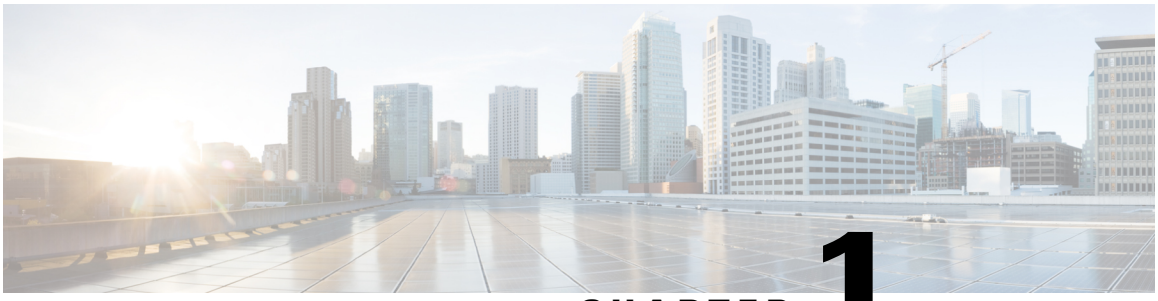
# Cisco WebEx Meetings Server Troubleshooting Guide Release 1.5

**First Published:** August 12, 2013

**Last Modified:** October 21, 2013

**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

# CONTENTS



CHAPTER 1

# Alarms, Logs, and Reports

This section includes troubleshooting topics about alarms, logs, and reports.



## Cannot Download Logs

**Problem** You cannot download your logs.

**Possible Cause** Your system is configured for SSL and you are using a Microsoft Internet Explorer version below 9. Internet Explorer below version 9 requires a specific header forcing it to cache downloaded files. It then deletes or never properly caches the files that you are attempting to save.

**Solution** Use Internet Explorer 9 or above. If you must use an older version of Internet Explorer, use the following solution: https://www.ibm.com/developerworks/mydeveloperworks/blogs/WCML2Thoughts/entry/internet_explorer_8_cannot_download_items_over_https_ssl_connection_with_ie8_ie_83?lang=en.

**Solution** Contact the Cisco TAC and set up a remote support account for the TAC to use to resolve the problem. Refer to "Setting Up a Remote Support Account" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

## Cannot Download Reports Using Microsoft Internet Explorer

**Problem** You cannot download reports when using Internet Explorer as your browser. You receive errors such as "Internet Explorer cannot download downloadReport from server. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later" or "File couldn't be downloaded."

**Possible Cause** Internet Explorer has the setting "Do not save encrypted pages to disk" enabled.

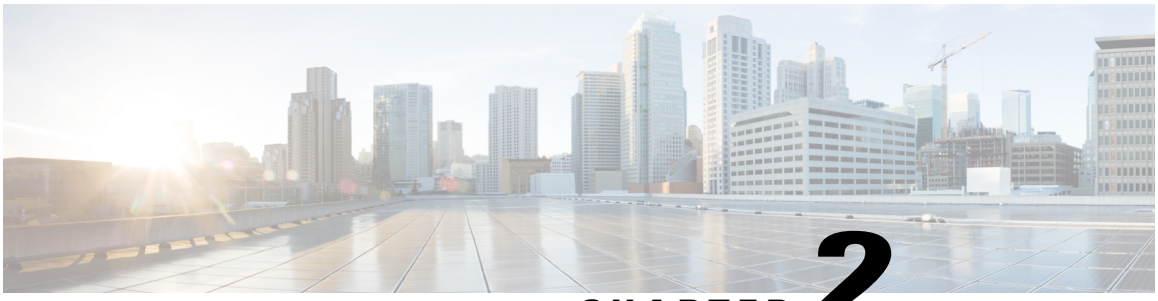
**Solution** Change your Internet Explorer security settings. Perform the following steps: Select **Tools** > **Internet Options** > **Advanced** > **Security** and deselect the "Do not save encrypted pages to disk" check box. Then select **OK**.

# Log Capture Size Problems

**Problem** The log capture size can become too large.

**Possible Cause** The log capture size can become too large, especially when obtaining logs from the archives. When obtaining logs from an archive, the log capture service gets the logs for an entire day even if you have selected only part of the day. The system was designed this way because unzipping the files can be a time-consuming process and can impact the performance of your system.

**Solution** Your log capture size can be minimized by selecting only the activities that you are trying to troubleshoot. The log capture size can also be minimized by performing a log capture as soon as you run into any issue, so that the log capture service does not have to go into the archives to obtain the logs.



CHAPTER 2

# Certificates

This section includes troubleshooting topics about certificates.



## Cannot Remove or Overwrite Existing Certificates

**Problem** You cannot remove or overwrite your existing certificate with a new one.

**Possible Cause** Cisco WebEx Meetings Server does not allow you to remove certificates but you can overwrite them. If you are unable to overwrite your certificate, SSO might be enabled.

**Solution** Sign in to the Administration site and disable SSO before you attempt to overwrite your certificate. Refer to "Disabling SSO" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

# Cannot Remove an SSO IdP Certificate

**Problem** You are unable to remove an SSO IdP certificate from your system.

**Possible Cause** The certificate format is incorrect.

**Solution** Upload new IdP certificates and make sure the certificate format is Base64 encoded X.509.

# Certificate Chain Error

**Problem** You receive a certificate chain error.

- **Possible Cause** One or more certificates are missing in the middle of the chain.
- **Possible Cause** The certificates are in the wrong order in the file.

- **Solution** Copy each individual certificate into a separate file.

- **Solution** Use your certificate viewer of choice (OpenSSL, Keychain) to examine the subject and issuer of each certificate to make sure the chain is complete.

- **Solution** Reorder the file correctly or add missing certificates and try again.

# Certificate Does not Match Private Key

**Problem** You receive an error message indicating that your certificate does not match the private key.

**Possible Cause** The private key that matches your certificate is no longer on your system. This can occur if you generated a second certificate signing request (CSR) or self-signed certificate, or performed any operation that changed hosts or URLs on your system.

**Solution** If you saved the private key that you downloaded from your system when you generated your CSR, you can upload that together with your certificate. Make sure the certificate is in PEM format. Open the saved private key file with a text editor and copy the private key. Include the -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY----- lines. Open your PEM-format certificate in a text editor and paste the private key at the top of the file, above the -----BEGIN CERTIFICATE----- line. Make sure there are no extra blank lines or text. Save this combined file and upload to your system. Note that if you changed hosts or URLs since generating your CSR, and you are using a SAN certificate, that certificate is no longer valid for your system. If you are using a wildcard certificate, you can perform this procedure. If you do not have the private key saved, you will need to generate another CSR and purchase a new certificate.

# Certificate Not Yet Valid Error

**Problem** You receive an error message indicating that your certificate is not yet valid.

**Possible Cause** The validity period of the certificate has not started yet.

- **Solution** Wait until the certificate becomes valid and upload it again.

- **Solution** Generate a new CSR and use it to obtain a new, valid certificate.

- **Solution** Ensure that the system time is correct.

# Expired Certificate Error

**Problem** You receive an expired certificate error.

**Possible Cause** The validity period of the certificate has ended.

**Solution** Generate a news CSR and use it to obtain a new, valid certificate. Ensure that the system time is correct.

# Incorrect X.509 Certificate to Validate SAML Assertion

**Problem** You receive the error message, "Incorrect X.509 certificate to validate SAML assertion. Contact your administrator for further support."

**Possible Cause** Your certificate or IdP is not valid.

**Solution** Validate your certificate or IdP as necessary.

# Invalid Certificate Error

**Problem** You receive an invalid certificate error.

**Possible Cause** The certificate file is malformed.

- **Solution** If uploading a PEM file, make sure there is no text or blank lines before the `-----BEGIN CERTIFICATE----` or after the `-----END CERTIFICATE-----`.

- **Solution** Make sure the certificate is in a supported format (X.509 in PEM, DER encoding or encrypted PKCS#12).

- **Solution** Generate a new CSR and use it to obtain a new, valid certificate.

# Invalid Domain Error—Wildcard Certificate

**Problem** You receive an invalid domain error message.

**Possible Cause** The user uploaded a wildcard certificate. One or more of the host names in the system or the site or admin URL are not in the same domain as specified in the common name of the certificate. When using a wildcard certificate, all hosts and URLs in the system must be in a single domain. If using multiple domains, you need a SAN certificate instead.

- **Solution** Check that you are using the correct certificate and upload it again.

- **Solution** Obtain a new certificate and upload it.

- **Solution** Examine the certificate using OpenSSL to see what domain is present in the certificate.

# Invalid Domain Error—SAN Certificate

**Problem** You receive an invalid domain error message.

**Possible Cause** The user uploaded a SAN certificate. The CN does not match the site URL.

- **Solution** Check that you are using the correct certificate and upload again.

- **Solution** Get a new certificate and upload again.

- **Solution** Examine the certificate using OpenSSL to see that all hosts are present.

# Key Decryption Error

**Problem** You receive a key decryption error.

- **Possible Cause** The key is encrypted and a password was not supplied.
- **Possible Cause** The key is encrypted and an incorrect password was supplied.
- **Possible Cause** The key is malformed.

- **Possible Cause** The key is not supported. Supported keys include PCKS#1, PKCS#8, encrypted PKCS#12.

- **Solution** Make sure that you are entering the correct password.

- **Solution** Try reading the key with OpenSSL.

# Key Size Error

**Problem** You receive a key size error message.

**Possible Cause** The user is trying to upload a private key and certificate or a certificate alone but the key length is too small.

**Solution** Obtain a new certificate and private key with a key size of at least 2048 bits. Use OpenSSL to verify the key length.

# Revoked Certificate Prevents Administration Site Access

**Problem** Your administrators and users cannot access the administration and end-user sites. The following error message is displayed: "There is a problem with this website's security certificate. This organization's certificate has been revoked."

**Possible Cause** You regenerated your private key and imported a revoked SSL certificate. After turning off maintenance mode, you see the following security alert: "The security certificate for this site has been revoked. This site should not be trusted."

**Solution** In Internet Explorer, select **Tools** > **Internet Options**, select the **Advanced** tab, and uncheck "Check for server certificate revocation." Regenerate and re-import your certificate. Refer to "Managing Certificates" in the *Cisco WebEx Meetings Server Administration Guide* for information on how to generate a new Certificate Signing Request (CSR), obtaining a certificate from a certificate authority, and importing the certificate to your system. Your administrators and users should be able to access the administration and end-user sites after you re-import your certificate.

# Self-Signed Certificate After Upgrade

**Problem** The system reverts to a self-signed certificate after a third-party certificate was uploaded.

**Possible Cause** You performed an upgrade, expansion, added high availability, changed a site URL, or a similar change.

**Solution** If the operation you performed changed the host names or URLs on your system, your existing certificate is no longer valid. Generate a new CSR and obtain a new certificate. If the operation did not change any host names or URLs, you might restore the private key and certificate by uploading them again.

# Cannot Establish TLS Due to Missing Extension in Certificate

**Problem** TLS cannot be established. When checking sniffing packets, it shows CUCM sends **Un-Support certificate** to Cisco WebEx Meetings Server during CUCM and Orion TLS handshaking.

**Possible Cause** CUCM check X509 Extended Key Usage in certificate.

**Solution** Use your certificate viewer of choice to ensure that your certificate authority has included the following extensions. If you find an extension is missing from your certificate, contact your certificate authority for assistance.

```
X509v3 Extended Key Usage:
TLS Web Server Authentication,
TLS Web Client Authentication
```

# Unable to Access Cisco WebEx Meetings Server from My Mobile Device

**Problem** I am unable to access Cisco WebEx Meetings Server from my mobile device.

**Possible Cause** Your self-signed certificate prevents you from accessing your system.

**Solution** Administrators who want to provide access to Cisco WebEx Meetings Server from mobile devices must send the certificate to all their users by email. Users will not be able to sign in without the certificate. In addition, some Cisco WebEx Meetings Server users might have certificates that are signed by a certificate authority that is not recognized by their mobile devices. *Instructions for administrators:* Sign in to the Administration site. Select **Settings** > **Security** > **Certificates**. Under SSL Certificate select **More Options**. Select **Export SSL Certificate**. The export process creates a file called CAcert.pem.txt. Rename this file with a .pem extension (for example, CAcert.pem). Email this .pem file to your users (Note that your users must be able to access the email on their mobile devices.). Make sure to include the following instructions to your users in the body of the email. *Instructions for end-users:* Open the .pem attachment to this email. On the **Install Profile** page, select **Install**, and then select **Install** again to confirm. Attempt to sign in to your Meetings application on your mobile device after making these changes.

# Untrusted Connection

**Problem** You receive an untrusted connection message. The client might not be able to verify the Cisco WebEx Meetings Server certificate using its truststore. Microsoft Internet Explorer uses the operating system truststore. Mozilla Firefox uses its own built-in truststore. To view Windows trusted root certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx.

