Troubleshooting Guide for Cisco Webex Meetings Server Release 4.0

First Published: 2019-04-29
Last Modified: 2019-11-04

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 1
  Cannot Download Logs 1
  Cannot Download Reports Using Microsoft Internet Explorer 1
  Cannot Generate System Logs 2
  Log Capture Size Problems 2

CHAPTER 2

Certificates 3
  Cannot Remove or Overwrite Existing Certificates 3
  Cannot Remove an SSO IdP Certificate 3
  Certificate Chain Error 4
  Certificate Does not Match Private Key 4
  Certificate Not Yet Valid 4
  Expired Certificate 5
  Incorrect X.509 Certificate to Validate SAML Assertion 5
  Invalid Certificate Error 5
  Invalid Domain Error—Wildcard Certificate 5
  Invalid Domain Error—SAN Certificate 6
  Key Decryption Error 6
  Key Size Error 6
  Unable to Access Webex Administration 6
  Self-Signed Certificate After Upgrade 7
  Cannot Establish TLS Due to Missing Extension in Certificate 7
  Unable to Access Cisco Webex Meetings Server from a Mobile Device 7
  Untrusted Connection 8

CHAPTER 3

Cisco Jabber 9
Cannot Connect to a Webex Meeting by Using Cisco Jabber 9

CHAPTER 4

Directory Integration 11
  A User Cannot Sign In After Directory Integration is Configured 11
  All Users Cannot Sign in After Directory Integration 12
  User Cannot Sign In After Switching from SSO to LDAP Authentication 12
  Multiple Users Cannot Sign In After Switching from SSO to LDAP Authentication 12
  An Administrator Cannot Sign in to the Webex Site 12
  A User Added in Cisco Webex Meetings Server Cannot Sign In 13
  Unified Communications Account Credentials Don't Work for Cisco Webex Meetings Server 13
  Cannot Activate a User Deactivated by Directory Synchronization 13
  User Status Does Not Update After Changing the Active Directory Server 13
  A User Added to an Active Directory Server Does Not Appear After Synchronization 14

CHAPTER 5

Disaster Recovery 15
  Audio Conferencing Not Working after Disaster Recovery for a Multi-Data Center System 15

CHAPTER 6

Downloading Applications 17
  The Cisco Webex Meetings Desktop Application Fails to Open 17
  Error 1316 Occurs During Application Installation 17

CHAPTER 7

Emails 19
  Administrators and Users Are Not Receiving Emails 19
  SMTP Email Server Issues on a System with TLS-Based Authentication 19
  Administrators Do Not Receive the Notification Emails for Reports 20

CHAPTER 8

General 21
  Text Fields Have Angled Corners Instead of Rounded Corners 21

CHAPTER 9

Installation and Deployment 23
  Use of Forward Proxies in Your System 23
  Use of Reverse Proxies in Your System 24
  Auto-Deployment Fails with error.deploy_summary.353 24
Auto-Deployment Fails with error.deploy_summary.363 or error.deploy_summary.365
Deployment Fails with an "Unsupported Configuration" Error
The End User Download Page is Broken After Completing an Update
Invalid Passphrase URL Error
Unable to Install Cisco Webex Meetings Server
The System Displays a Pre-check Error During an Update or Upgrade

CHAPTER 10  Licenses  27
Cisco Webex Meetings Server Is Running in Evaluation Mode

CHAPTER 11  Maintenance Mode  29
The “Rebooting” Message Does Not Go Away after You Turn off Maintenance Mode
Request to Turn Maintenance Mode on or off is Rejected

CHAPTER 12  Recordings  31
Cannot Start or Join Meetings, or View Recordings
Recordings Do Not Appear on the Host Recordings Pages
Meeting Recordings Do Not Appear on the Recordings Page
Clicking the Record Button Generates a Server Connect Error
Cannot Add a Storage Server
Meeting Recording Is Disabled
The Record Button is Disabled
Record Button Is Not Available After Secure Storage Is Restored
The Recording Panel Generates an Error
Some Users Do Not Receive Links to Their Meeting Recordings

CHAPTER 13  Servers  35
SMTP Sends Delivery Failure Replies
Users Are Seeing NTP Alerts
The Storage Server Is Not Backing up the System or the Recordings
Repeated Kernel Errors Appear in the Syslog
The CWMS System Fails to Boot up after an Update or Upgrade

