CHAPTER 23

Cisco Collaboration Clients and Applications

Last revised on: November 6, 2009

> **Note** This chapter is new for the current release of this document. Cisco recommends that you read this entire chapter before attempting to deploy collaboration clients and applications in your Cisco Unified Communications System.

Cisco Collaboration Clients and Applications provide an integrated user experience and extend the capabilities and operations of the Cisco Unified Communications System. These clients and applications enable collaboration both inside and outside the company boundaries by bringing together, in a single easy to use collaboration client, applications such as online meetings, presence notification, instant messaging, audio, video, voicemail, and many more.

There are a number of collaboration clients and applications available, and each provides an architectural view, deployment considerations, planning, and design guidance around integration into the Cisco Unified Communications System. Use this chapter to determine which of the following collaboration clients and applications are best suited for your deployment:

- Cisco WebEx Connect

  Cisco WebEx Connect is a collaborative software-as-a-service (SaaS) platform that enables developers, partners, and customers to create powerful collaborative business solutions that can extend their reach through collaborative solutions. Cisco WebEx Connect provides an open and extensible collaboration platform for enforcing enterprise-class security, scalability, performance, and availability, while delivering transparent communication with the Cisco Unified Communications solution. Cisco WebEx Connect contains two main components, the Cisco WebEx Connect Client and the Cisco WebEx Connect Platform.

- Cisco Unified Personal Communicator

  Cisco Unified Personal Communicator is a desktop application that allows users to easily access voice, video, web conferencing, instant messaging, voicemail, and presence information from a rich media interface on their desktop (PC or Mac). Cisco Unified Personal Communicator enhances productivity between teams and allows knowledge workers to collaborate anytime, anywhere, and easily escalate their communications through an easy-to-use user interface. For additional information, see the chapter on Cisco Unified Presence, page 22-1.

- Cisco Unified Mobile Communicator

  Cisco Unified Mobile Communicator is a mobility solution that gives users the ability to access and leverage Cisco Unified Communications applications from their mobile phones. The Cisco Unified Mobile Communicator and Cisco Mobile graphical clients work in conjunction with a server running the Cisco Unified Mobility Advantage software to provide a rich user interface for accessing and controlling mobile phone features and functionality. The system integrates into existing corporate LDAP directories, allowing users to use a single set of credentials across all devices. For more information, refer to the chapter on Cisco Mobility Applications, page 25-1.

Cisco WebEx Connect Architecture

Cisco WebEx Connect consists of two main components, Cisco WebEx Connect Client and Cisco WebEx Connect Platform. Cisco WebEx Connect provides an open and extensible collaboration platform for enforcing security, scalability, performance, and availability.

Cisco WebEx Connect Client

The Cisco WebEx Connect client is a rich client that resides on an end user's personal computer and provides a number of features. The Cisco WebEx Connect client can be installed on any personal computer running Microsoft Windows XP, Vista, or Windows 7 Operating Systems. Currently the Apple Macintosh and Linux operating systems are not supported.

Cisco WebEx Connect site administrators can use Single Sign On rather than creating separate user IDs and passwords for their end users, to allow end users to authenticate and sign in to Cisco WebEx Connect. For more information on Single Sign On with WebEx Connect, refer to the *WebEx Connect: User Provisioning and SSO* Developer Technical Note, available at

http://developer.webex.com/c/document_library/get_file?folderId=11835&name=DLFE-244.pdf

Presence

Cisco WebEx Connect (starting with the C6 release) leverages the Extensible Messaging and Presence Protocol (XMPP) for presence. XMPP is an open technology for real-time communications, and it powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data. For more information on XMPP, refer to the following sources:

- XMPP Standards Foundation at http://www.xmpp.org/
- XMPP Community pages at http://www.jabber.org/

XMPP has been adopted as the standard for most other instant messaging and presence networks, allowing Cisco to federate the Cisco WebEx Connect Presence information with other presence clouds supporting XMPP. The advantage to Cisco WebEx Connect users is that they can easily add users from other networks in their IM contact list and see their presence through federation. For more information on federating presence to other networks, refer to the Design Considerations for Cisco WebEx Connect, page 23-10.