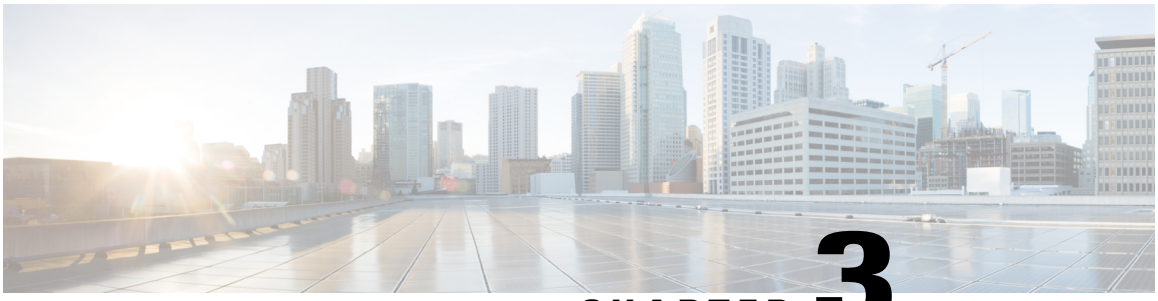
**Possible Cause** The system is using a self-signed certificate. This may occur because the system is a new installation or the customer had an existing certificate but performed an operation which invalidated that certificate and the system generated a self-signed certificate in its place.

**Solution** Purchase a certificate from a well-known certificate authority and upload it to the system. "Well known" means that the certificate authority's root certificate is in the truststore of all your browsers.

**Possible Cause** The issuer of the Cisco WebEx Meetings Server certificate is not trusted by the client.

- **Solution** Make sure that the issuer of the certificate is in your client's truststore. In particular, if you use a private or internal certificate authority, you are responsible for distributing its root certificate to all your clients or each client can add it manually.

- **Solution** Upload an intermediate certificate to Cisco WebEx Meetings Server. Sometimes, while the issuer of the certificate is an intermediate certificate authority that is not well known, it's issuer, the root certificate authority, is well known. You can either distribute the intermediate certificate to all clients or upload it to Cisco WebEx Meetings Server together with the end entity certificate.



CHAPTER 3

# Cisco Jabber

This section includes troubleshooting topics related to Cisco Jabber.



## Can't Connect to a WebEx Meeting Using Cisco Jabber

**Problem** I am having difficulty using Cisco Jabber to connect to a WebEx meeting.

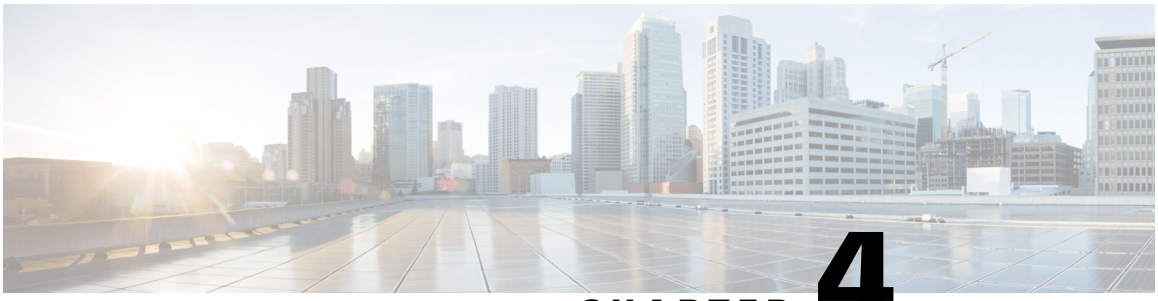
**Possible Cause** Cisco Unified Communications Manager IM and Presence server or Cisco Unified Presence server were not properly configured for the Cisco Jabber integration, or the user has entered an incorrect site URL or user credentials.

- **Solution** Administrators should check that port 443 is open. Cisco Jabber connects to Cisco WebEx Meetings Server through this port.

- **Solution** Administrators should ensure that the Cisco Unified Communications Manager IM and Presence server or Cisco Unified Presence server is properly configured and each user has a conferencing profile. The administrator adds the site URL to a conferencing server configuration on the presence server, and then adds that server configuration to a conferencing profile. Administrators can then associate users with that conferencing profile. When Cisco Jabber connects to the presence server, it gets the details from the conferencing profile. For more information see *Set Up On-Premises Deployments with Cisco Unified Communications Manager* in the Cisco Jabber for Windows Server Setup Guide or *Set Up Servers* in the Cisco Jabber for Windows Installation and Configuration Guide at http://www.cisco.com/en/US/products/ps12511/prod_installation_guides_list.html depending on the presence server you are using.

- **Solution** Verify that Jabber for Windows is operating properly. For more information about Jabber for Windows, refer to http://www.cisco.com/en/US/products/ps12511/prod_installation_guides_list.html.

- **Solution** Users should confirm with the Administrator that the site URL and the credentials they are using are correct. Administrators can verify user credentials by referencing the user's conferencing profile.



CHAPTER 4

# Directory Integration

This section includes troubleshooting topics about directory integration.



## A User Cannot Sign In After Directory Integration is Configured

**Problem** A user cannot sign in after directory integration is configured.

**Possible Cause** There is a problem with the user's Active Directory account.

**Solution** Check your Active Directory Server to see if the user has an account and if it is active.

**Possible Cause** The user's email account might not be valid.

**Solution** Check if the user has a valid email account. The accepted format is abc@mydomain.com.

**Possible Cause** The user might not be configured in your CUCM directory.

**Solution** Make sure the user is in your users list in CUCM. Users can sign in even when the user is not imported into your Cisco WebEx Meetings Server database yet. When LDAP authentication is enabled and a user tries

to sign in, your system checks if the email address exists in the database (local or remote user). If the user exists, it checks for the field *ADUserID* in the database for this user. This field is populated after performing a directory synchronization. If this field is empty, then your system checks the CUCM database to see if this user exists there. If the user exists in the CUCM database, it updates the *ADUserID* fields for this user record in the database and continues with authentication. Authentication succeeds as long as the user exists in the CUCM database and provides the correct credentials even though it was not previously synchronized using Directory Integration. After the first sign in, the user record is treated as an Active Directory synchronized user.

# All Users Cannot Sign in After Directory Integration

**Problem** All users cannot sign in after directory integration.

**Possible Cause** There might be a problem with your network.

**Solution** Check if there is a network connectivity problem between Cisco WebEx Meetings Server and CUCM or Active Directory.

**Possible Cause** Your CUCM AXL username and/or password have changed.

**Solution** Obtain the correct CUCM AXL username and/or password.

# User Unable to Sign In After Switching from SSO to LDAP Authentication

**Problem** A user is unable to sign in after switching from SSO to LDAP authentication.

**Possible Cause** SSO uses user IDs for authentication and LDAP uses user email addresses.

**Solution** Inform your user that he must use his email address to sign into his account.

# Some or All of Your Users are Unable to Sign In After Switching SSO to LDAP Authentication

**Problem** Some or all of your users are unable to sign in after you switched from SSO to LDAP authentication.

**Possible Cause** You have not performed a Cisco WebEx Meetings Server synchronization yet.

**Solution** Check to see if the affected users are already added into Cisco WebEx Meetings Server. If they are not, they cannot sign into the system.

**Solution** Sign in to the Administration site, select **Users** > **Directory Integration**, and perform a synchronization to import all active users from your CUCM Active Directory server to Cisco WebEx Meetings Server. After

you perform a synchronization, make sure to inform your users of the change and that they must use their email addresses to sign in. Refer to "Configuring Directory Integration" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

# An Administrator Cannot Sign in to the WebEx Site

**Problem** An administrator cannot sign in to the WebEx site.

**Possible Cause** There are problems with the administrator's credentials.

**Solution** Make sure the administrator has an account on the Active Directory server. The credentials on the WebEx site are different than those on the Administrator site.

# A User Added in Cisco WebEx Meetings Server Cannot Sign In

**Problem** A user added in Cisco WebEx Meetings Server cannot sign in.

**Possible Cause** You configured directory integration and enabled LDAP authentication.

**Solution** Make sure the user is configured in your Active Directory server and then synchronized with your Cisco WebEx Meetings Server system using the directory integration feature.

# A User's Account Might Not Be Used to Sign Into Cisco WebEx Meetings Server

**Problem** A user's account might not be used to sign into Cisco WebEx Meetings Server.

**Possible Cause** The credentials you use to sign into Jabber and other Unified Communications might be different than your WebEx site ID after you have configured directory integration. For example, after you enable LDAP authentication, your user ID becomes your email address.

**Solution** Inform your user that he must use his email address to sign into the WebEx site.

# You Cannot Activate a User

**Problem** You cannot activate a user.

**Possible Cause** The user was originally activated by CUCM Active Directory synchronization and is now deactivated.

**Solution** You cannot activate a deactivated user with the Cisco WebEx Meetings Server user management features if the user was originally deactivated by a CUCM Active Directory synchronization. Such users should be marked with an asterisk that indicates "User has been disabled on LDAP." You must activate the

user in Active Directory, perform a CUCM Active Directory synchronization, and then perform a directory integration synchronization.

**Possible Cause** The user was deactivated using Cisco WebEx Meetings Server user management. You activated the user on your CUCM Active Directory server and performed a synchronization but the user is still deactivated.

**Solution** Active the user by using the Cisco WebEx Meetings Server user management features. Sign into your Administration site, select **Users**, select the check box for the user you want to activate, and then select **Actions** > **Deactivate**.

# User Status is Not Updated After a Change is Made on Your Active Directory Server

**Problem** User status is not updated after a change is made in your Active Directory server.

**Possible Cause** You have not scheduled your Cisco WebEx Meetings Server synchronization to occur after your CUCM Active Directory synchronization. User status is updated in Cisco WebEx Meetings Server based on the user status that is configured in your Active Directory settings. For example, if a user is deleted from your Active Directory server, CUCM will mark this user as "Inactive" during the next synchronization and will delete this user after 24 hours. So if Cisco WebEx Meetings Server does not perform a synchronization within 24 hours, this user status will not be changed.

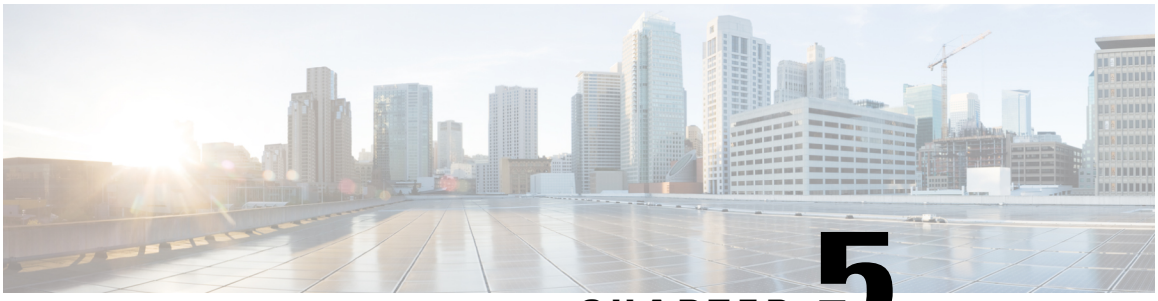
**Solution** Make sure you schedule your Cisco WebEx Meetings Server synchronization to occur after your CUCM Active Directory synchronization.

# A User Added to Active Directory Server Not Showing Up After Synchronization

**Problem** A user added to your Active Directory server is not showing up in your active users list after you perform a Cisco WebEx Meetings Server synchronization.

**Possible Cause** You might not have performed a CUCM Active Directory synchronization before your Cisco WebEx Meetings Server synchronization. CUCM does not communicate directly with Active Directory. After users are added, you must perform an Active Directory synchronization using CUCM before you synchronize your users with Cisco WebEx Meetings Server.

**Solution** To perform a CUCM Active Directory server synchronization, sign into your CUCM administration account and select **System** > **LDAP Directory**, and then select the **Perform Full Sync Now** button on the top menu. All new active users are imported to Cisco WebEx Meetings Server after the next directory integration synchronization.



CHAPTER 5

# Disaster Recovery

This section includes troubleshooting topics about disaster recovery.



## Audio Conferencing not Working after Disaster Recovery is Performed on a Two-Data-Center System

**Problem** On a secure teleconferencing system, your audio conferencing is not working after performing disaster recovery on a two-data-center system.

**Possible Cause** Your CUCM SIP trunk configuration must be updated. Before you perform the disaster recovery procedure, your application point and load balance point SIP trunks are configured with X.509 SIP trunk security profiles. At your first data center, your SIP trunks are configured with X.509 SIP trunk security profiles in that data center. At your second data center, your SIP trunks are configured with X.509 SIP trunk security profiles in that data center. Each SIP trunk security profile is indicated by its URL. After disaster recovery at your restored second data center is assigned the SIP trunk security profile URL of the first data center. This causes your audio conferencing features to fail. See the tables below for the required configurations for both data centers before disaster recovery.

