	22
Paris (Europe Summer Time, GMT+02:00)	23
Berlin (Europe Summer Time, GMT+02:00)	25
Athens (Greece Summer Time, GMT+03:00)	26
Cairo (Egypt Time, GMT+02:00)	28
Pretoria (South Africa Time, GMT+02:00)	29
Helsinki (Northern Europe Summer Time, GMT+03:00)	30
Tel Aviv (Israel Daylight Time, GMT+03:00)	31
Riyadh (Saudi Arabia Time, GMT+03:00)	32

Time Zone	Value
Moscow (Russian Time, GMT+04:00)	33
Nairobi (Nairobi Time, GMT+03:00)	34
Tehran (Iran Daylight Time, GMT+04:30)	35
Abu Dhabi, Muscat (Arabian Time, GMT+04:00)	36
Baku (Baku Daylight Time, GMT+05:00)	37
Kabul (Afghanistan Time, GMT+04:30)	38
Ekaterinburg (West Asia Time, GMT+06:00)	39
Islamabad (West Asia Time, GMT+05:00)	40
Mumbai (India Time, GMT+05:30)	41
Colombo (Colombo Time, GMT+05:30)	42
Almaty (Central Asia Time, GMT+06:00)	43
Bangkok (Bangkok Time, GMT+07:00)	44
Beijing (China Time, GMT+08:00)	45
Perth (Australia Western Time, GMT+08:00)	46
Singapore (Singapore Time, GMT+08:00)	47
Taipei (Taipei Time, GMT+08:00)	48
Tokyo (Japan Time, GMT+09:00)	49
Seoul (Korea Time, GMT+09:00)	50
Yakutsk (Yakutsk Time, GMT+10:00)	51
Adelaide (Australia Central Standard Time, GMT+09:30)	52
Darwin (Australia Central Time, GMT+09:30)	53
Brisbane (Australia Eastern Time, GMT+10:00)	54
Sydney (Australia Eastern Standard Time, GMT+10:00)	55
Guam (West Pacific Time, GMT+10:00)	56
Hobart (Tasmania Standard Time, GMT+10:00)	57
Vladivostok (Vladivostok Time, GMT+11:00)	58
Solomon Is (Central Pacific Time, GMT+11:00)	59
Wellington (New Zealand Standard Time, GMT+12:00)	60
Fiji (Fiji Time, GMT+12:00)	61

Time Zone	Value
Stockholm (Sweden Summer Time, GMT+02:00)	130
Tijuana (Mexico Pacific Daylight Time, GMT-07:00)	131
Chihuahua (Mexico Mountain Daylight Time, GMT-06:00)	132
Caracas (S. America Western Time, GMT-04:30)	133
Kuala Lumpur (Malaysia Time, GMT+08:00)	134
Recife (S. America Eastern Time, GMT-03:00)	135
Casablanca (Morocco Daylight Time, GMT+01:00)	136
Tegucigalpa (Honduras Time, GMT-06:00)	137
Nuuk (Greenland Daylight Time, GMT-02:00)	138
Amman (Jordan Daylight Time, GMT+03:00)	139
Istanbul (Eastern Europe Summer Time, GMT+03:00)	140
Kathmandu (Nepal Time, GMT+05:45)	141
Rome (Europe Summer Time, GMT+02:00)	142
West Africa (West Africa Time, GMT+01:00)	143
Madrid (Europe Summer Time, GMT+02:00)	144

### Country Values

The following table provides the values for the Country attribute.

Country	Value
Afghanistan	93
Albania	355
Algeria	213
American Samoa	1684
Andorra	376
Angola	244
Anguilla	1264
Antarctica	672_1
Antigua (including Barbuda)	1268
Argentina	54
Armenia	374

<b>Country</b>	<b>Value</b>
Aruba	297
Ascension Islands	247
Australia	61
Austria	43
Azerbaijan	994
Bahamas	1242
Bahrain	973
Bangladesh	880
Barbados	1246
Belarus	375
Belgium	32
Belize	501
Benin	229
Bermuda	1441
Bhutan	975
Bolivia	591
Bosnia_Herzegovina	387
Botswana	267
Brazil	55
British Virgin Islands	1284
Brunei	673
Bulgaria	359
Burkina Faso	226
Burundi	257
Cambodia	855
Cameroon	237
Canada	1_1
Cape Verde Island	238
Cayman Islands	1_9
Central African Republic	236
Chad Republic	235