The end-user's presence status is maintained by the Cisco WebEx presence servers in the Cisco WebEx Collaboration Cloud.

Instant Messaging

Users can send secure instant messages to other Cisco WebEx Connect users as well as to users on other instant messaging platforms. Cisco WebEx Connect users can easily escalate from their instant messaging session to a PC-to-PC VoIP call, an audio conference, a video conference, a desktop sharing session, or a WebEx meeting. Cisco WebEx Connect users can also transfer files to each other during an instant messaging session.

Instant messaging sessions between Cisco WebEx Connect users are secure, and the communication from the client to the Cisco WebEx Collaboration Cloud uses TLS encryption. TLS encryption is enabled by default by Cisco WebEx and cannot be turned off on a site-by-site basis by WebEx Connect site administrators. Furthermore, if desired, the instant messages themselves can be end-to-end encrypted using AES 256 bit encryption. All instant messaging sessions between Cisco WebEx Connect users and other XMPP clients are also encrypted using TLS encryption if the XMPP client supports encryption.

Spaces

Spaces provide team members an asynchronous collaboration environment. The main component is persistent group discussions and a SaaS-based document management system. Space owners can invite users from both inside and outside their corporate network to join their space. Spaces are known only to the members of a space. All content in the space is stored securely and encrypted inside the Cisco WebEx Collaboration Cloud.

Spaces are optional with Cisco WebEx Connect. Some customers may choose to provision Cisco WebEx Connect without spaces. For additional details on configuring spaces, refer to the *Cisco WebEx Connect Administrator's Guide*, available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Calendar Integration

Cisco WebEx Connect integrates with the Microsoft Outlook calendar that is running locally on the end user's computer. The Microsoft Outlook client on the end user's computer must be configured to communicate either with Microsoft Exchange Server or with Cisco WebEx Mail. If the end user has only webmail, Microsoft Outlook Web Access (OWA), or Cisco WebEx webmail, then calendar integration will not work.

Cisco WebEx Meeting Center Integration

Integration between Cisco WebEx Meeting Center and Cisco WebEx Connect can be enabled by specifying certain configuration information in the Cisco WebEx Connect client or in the Cisco WebEx Connect domain administration pages. When this integration is enabled, you can schedule Cisco WebEx Meeting Center meetings directly from Cisco WebEx Connect, allowing users to easily schedule and start WebEx web meetings from their Cisco WebEx Connect client. The Cisco WebEx Meeting Center integration can be set by an organization administrator or in the client by the end user.

To learn how to set Cisco WebEx Meeting Center as the administrator, refer to the documentation at

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17673.htm

Cisco Unified Communications Integration

Cisco WebEx Connect can be configured for Click-to-Call with Cisco Unified Communications Manager directly from within Cisco WebEx Connect. Cisco Unified Communications can be integrated into Cisco WebEx Connect in one of two ways, depending on your deployment topology and needs:

- Cisco WebEx Connect Unified Communications Widgets (Click-to-Call using CTI WebDialer, Voicemail, and Speeddail)
- Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect

Cisco WebEx Connect Unified Communications Widgets

Cisco WebEx Connect Unified Communications Widgets (CTI WebDialer, Voicemail, and Speeddial) run within the Cisco WebEx Connect widget framework and communicate with a web application via a REST interface (JSON/HTTPs). The web application provides a LDAP web service for LDAP queries using REST, a presence login service for login and presence management via REST, speed dial access via AXL/SOAP, and an administration point to provide configuration of back-end systems.

The CTI WebDialer widget gives users click-to-call integration and capabilities. Numbers (4 digits and greater) in Cisco WebEx Connect are hyperlinked, and users can click on the number to start a call without entering the phone number on the phone keypad. CTI monitoring must be enabled on Unified CM, and Unified CM integration must be enabled on the WebEx Connect administration pages.