***Table 1: First Data Center Configuration Before Disaster Recovery***

| SIP Trunk | SIP Trunk Security Profile: X.509 Subject Name |
|---|---|
| SIP trunk for a load balance point at your first data center | Site URL for your first data center (FQDN format) |
| SIP trunk for an application point at your first data center | Site URL for your first data center (FQDN format) |

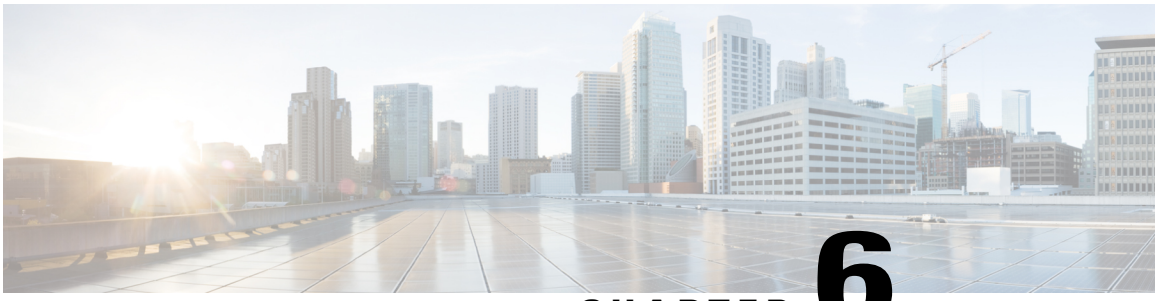
*Table 2: Second Data Center Configuration Before Disaster Recovery*

| SIP Trunk | SIP Trunk Security Profile: X.509 Subject Name |
|---|---|
| SIP trunk for a load balance point at your second data center | Site URL for your second data center (FQDN format) |
| SIP trunk for an application point at your second data center | Site URL for your second data center (FQDN format) |

**Solution** Launch CUCM and change the SIP trunk security profile for your second data center to the URL of the first data center in the X.509 Subject field. See the table below for the required configuration of your second data center after disaster recovery. Refer to the "Using the Disaster Recovery Feature" section of the *Cisco WebEx Meetings Center Administration Guide* for more information on disaster recovery. Refer to the "Configuring Cisco Unified Communications Manager (CUCM)" section of the *Cisco WebEx Meetings Center Planning Guide* for more information on configuring CUCM.

*Table 3: Second Data Center Configuration After Disaster Recovery*

| SIP Trunk | SIP Trunk Security Profile: X.509 Subject Name |
|---|---|
| SIP trunk for a load balance point at your second data center | Site URL for your first data center (FQDN format) |
| SIP trunk for an application point at your second data center | Site URL for your first data center (FQDN format) |



CHAPTER 6

# Downloading Applications

This section includes troubleshooting topics about downloading applications including the Cisco WebEx Productivity Tools, the Meetings application, and the Network Recording Player.



## Productivity Tool Download Automatic Sign In Unavailable with Firefox and Chrome Browsers

**Problem** If a user downloads the WebEx Productivity Tools from Internet Explorer, the WebEx site URL is pre-populated in the WebEx Assistant Application, thereby easing the process of end-user sign-in. However under Mozilla Firefox and Google Chrome this capability is not available.

- **Possible Cause** When the user downloads WebEx Productivity Tools using Internet Explorer, WebEx Assistant is able to read a browser cookie from the Internet Explorer browser cache that lets it uniquely identify the WebEx site and pre-populate that information in the sign-in screens.
- **Possible Cause** If a user downloads Productivity Tools using a browser other than Internet Explorer, the cookie information will be unavailable to WebEx Assistant since these browsers store cookies in an encrypted fashion, thereby making them accessible to desktop applications like WebEx Assistant.

1 **Solution** When the user initiates the download of WebEx Productivity Tools from the **Downloads** page, there are clear instructions given to users about how to manually sign-in to WebEx Assistant.

2 **Solution** If the above is a problem for your users we recommend pushing a silent installer to the desktops of your end-users. You can pre-populate one of the installation switches as part of a silent installation in the WebEx site URL. Refer to the *Cisco WebEx Meetings Server Deployment Guide* for more information.

# Signing into a SSO Site Using the Productivity Tools Fails

**Problem** You attempt to sign into your SSO-configured site using the Productivity Tools and your sign-in attempt fails.

**Possible Cause** Your IdP sign in might not support Internet Explorer 6.

**Solution** Add the following to your registry and attempt to sign in again using the Productivity Tools: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SCRIPTURL_MITIGATION | "ptoneclk.exe"=dword:00000001 | "outlook.exe"=dword:00000001 | ptWbxONI.exe"=dword:00000001 | ptUpdate.exe"=dword:00000001 | PTIM.exe"=dword:00000001 | ptSrv.exe"=dword:00000001

# Cisco WebEx Meetings Fails to Launch Due to Java Issues

**Problem** Your users experience intermittent failures to launch the Cisco WebEx Meetings application on Windows when they are connected to their corporate intranet using Cisco Any-Connect VPN Client. This failure occurs only when the user attempts to download and install the Cisco WebEx Meetings application the first time he tries to join a meeting. Once the application is installed on the user's PC this problem no longer occurs.

**Problem** This problem does not occur when the user attempts to join the meeting without VPN turned on (this assumes that the WebEx site is enabled for public access).

**Possible Cause** Your users are using an outdated version of Java.

**Solution** Update your end-user Windows desktops to the latest Java version. If this does not work, we recommend that you tell your users to manually install the Cisco WebEx Meetings application from the **Downloads** page. Alternatively users can download the Cisco WebEx Meetings application when they attempt to join the meeting for the first time. These workarounds assume that user PCs in your organization have administrator privileges. If they do not have administrator privileges, you can push the Cisco WebEx Meetings application to their PCs using the installation files provided on the **Download** page.

# Error 1316 Received During Application Installation

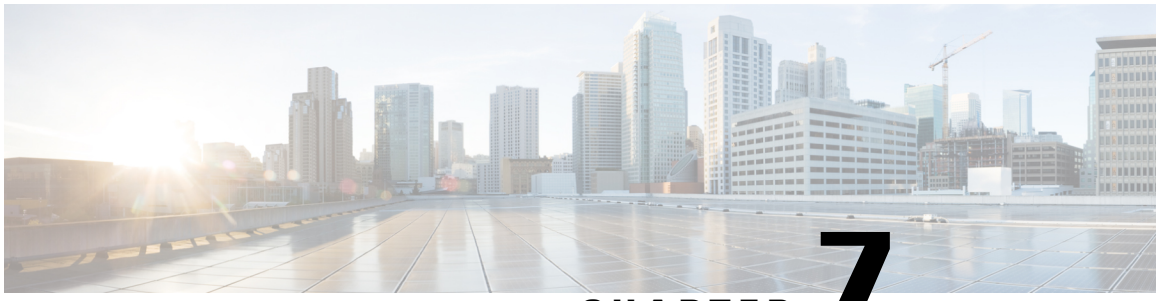
**Problem** You are installing one of the application downloads (Cisco WebEx Meetings, Productivity Tools, or Network Recording Player), the installation process stops, and you receive Error 1316.

**Possible Cause** You are attempting to install the same version of the application that is currently installed but the installer has a different name.

**Solution** Attempt one of the following actions to fix the problem:

- **Solution** Obtain an installer that includes the same version currently on your system but change the name displayed in the error message before attempting to reinstall it. Copy your modified installer to the path displayed in the error message.

- **Solution** Uninstall the existing application and then reinstall it.



CHAPTER 7

# Emails

This section includes troubleshooting topics about emails.



## Emails are not Being Received by Administrators and Users

**Problem** Emails are not being received by administrators and users.

**Possible Cause** Your SMTP hostname might be incorrectly configured.

**Possible Cause** Your SMTP server might be down.

**Possible Cause** SMTP server email requests might be blocked.

**Solution** Make sure your SMTP hostname is correctly configured. If it is not configured correct, put your system in maintenance mode and correct the SMTP information, save your changes and turn off maintenance mode. After your system restarts, the status should be UP. Refer to "Configuring an SMTP Server" in the Administration Guide for more information.

**Solution** Check your logs to determine if SMTP server email requests are being blocked. Fix your SMTP server issue or specify a different SMTP server.

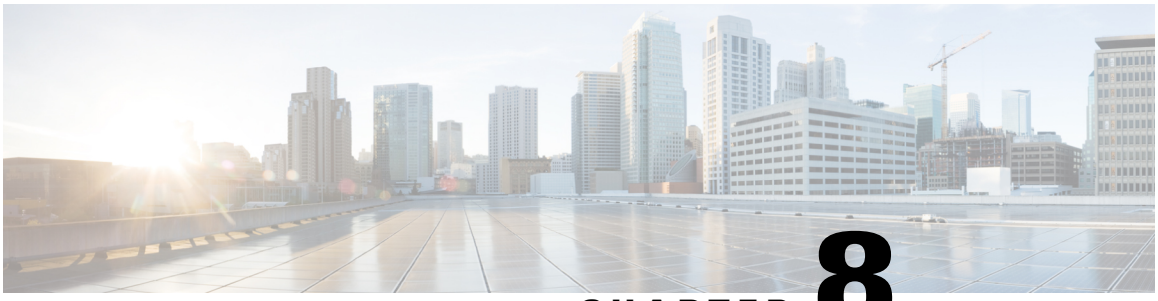
**Solution** You can test email by selecting **Users** > **Email Users** and then sending an email to a host.

## SMTP Email Server Issues on a System with TLS-Based Authentication

**Problem** My SMTP email server is not working.

**Possible Cause** TLS is enabled and your self-signed certificate is not accepted as valid by your system.

**Solution** This is a known limitation. You cannot configure your mail server to use a self-signed certificate with TLS enabled.



CHAPTER 8

# General

This section includes general troubleshooting topics.

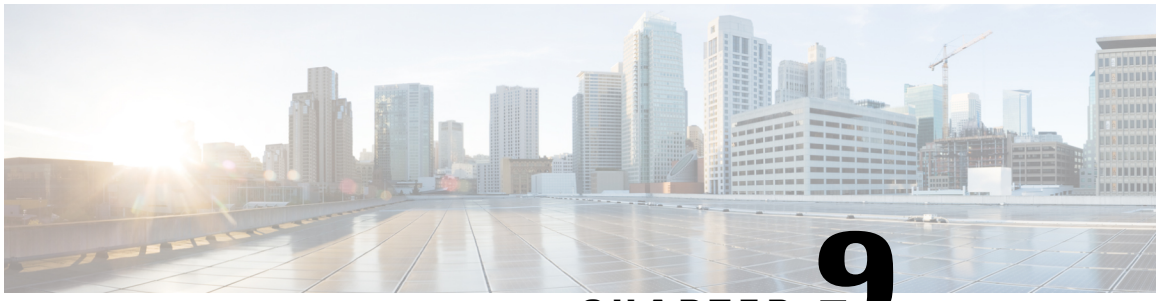


## You Are Seeing Text Fields with Angled Instead of Rounded Corners

**Problem** You are seeing text fields with angled corners instead of rounded.

**Possible Cause** You are using Microsoft Internet Explorer and your version settings are too low.

**Solution** Make sure you are in standard mode (not compatibility) and set to Internet Explorer 10. Specifically, make sure you are not set to Internet Explorer 7.



CHAPTER 9

# Installation and Deployment

This section includes troubleshooting topics about installation and deployment issues.



## Use of Forward Proxies in Your System

Although we do not recommend the use of intervening networking elements such as forward proxies between the client software (running on user desktops) and back-end system servers, we do not forbid their use with your system. We recommend you minimize such elements, as each intervening network element has the potential to introduce network latencies. These latencies result in a poor user experience for latency-sensitive aspects of Cisco WebEx meetings, including WebEx Video, Voice Connection using computer, and screen sharing. Intervening elements may affect the contents of each networking packet in unforeseeable ways, that could break these features.

If your end users experience these issues, we strongly recommend you remove intervening networking elements from your system then check if the problems are resolved.

**Note** Using forward proxies might interfere with quality-of-service (QoS) features.

### Performance Considerations

Proxies should not change the network traffic or add latencies into the overall flow of data in the system.

- The forwarding proxy should have less than 10 ms latency to process packets. It may be difficult for those forwarding proxies that check the packet content to process packets in under 10 ms. Long latencies negatively affect the audio, video, and data-sharing quality of the meeting experience for users. It may also affect the throughput between clients and servers because of the longer round trip time (RTT).
- The total latency should be controlled if there is more than one forwarding proxy between the virtual machines and the client.