<b>Country</b>	<b>Value</b>
Chile	56
China	86
Colombia	57
Comoros	269_1
Cook Islands	682
Costa Rica	506
Croatia	385
Cuba	53
Cyprus	357
Czech Republic	420
Denmark	45
Diego Garcia	246
Djibouti	253
Dominica	1767
Dominican Republic	1809
Ecuador	593
Egypt outside Cairo	20
El Salvador	503
Equatorial Guinea	240
Eritrea	291
Estonia	372
Ethiopia	251
Faeroe Islands	298
Falkland Islands	500
Fiji Islands	679
Finland	358
France	33
French Depts. (Indian Ocean)	262
French Guiana	594
French Polynesia	689
Gabon Republic	241



<b>Country</b>	<b>Value</b>
Gambia	220
Georgia	995
Germany	49
Ghana	233
Gibraltar	350
Greece	30
Greenland	299
Grenada	1473
Guadeloupe	590
Guantanamo (U.S. Naval Base)	53_1
Guatemala	502
Guinea	224
Guinea-Bissau	245
Guyana	592
Haiti	509
Honduras	504
Hong Kong	852
Hungary	36
Iceland	354
India	91
Indonesia	62
Iran	98
Iraq	964
Ireland	353
Israel	972
Italy	39_1
Ivory Coast	225
Jamaica	1876
Japan	81
Jordan	962
Kazakhstan	7_1

<b>Country</b>	<b>Value</b>
Kenya	254
Kiribati	686
Korea (North)	850
Korea (South)	82
Kuwait	965
Kyrgyzstan	996
Laos	856
Latvia	371
Lebanon	961
Lesotho	266
Liberia	231
Libya	218
Liechtenstein	423
Lithuania	370
Luxembourg	352
Macao	853
Macedonia	389
Madagascar	261
Malawi	265
Malaysia	60
Maldives	960
Mali	223
Malta	356
Marshall Islands	692
Mauritania	222
Mauritius	230
Mayotte Island	269
Mexico	52
Micronesia	691
Moldova	373
Monaco	377

<b>Country</b>	<b>Value</b>
Mongolia	976
Montserrat	1664
Morocco	212
Mozambique	258
Myanmar	95
Namibia	264
Nauru	674
Nepal	977
Netherlands	31
Netherlands Antilles	599_2
New Caledonia	687
New Zealand	64
Nicaragua	505
Niger	227
Niue	683
Norfolk Island	672
Northern Mariana Islands	1670
Norway	47
Oman	968
Pakistan	92
Palau	680
Panama	507
Papua New Guinea	675
Paraguay	595
Peru	51
Philippines	63
Poland	48
Portugal	351
Puerto Rico	1787
Qatar	974
Romania	40

<b>Country</b>	<b>Value</b>
Russia	7
Rwanda	250
San Marino	378
Sao Tome	239
Saudi Arabia	966
Senegal Republic	221
Serbia	381
Seychelles Islands	248
Sierra Leone	232
Singapore	65
Slovakia	421
Slovenia	386
Solomon Islands	677
Somalia	252
South Africa	27
Spain	34
Sri Lanka	94
St. Helena	290
St. Kitts and Nevis	1869
St. Lucia	1758
St. Pierre and Miguelon	508
St. Vincent	1784
Sudan	249
Suriname	597
Swaziland	268
Sweden	46
Switzerland	41
Syria	963
Taiwan	886
Tajikistan	992
Tanzania	255

Country	Value
Thailand	66
Togo	228
Tonga Islands	676
Trinidad and Tobago	1868
Tunisia	216
Turkey	90
Turkmenistan	993
Turks and Caicos	1649
Tuvalu	688
Uganda	256
Ukraine	380
United Arab Emirates	971
United Kingdom	41
United States of America	1
Uruguay	598
Uzbekistan	998
Vanuatu	678
Vatican City	39
Venezuela	58
Vietnam	84
Wallis and Futuna Islands	681
Western Samoa	685
Yemen	967
Zambia	260
Zimbabwe	263

### Region Values

The following table provides the values for the Region attribute.