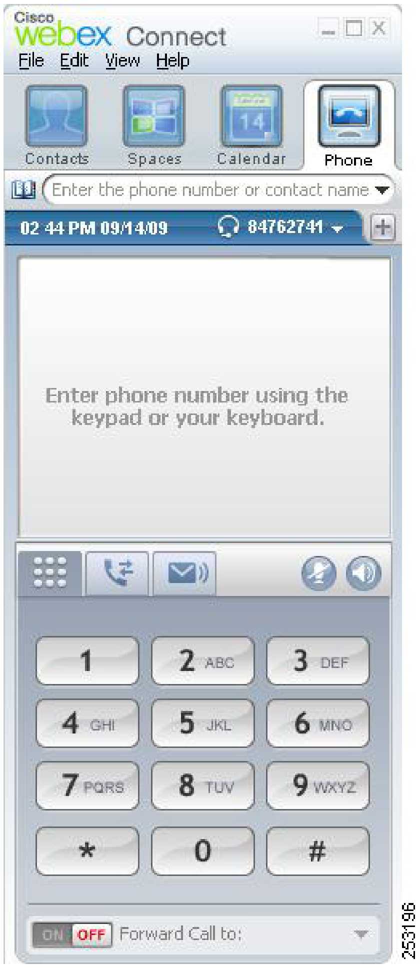
For more information on how to configure the Cisco WebEx Connect administrator pages, refer to:

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_singleptprov.htm

Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect

Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect provides for tight integration between Unified CM and Cisco WebEx Connect through the Client Services Framework to enable full call control inside the Cisco WebEx Connect client. The Client Services Framework allows for softphone call control where the desktop client serves as the audio endpoint, or it allows for desk phone control where the desktop client controls the Cisco Unified IP Phone, and in both cases it is represented by the Phone tab within WebEx Connect (see Figure 23-1).

Figure 23-1 WebEx Connect User Interface



Contacts are populated and used for click-to-call capability in the following ways:

- Click on any hyperlinked number that appears inside WebEx Connect. If this number is a valid extension or a valid number, Cisco Unified Communications Integration^{TM} will send a command to Unified CM to place the call with the end-user's IP phone if using desk phone integration or with the local PC if using softphone integration.
- Search for a contact name in the personal address book of Microsoft Outlook on the PC, or type in a phone number using the directory box in the softphone. The user needs to enter only a phone number or contact name, highlight the number, and then press dial.
- Manually call from the IP phone if using desk phone integration or from the local dial pad if using softphone integration. Call control will still be available from the WebEx Connect client.

Cisco WebEx Connect Platform

The Cisco WebEx Connect Platform is a multi-tenant Software-as-a-Service (SaaS) platform for synchronous and asynchronous collaboration. The WebEx Connect Platform is hosted inside the Cisco WebEx Collaboration Cloud.

For more information on the Cisco WebEx Software-as-a-Service offering, refer to

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

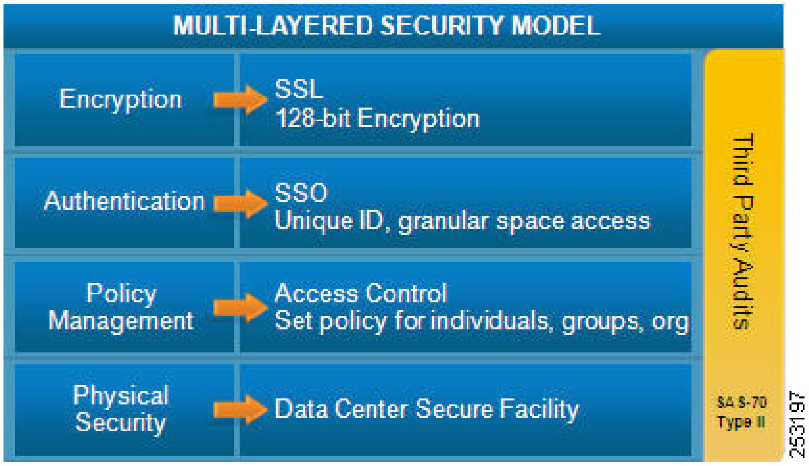
For more information on the Cisco WebEx Collaboration Cloud, refer to

http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html

Security

Figure 23-2 illustrates the separate but interrelated elements that compose the functional layers of the WebEx security model.