### Functionality

- If caching mechanisms (such as cookie caching) are used in the forward proxy, then that may break the functionality of your system. In this situation, we suggest you disable caching, although this may impact the performance of the forwarding proxy.
- User-level authentication should be turned off at forward proxies.
- If the connection between the forward proxy and the Cisco WebEx Meetings Server system bypasses the system's Internet Reverse Proxy (for "internal" users), the forward proxy must allow the system to *redirect* https connections between the system's virtual machines, each of which has its own https URL. This redirection is not visible to the forward proxy if the Cisco WebEx Meetings Server Internet Reverse Proxy is placed between the proxy and the internal virtual machines.

### Supported Proxies

- http
- SOCKS v4

**Note** SOCKS v5 is not supported

# Use of Reverse Proxies in Your System

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 in any way. 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.

# Auto-Deployment Fails for error.deploy_summary.353

**Problem** The user receives the following error during auto-deployment:
Error: error.deploy_summary.353 = The image used to deploy the virtual machines may be corrupted. Please obtain a new copy of the OVA file and deploy all the virtual machines again.

**Possible Cause** The previously downloaded OVA is corrupted.

- **Solution** Check to determine if the OVA downloaded from Cisco contains the correct checksum.

- **Solution** Make sure the datastore where new virtual machines are being deployed is available and not actively running any applications.

- **Solution** Make sure there are no visible storage alarms seen in VMware vCenter.

# Auto-Deployment Fails for error.deploy_summary.363 and Auto-Deployment Fails for error.deploy_summary.365

**Problem** You receive one of the following two error messages: Auto-Deployment Fails for error.deploy_summary.363 or Auto-Deployment Fails for error.deploy_summary.365.

**Possible Cause** You cannot deploy to the selected virtual machine.

**Solution** Select **Start Over** to restart the deployment.

# Invalid Passphrase URL Error

**Problem** If the "Invalid Passphrase" message displays, it might be because the URL was entered incorrectly or the CWMS (primary or secondary) Admin virtual machine was rebooted during a deployment, changing the deployment URL.

**Solution** If the error is a result of the Admin virtual machine being rebooted, you must delete the Admin virtual machine in the vCenter, restart the deployment from the beginning, including redeploying the Admin virtual machine.

**Solution** If other virtual machines were connected during the deployment, you must also delete those virtual machines.

# End User Download Page is Broken After Completing An Update

**Problem** End users are not able to access download link.

**Possible Cause** Static resources are cached to enhance the performance of web pages. However, end users might be using a web browser that has an old version. Javascript files might be cached where the Javascript files are loaded from your local machine instead from the server.

**Solution** Users should clear their browser cache and try re-accessing the download page.

# Unable to Install Cisco WebEx Meetings Server Due to Unsupported Product Version

**Problem** Unable to install Cisco WebEx Meetings Server on my virtual machine.

**Possible Cause** Your version of VMware ESXi is not supported.

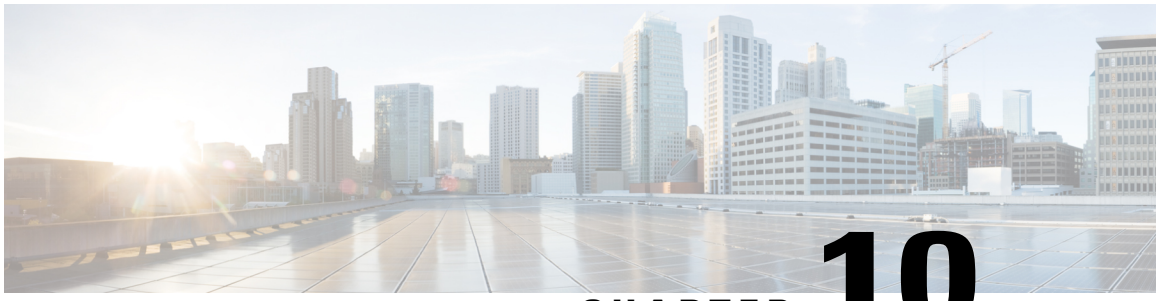
**Solution** Make sure you are using VMware ESXi 5.0 Update 1 or 5.1. Version 4.x is not supported.

# WebEx Meetings Plugin Installation in Microsoft Internet Explorer 8.0

**Problem** You receive an error message indicating that installation was unsuccessful when attempting to install the Meetings client.

**Possible Cause** The computer on which you are attempting to install the software does not have administrator privileges.

**Solution** Make sure that the computer has the most recent version of Cisco WebEx Meetings Server installed. Check if the computer has Windows Administrator Privileges. If it does not, that is causing the error message and failed installation. Obtain administrator privileges if possible. Make sure that the IE 8.0 Security Settings are set to their out-of-box defaults by selecting **Control Panel** > **Internet Options** > **Advanced** > **Reset**. If none of the above solve the problem, you must push the MSI Installer to the end-user desktop using a Windows Login script or similar method. You can access the MSI Packages for Meetings, Productivity Tools, and other applications from the Cisco WebEx Meetings Server Administration Site. Select **Settings** > **Downloads**. Refer to "Downloading and Mass Deploying Applications" in the *Cisco WebEx Meetings Server Planning Guide* for more information. If none of the above procedures solve the problem, contact the Cisco TAC for further assistance.



CHAPTER 10

# Licenses



## After High-Availability Failover, Your System Starts Free-Trial Mode

**Problem** After a high-availability failover, your system starts free-trial mode, giving you 180 days to restore your connection to Enterprise License Manager (ELM).

**Possible Cause** ELM only runs on your primary system. After failover, your high-availability system cannot connect with ELM.

**Solution** Reboot your primary system using VMware vCenter. Your system should reconnect to ELM automatically during the reboot process. If you still cannot connect with ELM after the reboot is complete, contact the Cisco TAC for additional assistance.

# Free Trial Alert Message Appears

**Problem** Your system indicates that it is running in free-trial mode on your Administration site.

**Possible Cause** After deploying your system, it is automatically placed in free-trial mode.

**Solution** Install licenses to end free-trial mode. Refer to the "Managing Licenses" section of the online help and *Administration Guide* for more information.

# Your License Usage has Exceeded the Number of Purchased Licenses

**Problem** You receive a licenses exceeded email.

**Possible Cause** Your license usage is exceeding the number of purchased licenses.

**Solution** Contact your Cisco sales representative and purchase a sufficient number of licenses to take usage to or below the number of installed licenses.

# Your License Usage has Exceeded the Number of Purchased Licenses and Your System Has Been Deactivated

**Problem** You receive an email indicating that your system has been deactivated due to a licenses exceeded condition.

**Possible Cause** You have exceeded the number of installed licenses for over six months.

**Solution** Contact your Cisco sales representative and purchase a sufficient number of licenses to take usage to or below the number of installed licenses.

# You Receive an Invalid Licenses Email

**Problem** You receive an email indicating that your system is operating with invalid licenses.

**Possible Cause** Your system cannot communicate with the License Server (ELM). If your system is configured for high availability, your primary system is not active, and your are using the failover system, the system is unable to communicate with the License Server.

**Solution** Reboot your primary system using VMware vCenter. Your system should reconnect to ELM automatically during the reboot process. If you still cannot connect with ELM after the reboot is complete, contact the Cisco TAC for additional assistance.

# You Receive an Invalid Licenses Email and Your System Has Been Deactivated

**Problem** You receive an email indicating that your system has been deactivated because you were operating with invalid licenses for over six months.

**Possible Cause** Your system cannot communicate with the License Server (ELM). If your system is configured for high availability, your primary system is not active, and your are using the failover system, the system is unable to communicate with the License Server.

**Solution** Reboot your primary system using VMware vCenter. Your system should reconnect to ELM automatically during the reboot process. If you still cannot connect with ELM after the reboot is complete, contact the Cisco TAC for additional assistance.

# You Cannot Access Cisco Enterprise License Manager (ELM) from Cisco WebEx Meetings Server

**Problem** Administrators cannot access ELM from Cisco WebEx Meetings Server.

**Possible Cause** During deployment, the Administration URL was configured with a less common top-level domains type such as ".infra."

**Solution** Use common top-level domain types such as ".com." This is a known issue and will be addressed in a future release of Cisco WebEx Meetings Server.

# Licensing Installation Fails with Multiple Browser Windows Open

**Problem** License installation fails.

**Possible Cause** Your Administration Site and ELM Administration pages are open on two different browser windows while both of them share same Administration Site URL.

**Solution** Make sure admin tab is closed, and click on Install button again. Sign into the Administration Site. Select **System** and then select **View More** in the Licenses section. Select **Manage Licenses** to open the ELM page. Close the original browser window that displays the **User Licenses** page. Select **Install License File** on the ELM page and proceed with your license installation. Refer to "Manage Licenses" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

# The Manage Licenses Button is Disabled

**Problem** The **Manage Licenses** button is disabled on the **User Licenses** page.

**Possible Cause** In a high-availability environment, your Administration site is running on a secondary virtual machine.

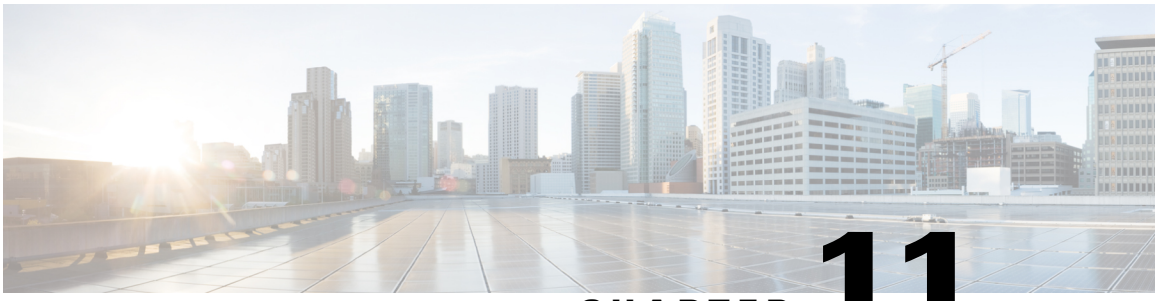
**Solution** Determine why your Administration site is running on your secondary virtual machine. Fix your primary system and reboot it from VMware vCenter. Your system should function normally after reboot.

# Out-of-Date License Alert Message

**Problem** You receive an out-of-date license alert message.

**Possible Cause** Your system version and license version do not match.

**Solution** Make sure you have installed the latest license version.



CHAPTER 11

# Maintenance Mode

This section includes troubleshooting topics about maintenance mode issues.



## Rebooting Message Does Not Go Away After You Turn Off Maintenance Mode

**Problem** After turning off maintenance mode, the rebooting message does not go away and your browser does not redirect you to the Administration sign-in page.

**Possible Cause** This is a known issue, but the cause is undetermined.

**Solution** Manually enter your Administration site URL to reach the sign-in page.

## Request to Turn Maintenance Mode On or Off is Rejected

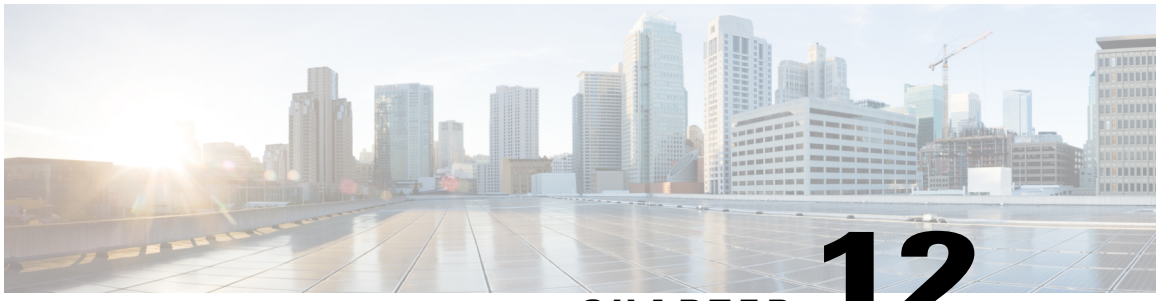
**Problem** Your request to turn maintenance mode on or off is rejected.

**Possible Cause** You selected the **Turn On Maintenance Mode** or **Turn Off Maintenance Mode** button too quickly.

**Solution** Wait a few seconds and select **Turn On Maintenance Mode** or **Turn Off Maintenance Mode** again.

**Possible Cause** There is already a system-altering change taking place (for example, adding or removing high-availability).

**Solution** Wait 30 minutes and select **Turn On Maintenance Mode** or **Turn Off Maintenance Mode** again.



CHAPTER 12

# Recordings

This section includes troubleshooting topics about recording issues.



## Cannot Start or Join Meetings or View Recordings Due to Unsupported Java Version

**Problem** Users cannot start or join meetings or view recordings on any browser.

**Possible Cause** Users are using unsupported Java versions.

**Solution** If you are using Microsoft Internet Explorer, enable ActiveX or install Java above 1.6.034 or above 1.7.06. If you are using Mozilla Firefox or Google Chrome, install Java above 1.6.034 or above 1.7.06 or download and reinstall your Cisco WebEx Meetings or Network Recording Player client manually. Then attempt to start or join a meeting or view a recording again.