Region	Value
U.S.	2
Australia	3

Region	Value
Canada	4
French Canada	5
China	6
France	7
Germany	8
Hong Kong	9
Italy	10
Japan	11
Korea	12
New Zealand	13
Spain	14
Switzerland	16
Taiwan	17
U.K.	18
Mexico	19
Argentina	20
Chile	21
Colombia	22
Venezuela	23
Brazil	24
Portugal	25
Belgium	26
Netherlands	27
Russia	28
India	29

### Language Values

The following table provides the values for the Language attribute.

Language	Value
Castilian Spanish	11
Dutch	14

<b>Language</b>	<b>Value</b>
English	1
French	7
German	9
Italian	10
Japanese	5
Korean	6
Latin American Spanish	12
Portuguese	15
Russian	16
Simplified Chinese	3
Traditional Chinese	4







# 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, page 145](#)

### 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 been set for deletion by the user, but you will need to contact the Cisco Technical Assistance Center (TAC) to retrieve the recording.

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.



#### Note

---

If a user inadvertently deletes a recording from the Cisco WebEx Meeting Recordings page but the recording is saved on the Network File System (NFS) storage server, contact the Cisco Technical Assistance Center (TAC) for assistance in recovering the recording.

---





## SNMP MIBs and Traps Supported

This section describes the MIBs available on your system. When you access your MIB data you will expose additional MIBs not listed in this section. The additional MIBs you expose through the process are primarily used internally for things like inter-virtual machine management. Cisco does not support customer-side SNMP monitoring that uses these MIBs, nor is there any guarantee that these MIBs will be used in future releases of Cisco WebEx Meetings Server.

- [Supported SNMP MIBs, page 147](#)
- [Supported SNMP Traps, page 151](#)

### Supported SNMP MIBs

The following sections describe the SNMP MIBs supported by Cisco WebEx Meetings Server.

#### Cisco WebEx Meetings Server System Information

Object	Type	Read/Write Privileges	OID	Description
cwCommSystemVersion	String	RO	.1.3.6.1.4.1.9.9.809.1.1.1	This object provides the version of the WebEx system.
cwCommSystemObjectID	AutonomousType	RO	.1.3.6.1.4.1.9.9.809.1.1.2	This object provides the sysObjectID defined in SNMPv2-MIB.

## CPU-Related MIBs

Object	Type	Read/Write Privileges	OID	Description
cwCommCPUTotalUsage	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.1.1	This object provides the total percentage of CPU usage of a host component. The total CPU usage contains CPU user usage, CPU system usage, and CPU nice usage. The CPU user time: CPU time spent in user space. The CPU system time: CPU time spent in kernel space. The CPU nice time: CPU time spent on low priority processes.
cwCommCPUUsageWindow	Gauge32	RW	.1.3.6.1.4.1.99.809.1.2.1.2	This object controls the duration (in seconds) to wait before sending notification (trap) after a CPU usage threshold is crossed. The notification is sent only if CPU usage crosses a threshold level (normal/minor/major) and remains in the new threshold level over the duration defined in this window.
cwCommCPUTotalNumber	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.1.3	This object provides the total number of CPUs on the system.
cwCommCPUUsageTable	n/a	Not accessible	.1.3.6.1.4.1.99.809.1.2.1.4	A list of CPU usage registering on the device.
cwCommCPUIndex	Unsigned32	RO	.1.3.6.1.4.1.99.809.1.2.1.4.1.1	This object uniquely identifies a CPU in the table. Each CPU has its own usage and breakdown values.
cwCommCPUName	String	RO	.1.3.6.1.4.1.99.809.1.2.1.4.1.2	This object provides the CPU name. For example, Intel(R) Xeon(TM) CPU 3.00GHz.
cwCommCPUUsage	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.1.4.1.3	This object provides the percentage of total CPU resources used. Usually GHz is used for measuring CPU power. Since GHz is too large for measuring some CPU usage categories, KHz is used as the measuring unit. The system speed (in KHz) multiplies by the fraction of each CPU section (for example, idle, nice, user) to get the CPU KHz of each category. KHz is used as the unit for all the CPU categories below.