Figure 23-2 WebEx Security Model



The bottom layer represents the physical security in the Cisco WebEx data centers. All employees go through an extensive background check and must provide dual-factor authentication to enter the datacenter.

The next level is policy management, where the WebEx Connect organization administrator can set and manage access control levels by setting different policies for individual users, groups, or the entire Cisco WebEx Connect organization. Black or white list policies, specific to external users or domains, can be created to restrict or allow instant messaging exchanges. The Cisco WebEx Connect organizational model also allows for the creation of specific roles and groups across the entire user base, which allows the administrator to assign certain privileges to roles or groups as well as to set policies, including access control, for the entire organization.

Access to Cisco WebEx Connect is controlled at the authentication layer. Every user has a unique login and password. Passwords are never stored or sent over email in clear text. Passwords can be changed only by the end-users themselves. The administrator can choose to reset a password, forcing the end-user to change his or her password upon the next login. Alternatively, an administrator may choose to use the Single Sign On (SSO) integration between Cisco WebEx Connect and the company's Active Directory to simplify end-user access management.

The encryption layer ensures that all instant messaging communications between Cisco WebEx Connect users is encrypted using the TLS encryption protocol. All instant messaging communications between Cisco WebEx Connect users and users of other XMPP clients is encrypted by default using TLS encryption. Voice calls using Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect in PC (softphone) mode can be encrypted using Secure Real-time Transport Protocol (SRTP). These settings can be controlled by the Cisco WebEx Connect site administrator or by the end user in the Cisco WebEx Connect client settings under the Unified Communications tab.

Cisco WebEx Connect Platform uses third-party audits such as the SAS70 Type II audit to provide customers with a independent semi-annual security report. This report can be reviewed by any customer upon request with the Cisco Security organization.

Cisco WebEx Connect Deployment

Cisco WebEx Connect can be deployed in a highly available redundant topology. Deployment of Cisco WebEx Connect Software-as-a-Service architecture consists of various network and desktop requirements described in this section.

High Availability

The benefit of using a multi-tenant Software-as-a-Service architecture is that any failure of an individual server in a group allows for transparent routing of requests to another available server in the Cisco WebEx Connect Platform.

The Cisco WebEx Network Operations Team provides 24x7 active monitoring of the Cisco WebEx Collaboration Cloud from the Cisco WebEx Network Operations Center (NOC). For a comprehensive overview of the Cisco WebEx technology, refer to the information at

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

Redundancy, Failover, and Disaster Recovery

Cisco WebEx's Global Site Backup architecture handles power outages, natural disaster outages, service capacity overload, network capacity overload, and other type of service interruptions. Global Site Backup supports both manual and automatic failover. The manual failover mode is typically used during maintenance windows. The automatic failover mode is used in case of real-time failover due to a service interruption.

Global Site Backup is automatic and transparent to the end users, is available for all users, and imposes no limits on the number of users that can fail-over.

Global Site Backup has three main components:

- Global Site Service — is responsible for monitoring and switching traffic at the network level.
- Database Replication — ensures that the data transactions occurring on the primary site are transferred to the backup site.
- File Replication — ensures that any file changes are maintained in sync between the primary and the backup site.

Network Requirements

WebEx Connect is a Software-as-a-Service application. The end user PC must be connected to the Internet for the end user to be able to log in to WebEx Connect. A standard Internet connection is all that is required. If an end user is remote, he or she does not have to connect through the company VPN to log in to WebEx Connect.