## Meeting Recordings Missing on Host Recordings Pages

**Problem** Meeting recordings are not listed on the **Recordings** page for any host user, although the host had enabled recording in meetings.

**Possible Cause** There might be a permission issue on the storage server for the specific mount point that Cisco WebEx Meetings Server is pointing to on the storage server configuration page (on the Administration site select **System** > **Servers** > **Storage Server**).

**Solution** This is a known issue.

# Record Button Generates Server Connect Error

**Problem** When a meeting host attempts to click the record button inside the meeting room, the meeting client pops up an error indicating that it cannot connect to the recording server.

**Possible Cause** The Cisco WebEx Meetings Server Tomcat user cannot write to the mount point.

**Solution** Update privileges on the NAS mount point to `777` using `chmod R 777 <mount-point-directory>` if the storage server is running on Linux OS. Then attempt to attach the NAS server to Cisco WebEx Meetings Server again.

# Cannot Add a Storage Server

**Problem** You cannot add a storage server.

**Possible Cause** The Cisco WebEx Meetings Server Tomcat user cannot write to the mount point.

**Solution** Update privileges on the NAS mount point to `777` using `chmod R 777 <mount-point-directory>` if the storage server is running on Linux OS. Then attempt to attach the NAS server to Cisco WebEx Meetings Server again.

# Meeting Recording Does Not Display for Host

**Problem** The meeting host does not see the meeting recording on the **Recordings** page for more than 10 minutes after the recorded meeting ended.

**Possible Cause** Your NBR WSS has no privilege to read/write files to the storage server.

**Solution** If you are using a Linux storage server, enter the following command: `chmon -R 777` *mount point directory*. If you want to recover the meeting records that were not generated on the **Recordings** page, contact the TAC.

# The Record Button is Gray

**Problem** Meeting hosts cannot record meetings because the **Record** button is gray.

**Possible Cause** NAS is not attached to Cisco WebEx Meetings Server.

**Solution** Sign in to the Administration site, select **System** > **Servers**, select the **Add Storage Server** link and specify the NFS server and mount point. For example, 170.70.80.90:/*Path to mount point on server*.

**Possible Cause** Recording is not enabled on Cisco WebEx Meetings Server.

**Solution** Sign in to the Administration site, select **Settings** > **Meetings**, and check the **Record** box under Participant Privileges.

**Possible Cause** Your storage server's usage has reached its limit as specified in the **Alarms** page of the Administration site.

**Solution** Make sure that the storage capacity on NAS is being monitored on the **Alarms** page. Sign in to the Administration site, select **Dashboard** > **Alarms**, select the **Edit** link, check the **Storage** option, drag the slider for the storage limit on the **Edit Alarms** page on the dashboard, and select **Save**. Alternatively, you can delete files from the storage server mount point to create more space.

**Possible Cause** Your storage server has been stopped or NFS service on the NAS has been stopped or restarted, preventing Cisco WebEx Meetings Server from accessing the mount point.

**Solution** Sign in to the Administration site, select **System** > **Servers** > **Storage Server** and reconfigure NAS.

# Recording Panel Generates Error

**Problem** After a meeting recording is in progress for a while, the recorder panel shows an error. When you mouse over the panel, it shows an audio or video error.

**Possible Cause** The Cisco WebEx Meetings Server Tomcat user cannot write to the mount point.

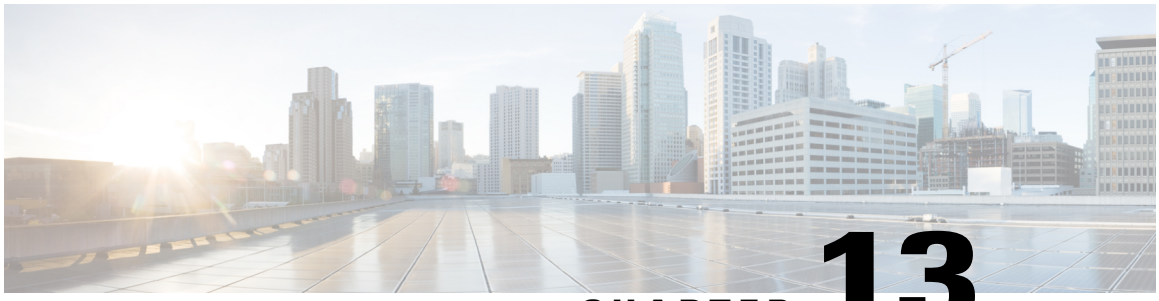
**Solution** Make sure that the mount point can be accessed and that Cisco WebEx Meetings Server can write to it.

# Recordings Do Not Show Up on the Recordings Page

**Problem** Recordings do not show up on the **Recordings** page for any host user even though the host has enabled recording in meetings.

**Possible Cause** There is a permissions issue on the storage server for the specific mount point that your system is pointing to.

**Solution** Sign in to your Administration site and select **System** > **Servers** > **Storage Server Configuration**. Make sure that your permissions are set correct.



CHAPTER 13

# Servers

This section includes troubleshooting topics about your mail and storage servers.



## SMTP Sends Failures When Administrator Email Uses an Underscore Character

**Problem** A user sends an email to the administrator and the email is returned as undeliverable.

**Possible Cause** Underscore characters are not supported for email addresses.

**Solution** Do not use underscore characters or other unsupported characters when sending emails to the administrator.

## External Server Connection Issues

**Problem** Administrators and users are not receiving emails from your system.

**Possible Cause** There might be a permissions issue on the storage server for the specific mount point that your system is pointing to (sign in to the Administration site and select **System** > **Servers** > **Storage Server**).

1 **Solution** Make sure that **sendmail** requests from the concerned Cisco WebEx Meetings Server are not blocked.

2 **Solution** Put your system into Maintenance Mode and correct the SMTP information on admin web. Save your changes and take the system out of Maintenance Mode. When the system finishes rebooting, the status should indicate "UP."

3 **Solution** Fix the SMTP server issue or specify a different SMTP server to work correctly with your system.

# NTP-Provisioned Time out of Sync on Virtual Machines

**Problem** An NTP alert is displayed at the top of the page shortly after the user logs in. The NTP provisioned times on each virtual machine are out of sync by three or more minutes.

**Possible Cause** The NTP provisioned times on each virtual machine are out of sync by three or more minutes.

1 **Solution** Wait to see if the message is cleared after times are synced.

2 **Solution** Confirm that ESXi hosts are configured with the correct DNS information and can reach the NTP host. For more information, refer to your VMware vSphere documentation.

# Your Storage Server is not Backing Up Your System or Recordings

**Problem** Your storage server is not backing up your system and meeting recordings.

**Possible Cause** Your storage server is unable to connect with a virtual machine on your system.

**Solution** Use VMware vSphere to configure your firewall settings. Refer to the "Networking Changes Required For Your Deployment" section in the *Cisco WebEx Meetings Server Planning Guide* for more information.

**Possible Cause** Storage server down. There is no connectivity to the server.

**Solution** Verify that the storage server is accessible from outside of Cisco WebEx Meetings Server. Verify that the storage server is powered on. Verify that there is network connectivity to the storage server. Verify if mount/access is possible from a non-Cisco WebEx Meetings Server machine. Verify that your storage server is not full.

CHAPTER 14

# Sign In and Meeting Issues

This section includes troubleshooting topics about sign in and meeting issues.

- User Cannot Access Product, page 50
- User is Dropped from Audio Conference, page 50
- WBX*INPROGRESSMEETING Table Does Not Record Data When Meeting Ends at Specific Time, page 51


# Account Activation Fails

**Problem** An administrator or user receives notification that his account has been activated but he is unable to sign into the account.

**Possible Cause** The account activation period has expired. After an account has been activated, administrators have two days and end-users have three days to sign in before the account deactivates.

**Solution** Go to your sign-in page and select the forgot password link to reset your account. When you receive your reset password email, follow the instructions to reset your password and sign into your account.

# Automatic Login Problems Occur After Cookies are Imported from Microsoft Internet Explorer

**Problem** A user checks the "Remember me" option after signing into Cisco WebEx Meetings Server on Microsoft Internet Explorer. If the user then installs Mozilla Firefox and imports all cookies from Internet Explorer, it causes the user to automatically sign in whenever he launches Firefox, even after signing out manually. When an administrator changes the authentication key on the Administration site or upgrades to a new version, it causes the user to always sign out of the site when he launches Firefox, even if he has checked on "Remember me" the last time he signed into Cisco WebEx Meetings Server.

**Possible Cause** Firefox adds a "." before the cookie domain name when importing cookies from Internet Explorer.

**Solution** Have your user clear his Firefox cookies manually.

# Browser Compatibility Issues

**Problem** You are using an Internet Explorer browser that is listed as compatible with this product but you receive a message that states your browser is not compatible.

**Possible Cause** A group policy setting on your system causes your browser to advertise that it is Internet Explorer 6 instead of Internet Explorer 8.

**Solution** If you are using Internet Explorer 8 for Windows XP with Service Pack 3, the incompatibility message is false and you can ignore it. You can prevent your system from sending this message by changing your compatibility settings. In Internet Explorer 8, select **Tools** > **Compatibility View Settings**. Remove the domain name of your Cisco WebEx Meetings Server from the list of web sites that you have added to your Compatibility View if it is present.

# Cannot Connect to WebEx Site or Administration Site

**Problem** You cannot connect to your WebEx site or Administration site using a browser that requires SSL 3.0.

**Possible Cause** FIPS is enabled which blocks SSL 3.0.

**Solution** Disable FIPS.

# Cannot Start or Join Meetings or View Recordings Due to Unsupported Java Version

**Problem** Users cannot start or join meetings or view recordings on any browser.

**Possible Cause** Users are using unsupported Java versions.

**Solution** If you are using Microsoft Internet Explorer, enable ActiveX or install Java above 1.6.034 or above 1.7.06. If you are using Mozilla Firefox or Google Chrome, install Java above 1.6.034 or above 1.7.06 or download and reinstall your Cisco WebEx Meetings or Network Recording Player client manually. Then attempt to start or join a meeting or view a recording again.

# Forwarded Meeting Invitations Do not Work After Upgrade

**Problem** A user schedules a meeting and then forwards the invitation to other participants. The participants are able to use the forwarded email to attend meetings initially but after the system is upgraded and they attempt to attend the meeting, they receive the error message, "The meeting does not exist or has already ended."

**Possible Cause** The upgrade procedure invalidates the meeting.

**Solution** After performing a system upgrade, inform your users that they must reschedule all meetings. Forward meeting emails as necessary.

# Graphics Quality Degrades When Application or Desktop Sharing is Used

**Problem** When I use the application sharing or desktop sharing features my graphics quality degrades.

**Possible Cause** When your system uses the application sharing or desktop sharing features, Cisco WebEx Meetings Server automatically disables certain graphics settings, including Aero mode and Clear-True Type.

**Solution** This feature is working as intended. After you stop using the application sharing or desktop sharing features, Cisco WebEx Meetings Server enables any graphics settings that it disabled during the use of those features.

# Join Before Host Meeting not Shown on Meetings Page

**Problem** A meeting configured with the "Join before host" option enabled is not showing up on your meetings page.

**Possible Cause** A user other than the host joined the meeting and then left before the host joined. On the Dashboard and Meeting Trends page, this meeting will be displayed with no participants.

**Solution** This is a known issue. If a meeting participant other than the host attends the meeting and then leaves before the host joins, the meeting is not recorded on the meetings page.

# Join Before Host Meeting Status is Incorrect

**Problem** You have enabled JMBH (join meetings before host) and JTBH (join teleconference before host) for your meetings. A meeting participant has joined a meeting only through the telephone but the Start button is still displayed on the **Meetings** page.

**Solution** This is a known issue. The system is waiting for the host to start the meeting on his web client or is still using the telephone to join the meeting for audio only.

# Cisco WebEx Meetings Fails to Launch Due to Java Issues

**Problem** Your users experience intermittent failures to launch the Cisco WebEx Meetings application on Windows when they are connected to their corporate intranet using Cisco Any-Connect VPN Client. This failure occurs only when the user attempts to download and install the Cisco WebEx Meetings application the first time he tries to join a meeting. Once the application is installed on the user's PC this problem no longer occurs.

**Problem** This problem does not occur when the user attempts to join the meeting without VPN turned on (this assumes that the WebEx site is enabled for public access).

**Possible Cause** Your users are using an outdated version of Java.

**Solution** Update your end-user Windows desktops to the latest Java version. If this does not work, we recommend that you tell your users to manually install the Cisco WebEx Meetings application from the **Downloads** page. Alternatively users can download the Cisco WebEx Meetings application when they attempt to join the meeting for the first time. These workarounds assume that user PCs in your organization have administrator privileges. If they do not have administrator privileges, you can push the Cisco WebEx Meetings application to their PCs using the installation files provided on the **Download** page.