Object	Type	Read/Write Privileges	OID	Description
cwCommCPUUsageUser	Gauge32	RO	.136.14.199.809.12.14.14	This object provides the CPU power executed in user mode.
cwCommCPUUsageNice	Gauge32	RO	.136.14.199.809.12.14.15	This object provides the CPU power executed on low priority processes. Nice is a program found on Unix and Linux. It directly maps to a kernel call of the same name. Nice is used to invoke a utility or shell script with a particular priority, thus giving the process more or less CPU time than other processes.
cwCommCPUUsageSystem	Gauge32	RO	.136.14.199.809.12.14.16	This object provides the CPU power executed in kernel mode.
cwCommCPUUsageIdle	Gauge32	RO	.136.14.199.809.12.14.17	This object provides the CPU power in idle status.
cwCommCPUUsageIOWait	Gauge32	RO	.136.14.199.809.12.14.18	This object provides the CPU power used when waiting for disk I/O to complete.
cwCommCPUUsageIRQ	Gauge32	RO	.136.14.199.809.12.14.19	This object provides the CPU power used when handling an interrupt request.
cwCommCPUUsageSoftIRQ	Gauge32	RO	.136.14.199.809.12.14.10	This object provides the CPU power used when handling a software interrupt request.
cwCommCPUUsageSteal	Gauge32	RO	.136.14.199.809.12.14.11	This object provides the CPU power used on other tasks when running in a virtualized environment.
cwCommCPUUsageCapacityTotal	Gauge32	RO	.136.14.199.809.12.14.12	This object provides the current total CPU power.
cwCommCPUMonitoringStatus	String	RO	.136.14.199.809.12.15	This object provides the monitoring status of CPU resources: <ul style="list-style-type: none"> <li>• closed (0)—Resource not available.</li> <li>• open(1)—Resource is available.</li> </ul>
cwCommCPUCapacityTotal	Gauge32	RO	.136.14.199.809.12.16	This object provides the overall CPU capacity.

**Cisco WebEx Meetings Server Memory Information**

Object	Type	Read/Write Privileges	OID	Description
cwCommMEMUsage	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.2.1	This object indicates the physical memory usage of the virtual machine.
cwCommMEMMonitoringStatus	String	RO	.1.3.6.1.4.1.99.809.1.2.2.2	This object provides the monitoring status of the memory resource: <ul style="list-style-type: none"> <li>• closed (0)—Resource not available.</li> <li>• open(1)—Resource is available.</li> </ul>
cwCommMEMTotal	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.2.3	This object provides the total physical memory size (in KB) of the host.
cwCommMEMSwapUsage	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.3.1	This object provides the host's physical memory usage (in percentage) and swap memory usage.
cwCommMEMSwapMonitoringStatus	String	RO	.1.3.6.1.4.1.99.809.1.2.3.2	This object provides the monitoring status of memory and swap memory. <ul style="list-style-type: none"> <li>• closed (0)— The memory and swap memory status is available.</li> <li>• open(1)— The memory and swap memory status is not available.</li> </ul>

**Disk Usage**

Object	Type	Read/Write Privileges	OID	Description
cwCommDiskUsageCount	Gauge32	RO	.1.3.6.1.4.1.99.809.1.2.5.1	This object provides the count of how many disks (for example, local disk, remote disk, meeting recording disk) available in the system.

Object	Type	Read/Write Privileges	OID	Description
cwCommDiskUsageIndex	Gauge32	RO	.136.14.1.99.809.1252.11	This object is an index of entries in the table that contain management information generic to the disk usage.
cwCommDiskPartitionName	String	RO	.136.14.1.99.809.1252.12	This object provides the disk partition name. For example, the partition /opt or /dev.
cwCommDiskUsage	Gauge32	RO	.136.14.1.99.809.1252.13	This object provides the current disk usage (in percentage) on the host.
cwCommDiskTotal	Gauge32	RO	.136.14.1.99.809.1252.14	This object provides the total disk space size (in MB) of this host.
cwCommDiskMonitoringStatus	String	RO	1.3.6.1.4.1.99.809.1.2.5.3	This object provides the monitoring status of disk resources. <ul style="list-style-type: none"> <li>• close (0)—The disk usage status is not available.</li> <li>• open (1)—The disk usage status is available.</li> </ul>

## Supported SNMP Traps

The following sections describe the SNMP traps supported by Cisco WebEx Meetings Server.

### Notification Events

The following are supported notification events.