CHAPTER 14  Sign in and Meeting Issues  37
CHAPTER 16

Telephony 51

Call Drops on a TLS High-Availability System 51
Call-In Issues 51
Call-Back Issues 52
Cannot Enter Meeting 52
EETone Does Not Play as Expected 52
Users Cannot Set EETone for Their Meetings 53
Caller ID Missing for Call-in Users 53
User Calls Drop after a Failover 54
Voice Activity Detection Support Issues 54
Secure Teleconferencing Works Only on One Data Center 55

CHAPTER 17

Upgrade, Update, and Expansion Issues 57

Internal Server Error after Starting an Update 57
No Confirmation Message Received After Performing an Update 58
Unable to Connect to ISO Image in the CD/DVD Drive 58
No System Updated Message or the Restart Button Does Not Appear 58
Update Failure 59
The Update System Process is Stuck 59
The Upgrade Button Is Dimmed 59
Expansion Fails 60
Upgrade Credentials Are Incorrect 60
Upgrade and Original Admin VMs Are Not on the Same ESXi 60
Upgrade and Original Admin VMs Not On the Same Subnet 60
Transfer of Archived Data Failed 61
Upgrade to Incorrect Version Attempted 61
Upgrade Original HA System Connection Failure 61
Upgrade Failed to Get Data 61
Upgrade Failed Disk Space Check 62
Upgrade Failed to Join Virtual Machines 62
Update Failed the NTP Verification Check 62
Upgrade Virtual Machine Disk Format Failed 63
Upgrade System Size Mismatch 63
Original System Size Changed During Upgrade  63
Upgrade Session In Progress  63
Failed to Connect to the Original Admin Site  63
Original System Admin URL Changed during Upgrade  63
Original System Site URL Changed during Upgrade  64
Original System Version Changed during Upgrade  64

CHAPTER 18  User Management  65
Auto Account Creation or Auto Account Update Failed  65
SSO URL API Reference  66
Importing Users with a CSV File Fails  67
No User Account Found in the System  68

CHAPTER 19  Virtual Machine Issues  69
Administration Virtual Machine on Your Primary or High-Availability System is Down  69
NIC Teaming Issues  69
A Virtual Machine Does Not Boot up after Deployment  70
A Virtual Machine Fails and Cannot Be Recovered  70
Virtual Machine Issues and Crashes  70
Virtual Machine Is Unreachable  71
Virtual Machine Repeatedly Reboots  71
A Virtual Machine Repeatedly Reboots after a Power Outage  71
CHAPTER 1

Alarms, Logs, and Reports

- Cannot Download Logs, on page 1
- Cannot Download Reports Using Microsoft Internet Explorer, on page 1
- Cannot Generate System Logs, on page 2
- Log Capture Size Problems, on page 2

Cannot Download Logs

Problem You cannot download logs.

Possible Cause Your system is configured for SSL and you are using a Microsoft Internet Explorer version earlier than version 9. Internet Explorer before version 9 requires a specific header forcing it to cache downloaded files. It then deletes or fails to properly cache 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. For more information, see the "Setting Up a Remote Support Account" section of the Cisco Webex Meetings Server Administration Guide.

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 Report 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 The setting Do not save encrypted pages to disk is enabled for Internet Explorer.

Solution Change your Internet Explorer security settings: Go to Tools > Internet Options > Advanced > Security and uncheck the Do not save encrypted pages to disk. Then click OK.
Cannot Generate System Logs

**Problem** Cisco Webex Meetings Server administrators cannot capture logs after a failed update of the system. Before you capture system logs, check the system status. If the system and all the virtual machines are up and running, you can proceed with log capture. If one or more virtual machines are down, log capture fails.

**Possible Cause** Cisco Webex Meetings Server is not in a healthy state and some components are not running. The system must be healthy and running to generate system logs.

**Solution** Retry the system update after reverting snapshots and contact the Cisco TAC if the update problem persists.

Log Capture Size Problems

**Problem** The log capture size is 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 selected only part of the day. This behavior is by design. Unzipping the files can be a time-consuming process and can impact the performance of your system.