Capacity and Bandwidth Requirements

A single end-user requires only a 56 kbps dial-up Internet connection to be able to log in to WebEx Connect and get the basic capabilities such as presence, instant messaging, and VoIP calling. However, for a small office or branch office, a broadband connection with a minimum of 512 kbps is required in order to use the advanced features such as file transfer, video conferencing, and team spaces.

Desktop Requirements

The WebEx Connect client is currently supported on Microsoft Windows client only. Table 23-1 lists the minimum desktop requirements to install and run Cisco WebEx Connect.

Table 23-1 Minimum Desktop Requirements to Install and Run Cisco WebEx Connect

Component	Cisco WebEx Connect with IM and Presence Only	Cisco WebEx Connect with IM, Presence, and Spaces	Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect
Operating System	Windows XP SP3 Windows Vista 32- bit	Windows XP SP3 Windows Vista 32-bit	Windows XP SP3 Windows Vista 32-bit
CPU	Intel Pentium Processor	Intel Pentium processor (1.8 GHz)	Intel Pentium Processor (2.4 GHz)
Disk Space	80 MB	80 MB	200 MB
Browser	Internet Explorer 6.0/7.0 Mozilla Firefox 3.0	Internet Explorer 6.0/7.0 Mozilla Firefox 3.0	Internet Explorer SP2 for XP Internet Explorer 7 for Vista Mozilla Firefox 3.0
I/O Ports	USB 2.0 (for video camera)	USB 2.0 (for video camera)	USB 2.0 (for video camera)
Email Program (Make sure you have selected the Cisco WebEx Connect setting that allows you to integrate with Microsoft Outlook.)	Microsoft Outlook 2003 or 2007	Microsoft Outlook 2003 or 2007	Microsoft Outlook 2003 or 2007
Audio	Full-duplex sound card and a headset	Full-duplex sound card and a headset	Full-duplex sound card and a headset
Video	At least 1.8 GHz CPU, 800x600 resolution, 256 colors or more, and a webcam	At least 1.8 GHz CPU, 800x600 resolution, 256 colors or more, and a webcam	At least 1.8 GHz CPU, 800x600 resolution, 256 colors or more, and a webcam

Ports and IP Address Ranges

Cisco WebEx Connect uses ports 80 and 443. By default, third-party XMPP clients use port 5222 for XMPP communications. Table 23-2 and Table 23-3 list the ports used with Cisco Unified Communications Integration™ for Cisco WebEx Connect.

Table 23-2 Ports Used for Inbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	How Cisco Unified Communications Integration™ for Cisco WebEx Connect Uses the Port
16384 to 32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. These ports are configured in Cisco Unified Communications Manager. For more information about device configuration files, see the *Cisco Unified Communications Manager System Guide*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 23-3 Ports Used for Outbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	How Cisco Unified Communications Integration™ for Cisco WebEx Connect Uses the Port
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file.
389	TCP	Connects to the LDAP server for contact searches.
2748	TCP	Connects to the CTI gateway, which is the CTIManager component of Cisco Unified Communications Manager.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	TCP	Provides secure SIP call signaling.
8443	TCP	Connects to the Cisco Unified Communications Manager IP Phone server to get a list of currently assigned devices.
8191	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.
16384 to 32766	UDP	Sends RTP media streams for audio and video.

Cisco WebEx services are offered over the following IP address ranges: 66.163.32.0 to 66.163.63.25 and 209.197.192.0 to 209.197.223.255. Cisco does not recommend configuring any access control lists (ACLs) based on these ranges because Cisco WebEx may reassign IP addresses from time to time.

Firewall Domain White List

Access control lists should be set specifically to allow all communications from the webex.com and webexconnect.com domains and all sub-domains for both webex.com and webexconnect.com. The WebEx Connect Platform sends emails to end-users for username and password communications. These emails come from the mda.webex.com domain.