Name	OID	Description
cwCommSystemResourceUsageNormalEvent	.1.3.6.1.4.1.99.8090.1	<p>This notification indicates that some system resource usage changes to the normal status. System could send out this notification once one of the following cases happens:</p> <ol style="list-style-type: none"> <li><b>1</b> The cwCommCPUUsage value of one CPU changes to be less than the value of pre-defined CPU Minor Threshold.</li> <li><b>2</b> The value of cwCommMEMUsage changes to be less than the value of pre-defined MEM Minor Threshold.</li> <li><b>3</b> The value of cwCommMEMSwapUsage changes to be less than in the value of pre-defined MEM SwapMinor Threshold.</li> <li><b>4</b> The value of cwCommFileUsage changes to be less than the value of pre-defined File Minor Threshold.</li> <li><b>5</b> The value of cwCommDiskUsage on one disk changes to be less than the value of pre-defined Disk Minor Threshold.</li> </ol>



Name	OID	Description
cwCommSystemResourceUsageMinorEvent	.1.3.6.1.4.1.99.809.02	<p>This notification indicates that some system resource usage changes to the minor status. System could send out this notification once one of the following cases happens:</p> <ol style="list-style-type: none"> <li><b>1</b> The cwCommCPUUsage value of one CPU changes to be larger than or equal to the value of pre-defined CPU Minor Threshold and be less than the value of cwCommCPUMajorThreshold.</li> <li><b>2</b> The cwCommMEMUsage value changes to be larger than or equal to the value of the pre-defined MEM Minor Threshold and be less than the value of pre-defined MEM Major Threshold.</li> <li><b>3</b> The cwCommMEMSwapUsage value changes to be larger than or equal to the value of pre-defined MEM Swap Minor Threshold and be less than the value of pre-defined MEM Swap Major Threshold.</li> <li><b>4</b> The cwCommFileUsage value changes to be larger than or equal to the value of pre-defined File Minor Threshold and be less than the value of pre-defined File Major Threshold.</li> <li><b>5</b> The cwCommDiskUsage value of one disk changes to be larger than or equal to the value of pre-defined Disk Minor Threshold and be less than the value of pre-defined Disk Major Threshold.</li> </ol> <p>The minor notification means the system has some issues and the system administrator must resolve them.</p>

Name	OID	Description
cwCommSystemResourceUsageMinorEvent	.1.3.6.1.4.1.99.809.0.3	<p>This notification indicates that some system resource usage changes to the major status. System could send out this notification once one of the following cases happens:</p> <ol style="list-style-type: none"> <li>1 The cwCommCPUUsage value of one CPU changes to be larger than or equal to the value of pre-defined CPU Major Threshold.</li> <li>2 The cwCommMEMUsage value changes to be larger than or equal to the value of pre-defined MEM Major Threshold.</li> <li>3 The cwCommMEMSwapUsage value changes to be larger than or equal to the value of pre-defined MEM Swap Major Threshold.</li> <li>4 The cwCommFileUsage value changes to be larger than or equal to the value of pre-defined File Major Threshold.</li> <li>5 The cwCommDiskUsage value of one disk changes to be larger than or equal to the value of pre-defined Disk Major Threshold.</li> </ol> <p>The major notification means the system is in critical status, it needs the system administrator to take action immediately.</p>

### Trap Data

The following are supported trap data. Set your MIB filter to only receive the traps described below.

Name	OID	Textual Convention	Description
cwCommNotificationHostAddressType	.1.3.6.1.4.1.99.809.1.24.1	InetAddressType	This object represents the type of the network address made available through cwCommNotificationHostAddress.
cwCommNotificationHostAddress	.1.3.6.1.4.1.99.809.1.24.2	InetAddress	This object provides the host IP address sent with the notification.

Name	OID	Textual Convention	Description
cwCommNotificationResName	.136.14.199.809.1243	CiscoWebExCommSysRes	This object provides the system resource name which is sent with notification. It indicates the named system resource has over pre-defined warning levels.  0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. open file descriptor (no MIB data) 4. one of the cwCommDiskTotal
cwCommNotificationResValue	.136.14.199.809.1244	Unsigned32	This object provides the system resource percentage usage value with notification.
cwCommNotificationSeqNum	.136.14.199.809.1245	Counter32	This object provides sequence number. It is used for tracking the order of the notifications.