# Maximum Meeting Capacity Exceeded

**Problem:**

The following error message displays when you attempt to join a WebEx meeting:

**You cannot join the meeting now because the number of concurrent users has reached the system's limit. Contact your administrator for further support.**

**Possible Cause:**

This error message displays if a participant attempts to join a meeting and exceeds the maximum number of concurrent users supported by your system.

**Solution:**

The audio portion of a WebEx meeting does not have a limit for the number of concurrent users. Once the maximum number of concurrent users have joined the WebEx meeting, the remaining users can dial in to the meeting and listen. However, exceeding the maximum number of supported users can cause performance issues.

# Meeting Issues Email Received

**Problem** You receive an email indicating that there are meeting issues.

**Possible Cause** There might be latency and jitter issues in the user's environment. Users, including those attending meetings through a virtual private network (VPN) might have limited network bandwidth.

**Solution** Sign into the Administration site, select **Dashboard**, and select the Meetings chart to see the **Meeting Trend** page. Examine the meetings that occurred at the date and time the Meeting Alert occurred. Look for meetings with a status of fair or poor. Note the meeting topic, host, and issue and contact the host to determine what the issue with the meeting was.

# Meeting Participants are Unable to Dial Out to Their Phones

**Problem** Meeting participants are unable to dial out to their phones. They receive a "failed to connect" error.

**Possible Cause** Your CUCM settings are configured incorrectly.

**Solution** Check your CUCM settings on the Audio page. Sign in to your Administration site and select **Settings** > **Audio** > **CUCM**. Make sure you have configured the correct IP addresses, transport, and port settings.

# Meeting Trend Data is One Hour Later on the One-Day and One-Week Charts

**Problem** On the **Meeting Trend** page, the data for one hour and one day charts is one hour later than that shown on the 1–6 month charts.

**Possible Cause** For the one-day and one-week Meeting Trend charts, future (scheduled) meeting data is computed every 4 hours. If you schedule a meeting, the meeting information is picked up during the four–hour interval.

**Solution** This is a known issue. Most scheduled meetings are recurring and we do not want to compute the information too frequently because it might impact system performance.

# Problem Launching a Meeting on Mozilla Firefox and Google Chrome Due to Inactive ActiveTouch General Plugin Container

**Problem** A user attempts to launch a meeting using Mozilla Firefox or Google Chrome and receives an error message such as the following: "We encountered a problem launching your meeting. Restart your web browser and try again, or join your meeting from a different web browser. If the problem persists, then contact your system administrator." Your browser gets stuck in a loop and fails to load Meeting Center.

**Possible Cause** The user disabled the ActiveTouch General Plugin Container on their browser.

**Solution** On Mozilla Firefox, have your user select **Tools** > **Add-ons** > **Plugins**, and enable **ActiveTouch General Plugin Container**, restart the browser, and try to attend the meeting again. On Google Chrome, have your user go to the URL, "chrome://plugins", enable **ActiveTouch General Plugin Container**, restart the browser, and try to attend the meeting again.

# Stuck on the "One Moment Please" Page When Trying to Start or Join a Meeting

**Problem** Users are stuck on the "One moment please..." page when attempting to start or join a meeting.

**Possible Cause** You are using Mozilla Firefox 18 and Firefox thinks that Java has a potential security issue and prompts the user to deactivate it. The user selects "Never activate plugins for this site." This causes Java to deactivate which disables users' ability to start or join a meeting with Java.

**Solution** If you believe there is a Java security issue, have your users start or join the meeting by either of the two methods listed on the page: Install the meeting application and then start or join the meeting again; or select **Run a temporary application** to start or join the meeting. If you do not believe there is a Java security issue, have your users clear their cookies, select **Always activate plugins for this site**, and then start or join their meeting using Java.

# A User Is not Able to Schedule Meetings with WebEx Assistant

**Problem** A user has downloaded WebEx Productivity Tools, but is not able to schedule meetings with WebEx Assistant.

**Possible Cause** The user might have multiple accounts configured in Microsoft Outlook.

**Solution** Instruct the user to remove the extra accounts and keep just one account in Microsoft Outlook that matches his or her Cisco WebEx profile.

# Users are Unable to Host or Attend Meetings

**Problem** A user is unable to host or attend a meeting.

**Possible Cause** The user has restricted PC permissions.

**Solution** Configure your system to manually push Cisco WebEx Meetings and Productivity Tools to the user's desktop. Select **Settings** > **Downloads** and select the **Manually push Cisco WebEx Meetings and Productivity Tools to user's desktop** option. See Configuring Your Download Settings for more information.

# Users Cannot Dial In to a Personal Conference Meeting

**Problem** Imported users cannot dial in to a Personal Conference Meeting.

**Possible Cause** The Administration site may not be finished processing all the imported users information. it takes a few minutes for a user's status to become Active in the system.

**Solution** On the **Users** page on the Administration site, verify that the imported users have an Active status. If the status is Active, ask the user to wait five minutes and try again. If the user cannot dial in to a Personal Conference meeting after waiting five minutes, restart the Web Server. Ask the user to wait another five minutes and try again.

**Possible Cause** Deactivated user is now an Active user.

**Solution** When you select the **Active** check box for a user on the **Users** page, a user should wait at least five minutes before trying to dial in to a Personal Conference meeting. If the user cannot dial in to a Personal Conference meeting after waiting five minutes, restart the Web Server. Ask the user to wait another five minutes and try again.

**Possible Cause** A user's Personal Conference account is deactivated.

**Solution** If a user has been deactivated in the system, the Personal Conference accounts associated with that user are also automatically deactivated. If a user scheduled a Personal Conference meeting before becoming deactivated, invitees will not be able to join the meeting because the participant access code will be considered invalid.

# Unable to Start a Meeting

**Problem** Unable to start a meeting.

**Possible Cause** Your network ports are not configured correctly.

**Solution** Ensure that your firewall or load balancing solution redirects requests to the correct ports to ensure end users can host and join meetings successfully.

# URL Entered in Mixed Case

**Problem** Site or Administration URL is entered in mixed case.

**Possible Cause** Browsers always send URLs in lowercase to the back end, which causes a mismatch because of case sensitivity.

**Solution** Site and Administration URL must be entered in lowercase.

# User Cannot Access Product

**Problem** TLS cannot be established. When checking sniffing packets, it shows CUCM sends "Un-Support certificate" to Cisco WebEx Meetings Server during CUCM and Cisco WebEx Meetings Server TLS handshaking.

**Possible Cause** Under Windows 7 32-bit and IE 8 environments, the local security setting has the following options: Use FIPS compliant algorithms for encryption, hashing, and signing enabled. The option path: gpedit.msc | Computer Configuration | Windows Settings | Security Settings | Local Policy | Security Options.

**Solution** If the TLSv1.0 option in IE advance settings is disabled then the user should enable the local policy. After enabling the local policy, IE 8 will work now with the TLSv1.0 turned off.

# User is Dropped from Audio Conference

**Problem** A user is dropped from an audio conference.

**Possible Cause** The user has low network connectivity speed (a few KB/sec).

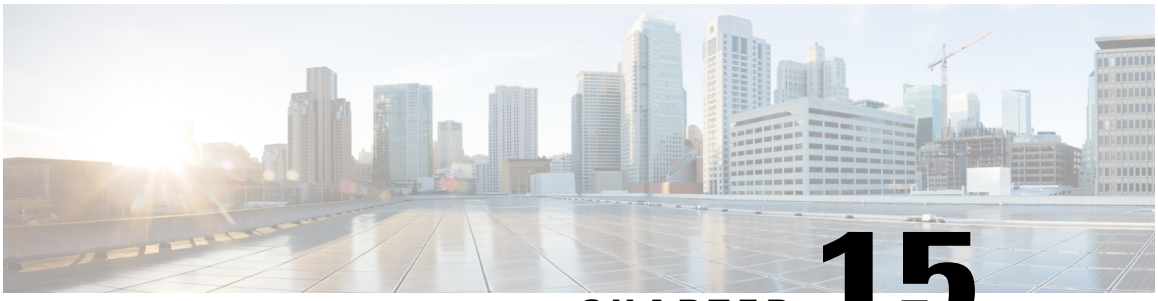
**Solution** Get the user's network connectivity speed to 100 KB/sec or higher to restore the ability to connect to the audio conference.

# WBX*INPROGRESSMEETING Table Does Not Record Data When Meeting Ends at Specific Time

**Problem** If a WebEx meeting ends at the statistics timestamp, such as 18:45 for 5-minutes statistics, 19:00 for hourly statistics, 9/27 00:00 for daily statistics, the corresponding WBX*INPROGRESSMEETING table does not capture data during the time that the daily statistics process would normally capture.

**Possible Cause** The DB Statistic job runs at a slower speed than the DB trigger job thereby producing a 5-minute delay in processing data.

**Solution** There is no current workaround. This issue will be fixed in a revision of the product.



CHAPTER 15

# Single Sign-On

This section includes troubleshooting topics about single sign-on (SSO) issues.



## SSO Fails After Completing Disaster Recovery Operation

**Problem** When a user completes a disaster recovery operation, SSO fails due to expired certificates.

**Possible Cause** Existing SSO certificates were installed before the application was installed.

**Solution** Reinstall SSO certificates after completing Disaster Recovery Operation. After you perform your restoration on the disaster recovery system, sign in to the Administration site and select **Settings** > **Security** > **Certificate** > **SSL Certificate** > **Generate CSR**.Under **More Options**, select **Download CSR** to download the generated CSR. Use the CSR to obtain a new SSL Certificate. Refer to the "Generating SSL Certificates" section of the Administration Guide for more information. Import your new SSL certificate by selecting **Settings** > **Security** > **Certificate** > **More Options** (Import SSL Certificate). Import the same SSL certificate into your ADFS (Active Directory Federation Service) for the site URL's relay party.

## SSO Protocol Error

**Problem** You receive the error message, "SSO protocol error. Contact your administrator for further support."

**Possible Cause** Your SSO administration site or IdP configuration contains errors.

**Possible Cause** SSO is not enabled.

**Possible Cause** Some or all of the required IdP attributes are not configured: firstname, lastname, email.

**Possible Cause** The NameID parameter of your SAML is not set to email.

**Solution** If you are unable to determine the cause of your SSO protocol error, generate a log and contact the Cisco TAC for further assistance. If you believe the cause is one of the above, make sure the required IdP attributes are configured and make sure the following IdP attributes are set to the user's email address: uid, SAML_SUBJECT..

# SSO Redirection Has Failed

**Problem** A user attempts to sign in and receives a "SSO Redirection Failed" message. The user is directed to an administrator for help.

**Possible Cause** An IdP attribute value in the user's account has violated account regulations. The following error messages can appear as a result of this problem:

- **Possible Cause** SSO protocol error. Contact your administrator for further support. See SSO Protocol Error, on page 53 for more information.
- **Possible Cause** No user account found in the system. Contact your administrator for further support.
- **Possible Cause** No X.509 certificate found in the system. Contact your administrator for further support.
- **Possible Cause** X.509 certificate has expired. Contact your administrator for further support.
- **Possible Cause** User account is locked. Contact your administrator for further support.
- **Possible Cause** User account is expired. Contact your administrator for further support.
- **Possible Cause** User account has been deactivated. Contact your administrator for further support.
- **Possible Cause** SAML assertion is expired. Contact your administrator for further support.
- **Possible Cause** Invalid Response message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed, on page 65 for more information.
- **Possible Cause** Auto Account Update failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed, on page 65 for more information.
- **Possible Cause** SSO protocol error. Contact your administrator for further support.
- **Possible Cause** No user name found in SAML assertion. Contact your administrator for further support.
- **Possible Cause** Only POST request is supported. Contact your administrator for further support.
- **Possible Cause** Incorrect SAML SSO POST data. Contact your administrator for further support.
- **Possible Cause** A Cisco WebEx Meetings Server certificate has not been imported into the SAML IdP.
- **Possible Cause** The site is not allowed to use SSO. Contact your administrator for further support.

- **Possible Cause** Incorrect X.509 certificate to validate SAML assertion. Contact your administrator for further support. See Incorrect X.509 Certificate to Validate SAML Assertion, on page 5 for more information.
- **Possible Cause** Loading configuration error. Contact your administrator for further support.
- **Possible Cause** The value of NameQualifier does not match site URL. Contact your administrator for further support.
- **Possible Cause** Unable to reach Assertion Party. Contact your administrator for further support.
- **Possible Cause** Failed to resolve SAML Artifact. Contact your administrator for further support.
- **Possible Cause** Invalid SAML Assertion. Contact your administrator for further support.
- **Possible Cause** Recipient does not match webex.com. Contact your administrator for further support.
- **Possible Cause** SAML assertion is unsigned. Contact your administrator for further support.
- **Possible Cause** User role is not allowed to login. Contact your administrator for further support.
- **Possible Cause** Invalid RequestedSecurityToken. Contact your administrator for further support.
- **Possible Cause** Invalid digital signature. Contact your administrator for further support.
- **Possible Cause** Untrusted Issuer. Contact your administrator for further support.
- **Possible Cause** Name Identifier format is incorrect. Contact your administrator for further support.
- **Possible Cause** Unable to generate AuthnRequest. Contact your administrator for further support.
- **Possible Cause** Unable to generate Logout Request. Contact your administrator for further support.
- **Possible Cause** InResponseTo does not match the request ID. Contact your administrator for further support.
- **Possible Cause** Invalid Request message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support.
- **Possible Cause** Auto Account Update failed. Contact your administrator for further support.
- **Possible Cause** Update user privilege failed or user is not allowed to update user privilege. Contact your administrator for further support.

