

Release Notes for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0)

Published July 28, 2006

These release notes contain information on new and changed support, new and changed functionality, limitations and restrictions, and open and resolved caveats for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0).

You can access the latest software upgrades for all versions of Cisco Unified MeetingPlace SMTP E-Mail Gateway on the Cisco Software Center website at <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.

Contents

These release notes contain the following sections:

- [System Requirements, page 2](#)
- [Related Documentation, page 2](#)
- [New and Changed Requirements and Support—Release 5.4\(11.0\), page 2](#)
- [New Functionality—Release 5.4\(11.0\), page 3](#)
- [Changed Functionality—Release 5.4\(11.0\), page 3](#)
- [Installation and Upgrade Information, page 3](#)
- [Caveats, page 4](#)
- [Obtaining Documentation, page 6](#)
- [Documentation Feedback, page 7](#)
- [Cisco Product Security Overview, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 10](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© <year> Cisco Systems, Inc. All rights reserved.

System Requirements

This section contains the following information:

- [Requirements for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4, page 2](#)
- [Compatibility Information, page 2](#)

Requirements for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4

System Requirements for Cisco Unified MeetingPlace Release 5.4 contains the most current information on SMTP E-Mail Gateway requirements. The document is available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.

Compatibility Information

- For information about the compatibility of SMTP E-Mail Gateway Release 5.4 with other Cisco Unified MeetingPlace components, refer to the “Cisco Unified MeetingPlace Component Compatibility Matrix” section in the “Introducing Cisco Unified MeetingPlace” chapter of the *Installation Planning Guide for Cisco Unified MeetingPlace Release 5.4* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.
- Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4 is not compatible with Cisco Security Agent. We recommend that you do not install Cisco Security Agent on a gateway server where SMTP E-Mail Gateway Release 5.4 is or will be installed.

If Cisco Security Agent is installed on an end-user system, users will see a security alert when they attempt to use the application-sharing feature. Users can choose to proceed with the feature and use application-sharing without difficulty.

Related Documentation

For descriptions and locations of Cisco Unified MeetingPlace documentation on Cisco.com, see the *Documentation Guide for Cisco Unified MeetingPlace*. The document is shipped with Cisco Unified MeetingPlace and is available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_documentation_roadmaps_list.html.

New and Changed Requirements and Support—Release 5.4(11.0)

This section contains information about new and changed requirements and support in the Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0) time frame only. Refer to the release notes of the applicable version for information on new and changed support with earlier versions of SMTP E-Mail Gateway. Release notes for all versions of SMTP E-Mail Gateway are available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

WORKING DRAFT -- CISCO CONFIDENTIAL

Cisco Unified MeetingPlace Audio Server 5.4 Support

You can use this release of the Cisco Unified MeetingPlace SMTP E-Mail Gateway with Audio Server Release 5.4.

New Functionality—Release 5.4(11.0)

This section contains information about new functionality for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0) only. Refer to the release notes of the applicable version for information on new functionality in earlier versions of SMTP E-Mail Gateway. Release notes for all versions of SMTP E-Mail Gateway are available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

Logging Updates

When enabling verbose logging for the SMTP E-Mail Gateway on the Notification tab in the Cisco Unified MeetingPlace Gateway Configurations tool, you do not need to restart the SMTP E-Mail Gateway. (Note that when changing the verbose logging setting on the E-Mail Gateway tab, a restart is required.)

New Video Notification Tags

The following additional tags are available for video notifications:

- <!--#Cisco ListTerminals -->
- <!--#Cisco RadInSessionCtrlUrl -->
- <!--#Cisco MeetingCategory -->

The tags allow you to insert a list of invited video terminals, a hyperlink to Video Administration for Cisco Unified MeetingPlace for the meeting, or the meeting category.

Changed Functionality—Release 5.4(11.0)

There is no changed functionality for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0).

Refer to the release notes of the applicable version for information on changed functionality in earlier versions of SMTP E-Mail Gateway. Release notes for all versions of SMTP E-Mail Gateway are available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

Installation and Upgrade Information

- [Installing Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4 for the First Time, page 4](#)
- [Upgrading to Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4, page 4](#)

WORKING DRAFT -- CISCO CONFIDENTIAL

Installing Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4 for the First Time

We recommend that you install the SMTP E-Mail Gateway after installing Cisco Unified MeetingPlace Web Conferencing.

For instructions on installing the SMTP E-Mail Gateway, refer to the “Installing Cisco Unified MeetingPlace SMTP E-Mail Gateway” chapter of the *Administration Guide for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html.