**Solution** You can minimize the log capture size by selecting only the activities that you require for troubleshooting. Try performing a log capture as soon as you encounter an issue, so that the log capture service does not have to go into the archives to obtain the logs.
Certificates

• Cannot Remove or Overwrite Existing Certificates, on page 3
• Cannot Remove an SSO IdP Certificate, on page 3
• Certificate Chain Error, on page 4
• Certificate Does not Match Private Key, on page 4
• Certificate Not Yet Valid, on page 4
• Expired Certificate, on page 5
• Incorrect X.509 Certificate to Validate SAML Assertion, on page 5
• Invalid Certificate Error, on page 5
• Invalid Domain Error—Wildcard Certificate, on page 5
• Invalid Domain Error—SAN Certificate, on page 6
• Key Decryption Error, on page 6
• Key Size Error, on page 6
• Unable to Access Webex Administration, on page 6
• Self-Signed Certificate After Upgrade, on page 7
• Cannot Establish TLS Due to Missing Extension in Certificate, on page 7
• Unable to Access Cisco Webex Meetings Server from a Mobile Device, on page 7
• Untrusted Connection, on page 8

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. For more information, see “Disabling SSO” in the Cisco Webex Meetings Server Administration Guide.

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 ensure that 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. Ensure that 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. Ensure that there are no extra blank lines or text. Save this combined file and upload to your system.

**Solution** 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 the preceding procedure. If you do not have the private key saved, you must generate another CSR and purchase a new certificate.

Certificate Not Yet Valid

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.

**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** Verify that the system time is correct.
Expired Certificate

Problem You receive an "expired certificate" error.
Possible Cause The validity period of the certificate has ended.
Solution Generate a new CSR and use it to obtain a new, valid certificate. Verify 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 Ensure that 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 system uses a wildcard certificate and not all hosts and URLs are in the same domain.
Possible Cause To use a wildcard certificate, all hosts and URLs in the system must be in a single domain. For multiple domains, you need a SAN certificate instead.
Solution Ensure 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 the domain that is specified in the certificate.
Solution The certificate specifies the domain in the common name. Verify that the domain is the same for all hostnames and URLs for the system:
Solution System hostnames
Solution Site URL
Invalid Domain Error—SAN Certificate

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

- **Possible Cause** The system is using a SAN certificate and the CN does not match the site URL.
- **Solution** Ensure 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** Ensure that you enter the correct password.
- **Solution** Try reading the key with OpenSSL.

Key Size Error

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

- **Possible Cause** You are trying to upload a private key and certificate.
- **Possible Cause** You are trying to upload a certificate, 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.

Unable to Access Webex Administration

**Problem** Administrators and users cannot access the administration and end-user sites. The following error message appears: "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, the following security alert appears: "The security certificate for this site has been revoked. This site should not be trusted."

Solution In your browser, disable the "Check for server certificate revocation" option. Regenerate and import your certificate. For more information, see "Managing Certificates" in the Cisco Webex Meetings Server Administration Guide.

Self-Signed Certificate After Upgrade

Problem The system reverts to a self-signed certificate after you upload a third-party certificate.

Possible Cause If the operation you performed changed the hostnames or URLs on your system, your existing certificate is no longer valid. You performed an upgrade or expansion, added high availability, changed a site URL, or made another similar change.

Solution Generate a new CSR and obtain a new certificate. If the hostnames and URLs have not changed, upload the private key and certificate 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 a Mobile Device

Problem Cannot access Cisco Webex Meetings Server from a mobile device.

Possible Cause The system uses a 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 the administrators by email. Administrators cannot 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.
Untrusted Connection


Possible Cause The system is using a self-signed certificate. New installations of Cisco Webex Meetings server use self-signed certificates. If a system has an existing certificate and you perform an operation which invalidates that certificate, the system generates a self-signed certificate.

Solution Purchase a certificate from a well-known certificate authority and upload it to the system. "Well known" means that the root certificate for the certificate authority 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 Ensure that the issuer of the certificate is in the truststore for your client. If you use a private or internal certificate authority, distribute the 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, the issuing 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.
Cisco Jabber

• Cannot Connect to a Webex Meeting by Using Cisco Jabber, on page 9

Cannot Connect to a Webex Meeting by Using Cisco Jabber

Problem Cisco Jabber cannot connect to a Webex meeting.

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

• Solution Verify that port 443 is open. Cisco Jabber connects to Cisco Webex Meetings Server through this port.

• Solution Verify 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 Cisco Jabber for Windows Install and Upgrade Guides 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 Cisco Jabber for Windows Install and Upgrade Guides.

• 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 conferencing profile.
Cannot Connect to a Webex Meeting by Using Cisco Jabber
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 whether the user has an account and whether it is active.

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

Solution  Ensure that the user has a valid email account. The accepted format is abc@mydomain.com.

Possible Cause The user might not be configured in the Cisco Unified Communications Manager (CUCM) directory.

