Main page: Cisco Unified MeetingPlace, Release 7.1

Previous page: System Requirements

Contents

- 1 Media Server Administration
- 2 Cisco Unified Communications Manager Requirements
- 3 Cisco Security Agent (CSA)
- 4 McAfee VirusScan Enterprise
- 5 Directory Service Requirements
- 6 License Requirements
- 7 Reservationless Single Number Access (RSNA) Requirements
- 8 Cisco Unified MeetingPlace Conference Manager Requirements
    - 8.1 Restrictions

Media Server Administration

The Media Server Administration pages require Internet Explorer 6 or Internet Explorer 7.

Cisco Unified Communications Manager Requirements

Cisco Unified MeetingPlace Release 7.1 requires Cisco Unified Communications Manager (CUCM) Release 6.1(2) or later using standard SIP Trunk configuration.

- Directory Services was tested against CUCM Release 6.1.5, 7.1.5, 8.0.2, 8.5 and 8.6.
- Media Server and Video Interoperability were tested against CUCM Release 7.1.5, 8.0, 8.5 and 8.6.
- The telephone user interface was tested against CUCM 6.1.5, 7.1.5, 8.0, 8.6.

Cisco Unified Communications Manager Release 6.1.x is automatically included with new sales shipments of Cisco Unified MeetingPlace Release 7.1. Upgrades do not inlude UC Manager software.

Note: Cisco Unified MeetingPlace Release 7.1 MR1 was tested against and supports CUCM-SME Release 8.5.

In the following cases, you may connect Cisco Unified MeetingPlace to Cisco Unified Communications Manager Release 6.0(3) or later release:

- Video installations in which only Cisco Unified Video Advantage is used
- Audio-only installations

Cisco Security Agent (CSA)

Cisco Unified MeetingPlace Release	CSA version for Application Server	CSA version for Web Server
Release 7.1	Release 6.0.1.112	Release 6.0.1.140

For information about Cisco Security Agent, see http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html.

McAfee VirusScan Enterprise

Cisco Unified MeetingPlace supports the following on the Web Server:

- McAfee VirusScan Enterprise versions 8.0i and later
- McAfee VirusScan Enterprise versions 8.7i and later as included in the McAfee Endpoint Protection Suite

If you install McAfee VirusScan Enterprise 8.7i or later, make sure that you uncheck the following settings in the Access Protection Rules (found in the Access Protection Properties window) so that Cisco Unified MeetingPlace Web will function properly:

- **Prevent programs registering as a service** found in the Common Maximum Protection category
- **Protect Cached files from password and email...** (4th Option) in the Anti-virus Maximum Protection category
- **Protect network settings** found in the Common Standard Protection category

If you are deploying an SMA-2S configuration, make sure that you also uncheck **Prevent HTTP Communication** found in the Common Maximum Protection category. Unchecking this setting ensures that the internal site will be able to communicate with the DMZ site.

To find out more information about McAfee VirusScan Enterprise use this link http://www.mcafee.com/us/products/virusscan-enterprise.aspx

Directory Service Requirements

Directory Service enables the system to populate and synchronize the Cisco Unified MeetingPlace user database with the Cisco Unified Communications Manager user database. The Cisco Unified Communications Manager user database is typically integrated with an LDAP directory, the following of which are supported by Cisco Unified MeetingPlace Directory Service:

- Microsoft Windows Active Directory 2000
- Microsoft Windows Active Directory 2003
- Microsoft Windows Active Directory Windows 2008
- Netscape Directory Server Version 4.*x*
- iPlanet Directory Server Version 4.*x*
- SunONE Directory Server Version 5.*1*
- Sun Java Version 5.2

- Novell eDirectory Release 4.x, 5.x, 6.x

  Note: Novell eDirectory requires a custom configuration. See http://www.novell.com/coolsolutions/appnote/16752.html for information about Novell eDirectory Release 4.x and http://www.novell.com/communities/node/3028/ for information about Novell eDirectory Release 5.x and 6.x.

License Requirements

Cisco Unified MeetingPlace requires licenses depending on the features you use. For a list of all the licenses, see About Licenses.

Reservationless Single Number Access (RSNA) Requirements

- To use Cisco Unified MeetingPlace with RSNA, you must use Cisco Unified Communications Manager Release 6.1.3 or later.
- A maximum of two Cisco Unified MeetingPlace Release 7.1 systems may be deployed with the RSNA configuration with no Application Server redundancy at this time.
- A single Cisco Unified Communications Manager cluster must be configured to process both inbound and outdial calls to both Cisco Unified MeetingPlace RSNA systems. If the RSNA systems are in different locations, they share an IP address and hostname for database replication and the same VLAN must be configured to work in both data sites.
- Web conferencing may be used with RSNA, but Cisco does not recommend it because the Web Servers connected to the two RSNA Application Servers operate independently. Cisco Unified MeetingPlace Web Conferencing URLs will be different on the two RSNA systems. Accessing the wrong URL will result in the meeting not being found. It is up to the System Administrator to make sure users know which web conferencing server to access for their meetings. Meetings are accessed on a web server using the profile number of the host user.
- The following maximum ports are possible:
  - 3000 audio (1500 on each system in the high capacity mode)
  - 2000 Web (1000 on each system)
  - 240 or 480 video (160 or 300 on each system) if the system has 12 (2x6) audio blades and 12 (2x6) video blades
- Cisco Unified MeetingPlace RSNA does not currently support Cisco WebEx.

Cisco Unified MeetingPlace Conference Manager Requirements

Restrictions

- Sun Java JRE 6 update 16 and update 18 are not supported. Prior versions (updates) are supported. Later versions (updates) are supported if latest Conference Manager hotfix is installed.