Upgrading to Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4

Upgrading a legacy SMTP E-Mail Gateway system to Release 5.4 requires a legacy third-party Windows server with system specifications comparable to Cisco MCS specifications required for the same deployment. For information on Cisco MCS specifications, go to <http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html>.

To upgrade the SMTP E-Mail Gateway, use the installation instructions in the “Installing Cisco Unified MeetingPlace SMTP E-Mail Gateway” chapter of the *Administration Guide for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html.

Caveats

This section lists Severity 1, 2, and 3 caveats.

You can find the latest caveat information for Cisco Unified MeetingPlace SMTP E-Mail Gateway version 5.4(11.0)—in addition to caveats of any severity for any release—by using Bug Toolkit, an online tool available for customers to query defects according to their own needs. Bug Toolkit is available at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. For information on using Bug Toolkit, see the “Using Bug Toolkit” section on page 5.

**Note**

To access Bug Toolkit, you must be logged on to Cisco.com as a registered user.

This section contains caveat information for SMTP E-Mail Gateway Release 5.4(11.0) only. Refer to the release notes of the applicable version for caveat information for earlier versions of SMTP E-Mail Gateway. Release notes for all versions of SMTP E-Mail Gateway are available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

Open Caveats—Release 5.4(11.0)

Click a link in the Caveat Number column to view the latest information on the caveat in Bug Toolkit. (Caveats are listed in order by severity, then by component, then by caveat number.)

WORKING DRAFT -- CISCO CONFIDENTIAL

Table 1 Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0) Open Caveats

Caveat Number	Severity	Component	Description
CSCse56808	2	smtp-gateway	JPN: Corruption at Cisco ListInvitees tag in notification with JPN name
CSCse22561	3	smtp-gateway	WAV file not attach to email notification
CSCse48541	3	smtp-gateway	SMTP notification shows audio/web info for video only meeting
CSCse56817	3	smtp-gateway	Update notif is not sent when a video mtg is changed to audio/web mtg.
CSCse56863	3	smtp-gateway	Request to revise Japanese notification templates

Resolved Caveats—Release 5.4(11.0)

There are no resolved caveats for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.4(11.0).

Using Bug Toolkit

To access Bug Toolkit, you need an Internet connection, web browser, and Cisco.com user ID and password. For more detailed information on Bug Toolkit, click Help in any Bug Toolkit window.

To Use Bug Toolkit

- Step 1** Open your web browser and go to <http://www.cisco.com/cgi>.
- Step 2** Click the **Launch Bug Toolkit** link.
- Step 3** To look for information about a specific caveat, enter the ID number in the Enter Known Bug ID field. To view all caveats for a Cisco Unified MeetingPlace component, go to the “Search for Bugs in Other Cisco Software and Hardware Products” section, and enter **meetingplace** in the Product Name field.
- Step 4** Click **Next**. The Cisco Unified MeetingPlace search window displays.
- Step 5** Choose the filters to query for caveats. You can choose any or all of the available options:
 - a.** Choose the Cisco Unified MeetingPlace version:
 - Choose the major version for the major releases (such as 5.3 or 5.4). A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.
 - Choose the revision for more specific information. A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.
 - b.** Choose the Features or Components to query; make your selection from the Available list and click **Add** to place your selection in the Limit Search To list.

To query for all Cisco Unified MeetingPlace caveats for a specified release, choose **All Features** in the left window pane.



Note The default value specifies All Features and includes all of the items in the left window pane.

- c.** Enter keywords to search for a caveat title and description, if applicable.

WORKING DRAFT -- CISCO CONFIDENTIAL

Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- d. Choose the Set Advanced Options, including the following items:
 - Bug Severity Level—The default specifies 1-3.
 - Bug Status Group—Check the **Fixed** check box for resolved caveats.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.
 - e. Click **Next**. Bug Toolkit returns a list of caveats on the basis of your query.

You can modify your results by submitting another query and using different criteria. Or you can save your query for future use.
-

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

WORKING DRAFT -- CISCO CONFIDENTIAL

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

WORKING DRAFT -- CISCO CONFIDENTIAL

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

WORKING DRAFT -- CISCO CONFIDENTIAL

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

WORKING DRAFT -- CISCO CONFIDENTIAL

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

WORKING DRAFT -- CISCO CONFIDENTIAL

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2006 Cisco Systems, Inc. All rights reserved.

WORKING DRAFT -- CISCO CONFIDENTIAL

WORKING DRAFT -- CISCO CONFIDENTIAL

WORKING DRAFT -- CISCO CONFIDENTIAL