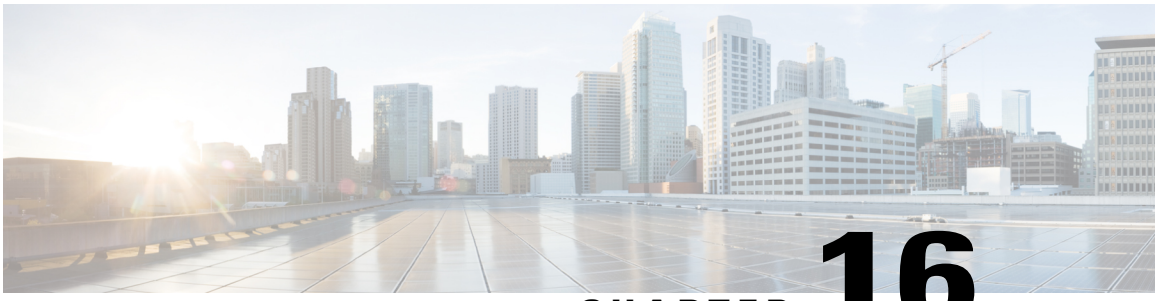
**Solution** Examine your URL API to determine which account values are causing the failure. Refer to the "Setting and Changing SSO URL API Parameters" section in the Planning Guide for more information.

# SSO Error Codes

The following table lists the SSO error codes.

| Error Description | Error Code |
|---|---|
| SSO protocol error | 1 |
| No user name found in SAML assertion | 2 |

| Error Description | Error Code |
|---|---|
| No user account found in the system | 3 |
| No X.509 certificate found in the system | 4 |
| Only POST request is supported | 5 |
| Incorrect SAML SSO POST data | 6 |
| The site is not allowed to use SSO | 7 |
| Incorrect X.509 certificate to validate SAML assertion | 8 |
| Loading configuration error | 9 |
| The value of NameQualifier does not match site URL | 10 |
| Unable to reach Assertion Party | 11 |
| Failed to resolve SAML Artifact | 12 |
| Invalid SAML assertion | 13 |
| Recipient does not match webex.com | 14 |
| X.509 certificate has expired | 15 |
| User account is locked | 16 |
| User account is expired | 17 |
| User account has been deactivated | 18 |
| SAML assertion is expired | 19 |
| SAML assertion is unsigned | 20 |
| User role is not allowed to login | 21 |
| Invalid RequestedSecurityToken | 22 |
| Invalid digital signature | 23 |
| Untrusted Issuer | 24 |
| Name Identifier format is incorrect | 25 |
| Unable to generate AuthnRequest | 26 |
| Unable to generate Logout Request | 27 |
| InResponseTo does not match the request ID | 28 |
| Invalid Response message | 29 |
| Invalid Request message | 30 |
| Auto Account Creation failed | 31 |
| Auto Account Update failed | 32 |



CHAPTER 16

# Telephony

This section includes telephony troubleshooting topics.



## Call Dropped on TLS High-Availability System

**Problem** In a large environment with configured for TLS (security encryption conferencing) conference calls might be dropped.

**Possible Cause** Your network is disconnected between your primary and high-availability virtual machines for a few minutes while a meeting is taking place. The network then recovers while the meeting is still taking place.

**Solution** Participants must manually rejoin their meeting.

## Call-Back Issues

**Problem** When you attempt to have the system call your phone number, the phone does not ring and you receive an error message: "Call back failed; no answer."

**Possible Cause** You need to reconfigure your CUCM servers.

**Solution** In CUCM, go to the SIP trunks configured for Cisco WebEx Meetings Server, and check the configured **Calling Search Space**. Go to your phone under **Devices**, and check the configured partition. Select **Call Routing** > **Class of Control** > **Calling Search Space**, go to the configured calling search space and make sure it has the partition listed configured for your phone.

# Call-In Issues

**Problem** Users hear a reorder tone before or after the complete number is dialed.

**Problem** The "Your call cannot be completed as dialed" message is played by the annunciator.

**Possible Cause** You need to reconfigure your CUCM servers.

**Solution** In CUCM, go to the route pattern being used for Cisco WebEx Meetings Server, and check the configured partition. Then go to the device you are calling from and check the configured **Calling Search Space**. Select **Call Routing** > **Class of Control** > **Calling Search Space**, go to the configured calling search space and make sure it has the partition listed configured for the route pattern for Cisco WebEx Meetings Server. If the partition is set to **<None>** any device configured in Cisco Unified Communications Manager would be able to call Cisco WebEx Meetings Server.

# Cannot Enter Meeting

**Problem** During call-in, a user's call terminates or there is no sound after entering the meeting ID followed by #.

**Problem** During call-back, a user's call terminates after entering 1 to join the meeting.

**Possible Cause** You need to reconfigure your CUCM servers.

**Solution** In CUCM, check your SIP route patterns configured for Cisco WebEx Meetings Server and check the configured route partition. Go to the SIP trunks configured for the load balancers and check the configured **Rerouting Calling Search Space** and **Out-Of-Dialog Refer Calling Search Space**. Select **Call Routing** > **Class of Control** > **Calling Search Space**, go to the configured Rerouting Calling Search Space and Out-Of-Dialog Refer Calling Search Space and make sure they each have the partition listed configured for the SIP Route Pattern for Cisco WebEx Meetings Server.

# User Calls are Dropped After Failover

**Problem** User calls are dropped after failover occurs on your high-availability system.

**Possible Cause** Your system has TLS enabled and uses a KPML IP phone. TAS attempts to send a subscribe SIP message to Cisco Unified Communications Manager (CUCM). The subscribe message cannot pass CUCM validation due to the change in the TAS IP address. To configure your CUCM settings, sign into the Administration Site and select **Settings** > **Audio** and then find the CUCM fields.

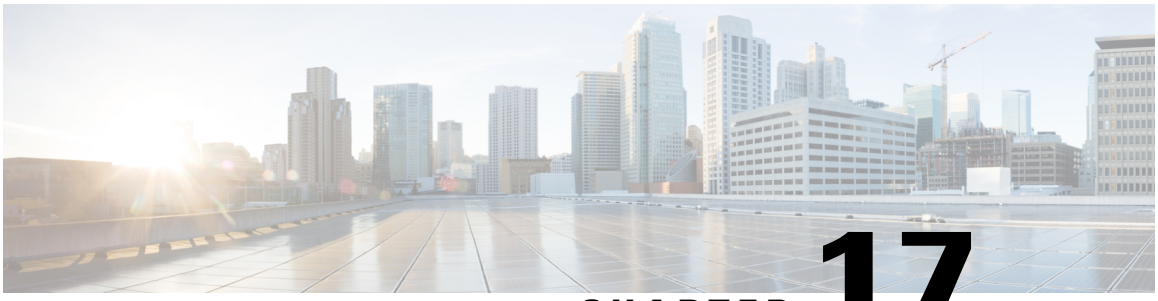
**Solution** This is a known issue and there are no configuration changes that can fix this problem at this time. When calls are dropped because of this problem, users must rejoin the meeting by dialing back in.

# Voice Activity Detection (VAD) Support Issues

**Problem** Cisco WebEx Meetings Server does not recognize the remote peer VAD enable/disable condition and disables the VAD parameter by default. VAD, also known as speech activity detection or speech detection, is a technique used in speech processing in which the presence or absence of human speech is detected.

**Possible Cause** Cisco WebEx Meetings Server does not perform the SDP-based negotiation for VAD support. Starting from Cisco WebEx Meetings Server 1.1 MR2 and later, by default Cisco WebEx Meetings Server disables VAD. Earlier versions of Cisco WebEx Meetings Server enable VAD by default. By disabling VAD, the bandwidth consumed for the codec that is being used will not exceed the standard bandwidth requirements for that codec. For example, the bandwidth consumption for G.711 will be 64 kbps when VAD is disabled. VAD does not impact user experience in any way. When VAD is enabled, Cisco WebEx Meetings Server helps to save network bandwidth depending on the active speech detected. When there is silence, Cisco WebEx Meetings Server sends a special SID packet indicating the silence and stops sending packets which helps to save network bandwidth. It starts sending audio packets again when there is voice activity detected.

**Solution** VAD negotiation through SDP is not currently supported by Cisco WebEx Meetings Server.



CHAPTER 17

# Upgrade, Update, and Expansion Issues

This section includes troubleshooting topics about upgrades, updates, and expansions.



## Internal Server Error Received After Starting Update

**Problem** After starting an update, there is an update in-progress pop up page that appears. During the update you receive the following error message: "Internal Server Error (HTTP request /maintenanceLock/unlock)."

**Possible Cause** The Administration Web application server receives an internal error that interrupted the update.

**Solution** Restart all your virtual machines gracefully by using **Shut Down Guest** on each virtual machine using the vSphere client. Then power on all virtual machines. Check that the Administration Dashboard shows that the version is updated. If so, your update was successful and you can take your system out of maintenance mode and continue. Otherwise, please contact technical support for further assistance.

## No Confirmation Message Received After Performing an Update

**Problem** After the update in-progress pop up page appears, there is no message indicating whether the update was successful or failed. Instead, you are directed to the Administration site sign-in page and the Administration Dashboard shows the old version.

**Possible Cause** An Administration Web application server HTTP session timeout has occurred or your HTTP session was disconnected.

**Solution** Check your virtual machine console window for the update status. If there is an error, the console window tells you which phase the error occurred in: validation, database preparation, repository preparation, system update, or the update package archive phase. Restart all your virtual machines gracefully by using **Shut Down Guest** on each virtual machine using the vSphere client. Then power on all virtual machines. Check that the Administration Dashboard shows that the version is updated. If so, your update was successful and you can take your system out of maintenance mode and continue. Otherwise, please contact technical support for further assistance.

# Unable to Connect to ISO Image in the CD/DVD Drive

**Problem** You are unable to connect to the ISO image in the CD/DVD drive to perform an installation.

**Possible Cause** Your Administration site virtual machine's CD/DVD is not connecting to the ISO image. You might be attempting to connect to the wrong virtual machine, or it is connecting slowly (this can be caused by activity in VMware vCenter).

**Solution** Connect the ISO image using the vSphere client. Check that your ISO image is connected to the correct virtual machine. The Administration site displays the hostname of the virtual machine. Make sure it matches. It is normally the primary Admin virtual machine unless you are updating a high-availability system that is not yet attached to a primary system. If the CD/DVD drive shows "Connecting" as its status, wait until it is finished.

# Update Completes but No "System Updated" or "Restart" Button Appears

**Problem** You perform an update and the update completes successfully, but you do not see text stating "System Updated" or a "Restart" button.

**Solution** Check your virtual machine console window for the update status. If there is an error, the console window tells you which phase the error occurred in: validation, database preparation, repository preparation, system update, or the update package archive phase.

# Update Failure

**Problem** Your update fails.

**Possible Cause** A connection issue occurs (a network glitch, input/output problem, or another issue for your Internet Reverse Proxy) or one or more virtual machines is not accessible.

- **Solution** Check your virtual machine console window for the update status. If there is an error, the console window tells you which phase the error occurred in: validation, database preparation, repository preparation, system update, or the update package archive phase.

- **Solution** Collect logs: /opt/log/upgrade/*, /opt/log/webadmin/*, and so on.

- **Solution** Roll back all virtual machines to a backed up version, or restore the backup taken before you attempted your update, and then retry your update.

# Update System Process is Stuck

**Problem** The update process is stuck at "Updating system..." for an hour or more.

- **Possible Cause** Your ISO package is unable to get placed in the datastore and the vSphere client is experiencing a slow network connection.
- **Possible Cause** Your system is experiencing slow disk input/output or congested input/output on the datastore. Too many hosts are connecting to and accessing the same datastore or disk array.

- **Solution** Check your virtual machine console window for the update status. If there is an error, the console window tells you which phase the error occurred in: validation, database preparation, repository preparation, system update, or the update package archive phase.

- **Solution** Roll back your update, put your ISO in the datastore or, if your administration virtual machine's CD/DVD drive is connecting locally using the vSphere client, then be sure the vSphere client has a local hardwire connection into your company's Intranet (not over VPN).