Instant Messaging Logging

Cisco WebEx Connect instant messaging communications are logged on the local hard drive of the personal computer where the user is logged in. Instant message logging is a capability in Cisco WebEx Connect that can be enabled through the Org Admin tool. If instant message logging is enabled for Cisco WebEx Connect, instant messages are logged and kept in the following path:

file:///c:/Documents and Settings/user/*_Connect/Archive/_username*

The end-user can set logging specifics, whether to enable or disable logging, and how long the logs are kept. These settings are located under General IM in the Cisco WebEx Connect client settings.

The Cisco WebEx Connect Advanced Auditor that was available in previous releases of Cisco WebEx Connect is not compatible with the C6 release of Cisco WebEx Connect. Customers looking for advanced auditing and e-discovery capabilities should consider third-parties solutions. Currently Cisco does not provide support for advanced auditing and centralized logging of instant messaging communications.

Design Considerations for Cisco WebEx Connect

Cisco WebEx Connect design and deployment consists of interfacing with the Cisco WebEx Connect Client and Cisco WebEx Connect Platform in addition to Cisco Unified Communications Manager and third-party applications. When deploying Cisco WebEx Connect, use the design considerations described in the following sections.

One Unified CM Integration per Managed Connect Domain

In the current release of WebEx Connect, all end users on the same managed Connect domain have to use the same Unified CM integration. The Connect roadmap calls for the creation of sub-groups of end-users; and once these sub-groups are enabled, the administrator can assign a different Unified CM integration to different sub-groups.

Unified CM CTI Manager

When integrating with Cisco Unified Communications Widgets for Cisco WebEx Connect, only click-to-call is available from the CTI WebDialer. No other call flow and call control capabilities are available.

Refer to the chapter on Call Processing, page 8-1, for supported maximum CTI limits. The CTI numbers are key when using CTI WebDialer with the Cisco Unified Communications Widgets for Cisco WebEx Connect, as well as for desk phone control mode with the Cisco Unified Communications Integration^{TM} for Cisco WebEx Connect.

Third-Party XMPP Clients Connecting to Cisco WebEx Connect Platform

While Cisco does not officially support any other XMPP clients to connect to the Cisco WebEx Connect Platform, the nature of the XMPP protocol is to allow end-users to connect to presence clouds with various XMPP clients. A list of XMPP software clients is available at

http://xmpp.org/software/clients.shtml

Organization policies cannot be enforced on third-party XMPP clients, and features such as end-to-end encryption, desktop share, video calls, PC-to-PC calls, and teleconferences are not supported with third-party clients. To allow non-WebEx Connect XMPP IM clients to authenticate to your Connect domain(s), DNS SRV records must be updated. The specific DNS SRV entry can be found in the Cisco WebEx Connect site administration space, under Configuration and IM Federation.

The use of non-Connect XMPP clients in the Cisco WebEx Connect site administration space, under Configuration and XMPP IM Clients, must be explicitly allowed.

Instant Message and Presence Federation Using Third-Party XMPP Clients

The Cisco WebEx Connect network can federate with XMPP-based instant messaging networks such as GoogleTalk and Jabber.org. A list of public instant messaging networks based on XMPP is available at

http://xmpp.org/

WebEx Connect can federate with IBM Lotus Sametime through the IBM Lotus Sametime XMPP gateway, and with Microsoft Office Communications Server through the Microsoft Office Communications Server XMPP gateway. When using these third-party XMPP gateways, the configuration must be enabled at the back end of the IBM Lotus Sametime and Microsoft Office Communications Server deployments. Cisco does not officially support these configurations, nor does Cisco guarantee interoperability between clients.

Currently WebEx Connect does not interoperate with Yahoo! Messenger and Windows Live Messenger, but it can federate with AIM through a federation gateway.

Other Resources and Documentation

The *Cisco WebEx Connect Administrator's Guide* is available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

The Cisco WebEx Connect end-user guide is available at

http://www.webex.com/webexconnect/help/wwhelp/wwhimpl/js/html/wwhelp.htm