- **Solution** Roll back your update, migrate your virtual machine to a new datastore, and retry your update.

# Upgrade Button Grayed Out

**Problem** The **System** page on your Administration site does not have an **Upgrade** button or the button is grayed out.

**Possible Cause** You are attempting an update, upgrade, or expansion on the high-availability Administration site instead of the primary system Administration site.

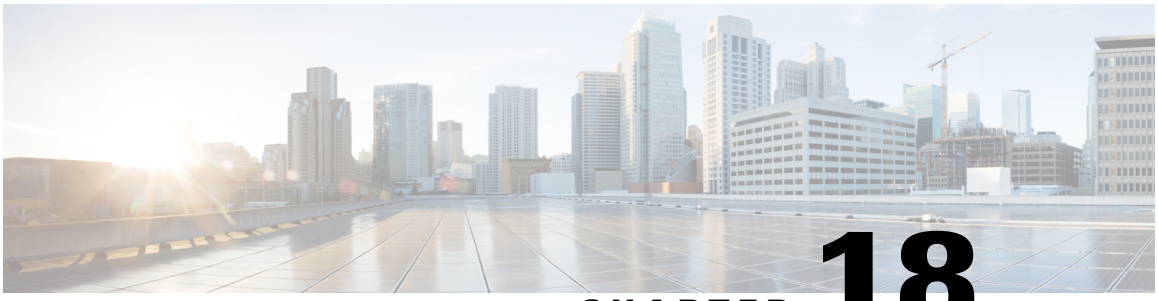
**Solution** Make sure your primary administration virtual machine is powered on. Sign out from the Administration site, start a new browser session and sign in again. If the issue persists, make sure your primary administration process is still working.

# Upgrade or Expansion Fails

**Problem** Your upgrade or expansion attempt fails.

**Possible Cause** A data file on your system might be corrupted.

**Solution** Check your log file to see if an error or other problem appears on it. Roll back your existing system. Reinstall a new system, or roll back a new system if VMware snapshots were taken or disaster recovery was configured after OVA installation, and then retry your upgrade or expansion.



CHAPTER 18

# User Management

This section includes troubleshooting topics about user management issues.



# Auto Account Creation or Auto Account Update Has Failed

**Problem** You receive one of the following error messages:

- **Problem** Auto Account Creation failed. Contact your administrator for further support.
- **Problem** Auto Account Update failed. Contact your administrator for further support.

**Possible Cause** Your IdP updatetimestamp attribute might not be configured. It is possible that there are other IdP configuration issues as well.

**Solution** Check whether the required attribute mappings are configured in IdP correctly, such as *firstname*, *lastname*, *email*, *SAML_SUBJECT*, or *Name_ID*. Pay special attention to the Name_ID and *SAML_SUBJECT* settings. Some IdP configurations use *Name_ID* and others use *SAML_SUBJECT*. We recommend that you configure all accounts so *Name_ID* has the same value as *SAML_SUBJECT*.

**Solution** TC1 (Tracking Code 1), ……, TC10 (Tracking Code 10) are special attributes. If the tracking code is configured as required in the Administration at **Users** > **Tracking Codes**, they are required attribute mappings.

**Solution** If the input mode of a tracking code is dropdown menu, then the following applies:

- **Solution** If the tracking code is configured as **Required**, the attribute value must be one of the active values in the dropdown menu.
- **Solution** If current tracking code is configured as not Required, the attribute value can be empty or one of the active values in dropdown menu.

**Solution** For example, if IdP is ADFS 2 and you have not configured Tracking Codes (*SAML_SUBJECT* is not required in ADFS 2), the following mapping is required:

| LDAP Attribute | Outgoing Claim Type |
|---|---|
| E-Mail-Addresses | Name_ID |
| E-Mail-Addresses | email |
| Given-Name | firstname |
| Surname | lastname |

**Note** **Solution**

- **Solution** We recommend that you map the *Name_ID* to the email address.
- **Solution** The attribute name is case sensitive. Make sure the user's attribute value is not empty.
- **Solution** We recommend that you do not configure your tracking codes as **Required**.
- **Solution** We recommend that you do not configure the input mode of your tracking codes as dropdown menu.

**Solution** Then make sure the user's attribute value is not empty.

# SSO URL API Reference

When creating users, you must synchronize users' information on the Cisco WebEx database with the SSO site. The following table provides the arguments that must be synchronized:

| Argument | Value | Description |
|---|---|---|
| firstname | String | User's first name is required with a maximum length of 32 characters. |

| Argument | Value | Description |
|---|---|---|
| lastname | String | User's last name is required with a maximum length of 32 characters. |
| email | String | User's email address is required with a maximum length of 64 characters. |
| TC1 | String | User's tracking code 1. Optional/required (configured in the Administration site. Refer to the Administration Guide for more information on user management. The maximum length is 132 characters.<br>• If the tracking code is configured as required, then you must provide the value.<br>• If the input mode for current tracking code is **Dropdown menu**, then if you provide the value that you configure in the dropdown menu.<br>**Note** The value must be active in the dropdown menu. |

The account information described above is configured with the following features:

- User configuration:
  - Administration site: Select **Users** > **Edit User** to display the user account fields.
  - End-user site: Select **My Account** to display the user account fields.
- Tracking code configuration:
  - Administration site: Select **Users** > **Tracking Codes** and set your **Input mode** to **Dropdown menu** and configure your **Usage** setting. Then select **Edit list** to configure your dropdown menu settings.

# Importing Users with a CSV File Fails

**Problem** You attempt to import users with a CSV file and the operation fails. You receive an error message that indicates you have selected an invalid file.

**Possible Cause** Import files must be unicode UTF-8 or UTF-16. Microsoft Excel only saves UTF files as *.txt.

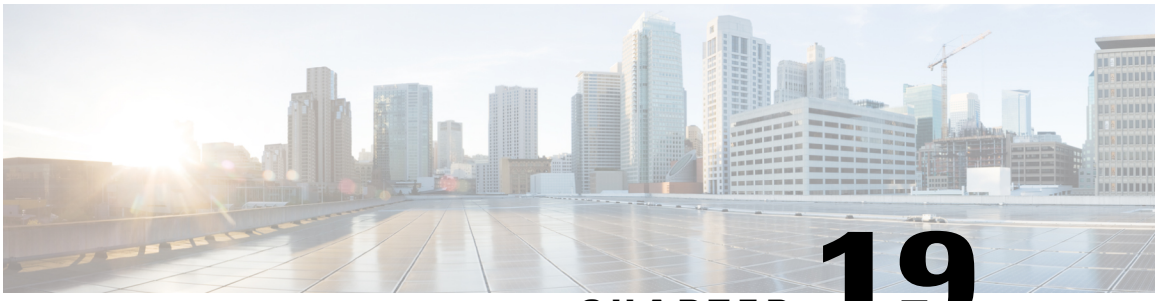
**Solution** Make any changes to your file in Excel, then save as unicode UTF-16 (*.txt). Once the save is complete, rename the file to *.csv. Select the tab delimited file option when importing the CSV into Cisco WebEx Meetings Server.

# No User Account Found in the System

**Problem** You receive the error message, "No user account found in the system. Contact your administrator for further support."

**Possible Cause** The user does not exist on the system and auto account creation is not turned on.

**Solution** Make sure you have added the user on the system and make sure auto account creation is turned on.



CHAPTER 19

# Virtual Machine issues

This section includes troubleshooting topics about virtual machine issues.



## Administration Virtual Machine on Your Primary or High-Availability System is Down

**Problem** Your administration virtual machine on your primary or high-availability system is down. You can view your system status by selecting **System** > **View More** > **Properties**. The Administration Site is inaccessible and you see an error message in your browser window (for example, "We've hit a glitch in processing your request.").

**Possible Cause** There may be a problem with the management of the virtual machine in VMware vSphere.

**Solution** Obtain your VMware logs (kb.vmware.com) and provide them to your Cisco TAC representative. Your representative will use the logs to determine if there is a virtual machine issue on your system. Note that the Tasks and Events messages (virtual machine events from the Tasks and Events tab) are important for troubleshooting purposes.

# NIC Teaming Issues

**Problem** You configured NIC teaming for failover and load balancing and all of your virtual machines seem to be running properly but you begin to encounter problems running the product at maximum load due to meeting failures.

**Possible Cause** Open your VMware vSphere console and determine if your NIC teaming is working properly on the UCS Servers that are hosting Cisco WebEx Meetings Server virtual machines. This often occurs due to a failed connection from a NIC, forcing another NIC to take on the full network load. This is especially important if your NICs are Gigabit-Ethernet NICS since at maximum port load any one of your NICs would be running to maximum link capacity. So a catastrophic failure on one Gigabit-Ethernet NIC causes the entire networking load to fall on the other NIC, saturating the link and causing application-level issues within Cisco WebEx Meetings Server.

**Solution** Put Cisco WebEx Meetings Server in maintenance mode, fix or replace the failed NIC, and then restore service to end-users.

# Virtual Machine Does Not Boot Up After Deployment

**Problem** The virtual machine does not boot up after deployment.

**Possible Cause** The Cisco UCS Server (on which the virtual machine is deployed) does not meet the minimum requirements for the system size.

**Solution** Check the system requirements for your system size and ensure that there is enough CPU, memory, and free disk space. Refer to the *Cisco WebEx Meetings Server System Requirements* for more information.

# Virtual Machine Fails and Cannot Be Recovered

**Problem** One of your virtual machines fails and you are unable to fix it even with the assistance of the Cisco TAC.

**Possible Cause** There are several possible causes including the following: you have a corrupt database, you have a faulty configuration, unsupported maintenance activity, power failures, hardware failures, and more.

**Solution** If a virtual machine on your high-availability configuration fails, remove the high-availability virtual machine from your system. Redeploy all of your high-availability virtual machines and then reconfigure the system for high availability. Refer to "Configuring a High Availability System" in the *Cisco WebEx Meetings Server Administration Guide* for more information. Similarly if an Internet Reverse Proxy virtual machine fails, you must remove that virtual machine from your system. Then redeploy and reconfigure your Internet Reverse Proxy virtual machine. Refer to "Adding Public Access" in the *Cisco WebEx Meetings Server Administration Guide* for more information. For any other virtual machine, your must rebuild your system using the Disaster Recovery feature. Refer to "Using the Disaster Recovery Feature" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

# Virtual Machine Issues and Crashes

**Problem** Your virtual machine crashes and does not resume functioning.

**Possible Cause**

**Solution** Attempt to perform the following solutions:

- **Solution** Attempt to restart your virtual machine from VMware vCenter.

- **Solution** If you took snapshots of your virtual machines, attempt to restore a snapshot.

**Note** **Solution** Snapshots might not contain all of your configuration information and you might have to perform some configuration tasks to restore all functions on your system.

- **Solution** If you configured a storage server, you can attempt to perform a disaster recovery procedure to restore your system. Refer to "Using the Disaster Recovery Feature" in your Administration Guide for more information.

- **Solution** If none of the above solve your problem, contact the Cisco TAC for assistance. You can contact the TAC at the following URL: http://www.cisco.com/cisco/web/support/index.html

# Virtual Machine Repeatedly Reboots

**Problem** The virtual machine on which I have deployed the Cisco WebEx Meetings Server OVA, repeatedly reboots.

**Possible Cause** NTP is not configured on the ESXi host.

**Solution** Configure NTP on your ESXi host, check the DNS on your ESXi host to make sure it is resolving the NTP server correctly, and then redeploy the OVA to the virtual machine.

# Your Virtual Machine is Repeatedly Rebooting After a Power Outage

**Problem** Your virtual machine is repeatedly rebooting after a power outage without allowing the operating system to load. No SSH or GUI access is available.

**Possible Cause** Your file system is corrupted.

**Solution** This is applicable to any Cisco WebEx Meetings Server virtual machine. When a virtual machine boots, you will see this message on the console: **Booting Cent OS (<string_numbers_letters>) in <number> seconds**. Press any key to interrupt the boot process and display the GNU GRUB boot loader menu. Press **e** to edit the commands before booting the virtual machine. Press the down arrow key to select the **kernel** line and then press **e** to edit the kernel line. Append this text to the kernel line: **init=/bin/sh** (make sure there is a space before init). Press the Enter key to save your changes and return to the previous menu. Press **b** to boot. Mount the root file system by typing this command: **mount -o remount,rw / .** Invoke superuser mode by entering **su** at the command line to get root access. From there, enter **fsck** to check and repair your file system. Press **y** to the prompts to repair any issues found. After you are finished, reboot the virtual machine by using the RESET function in vCenter. If the issue is resolved, the virtual machine should boot normally. Check the system status by entering **hastatus** at the command line. If this does not work and TAC is unable to find any workaround, follow the Disaster Recovery process that is described in the *Cisco WebEx Meetings Server Administration Guide*.