Solution  Verify that the user appears in the users list in CUCM. Users can sign in, even before the user account is imported into your Cisco Webex Meetings Server database. When LDAP authentication is enabled and a user tries to sign in, your system verifies that 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. The system populates this field after you perform a directory synchronization. If the field is empty, the system checks the CUCM database to see whether the user exists there. If the user exists in the CUCM database, the system updates the ADUserID fields for the user record in the database. Authentication continues and succeeds, as long as the user exists in the CUCM database and provides the correct credentials. After the first sign in, the system treats the user 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** Verify network connectivity between Cisco Webex Meetings Server and Cisco Unified Communications Manager (CUCM) or Active Directory.

**Possible Cause** The CUCM AXL username or password has changed.

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

User Cannot Sign In After Switching from SSO to LDAP Authentication

**Problem** A user cannot sign in after you switch from using SSO to LDAP authentication.

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

**Solution** Inform all users that they must use their email addresses to sign into their accounts.

Multiple Users Cannot Sign In After Switching from SSO to LDAP Authentication

**Problem** Some or all of your users cannot sign in, after you switched from SSO to LDAP authentication.

**Possible Cause** You did not perform a Cisco Webex Meetings Server synchronization.

**Solution** Verify that the affected users are listed as users in the Cisco Webex Meetings Server. If they are not, they cannot sign into the system.

**Solution** Sign in to Webex Site Administration, and go to Users > Directory Integration. Perform a synchronization to import all active users from your CUCM Active Directory server to Cisco Webex Meetings Server. After the synchronization is complete, inform the users about the change and that they must use their email addresses to sign in. For more information, see “Configuring Directory Integration” in the *Cisco Webex Meetings Server Administration Guide*.

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** Ensure that the administrator has an account on the Active Directory server. The credentials for the Webex site are different than those for Webex Administration.
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**
Ensure that the user is configured in your Active Directory server and then synchronized with your Cisco Webex Meetings Server system.

Unified Communications Account Credentials Don't Work for Cisco Webex Meetings Server

**Problem**
Unified Communications account credentials may not be valid for Cisco Webex Meetings Server.

**Possible Cause**
The credentials used to sign into Jabber or other Unified Communications can be different than the Webex site ID after you configure directory integration. For example, after you enable LDAP authentication, the user email address becomes the user ID.

**Solution**
Inform users that they must use their email addresses to sign into the Webex site.

Cannot Activate a User Deactivated by Directory Synchronization

**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 in Cisco Webex Meetings Server user management, if the user was originally deactivated by a CUCM Active Directory synchronization. Such users are marked with an asterisk that indicates "User has been disabled on LDAP." 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 by 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**
Activate the user by using Cisco Webex Meetings Server user management. Sign into Webex Site Administration, and go to Users. Click the check box for the user you want to activate, and then click Actions > Activate.

User Status Does Not Update After Changing the Active Directory Server

**Problem**
User status is not updated after a change is made in the Active Directory server.
Possible Cause You did not schedule Cisco Webex Meetings Server synchronization to occur after the CUCM Active Directory synchronization. User status updates in Cisco Webex Meetings Server are based on the user status that is configured in your Active Directory settings. For example, if you delete a user from your Active Directory server, CUCM marks the user as Inactive during the next synchronization. The system deletes the user after 24 hours. If Cisco Webex Meetings Server does not perform a synchronization within 24 hours, the user status does not change.

Solution Ensure that you schedule your Cisco Webex Meetings Server synchronization to occur after your CUCM Active Directory synchronization.

A User Added to an Active Directory Server Does Not Appear After Synchronization

Problem A user added to the Active Directory server does not appear in the active users list, even after you perform a Cisco Webex Meetings Server synchronization.

Possible Cause You did not perform a Cisco Unified Communications Manager (CUCM) Active Directory synchronization before the Cisco Webex Meetings Server synchronization. CWMS does not communicate directly with Active Directory. After you add users, perform an Active Directory synchronization with CUCM before you synchronize your users with Cisco Webex Meetings Server.

Solution Perform a CUCM Active Directory server synchronization:
1. Solution Sign into Webex Administration.
2. Solution Go to System > LDAP Directory.
3. Solution Click Perform Full Sync Now.

Solution All new active users are imported into Cisco Webex Meetings Server at the next directory integration synchronization.
Audio Conferencing Not Working after Disaster Recovery for a Multi-Data Center System

**Problem** On a secure teleconferencing system, audio conferencing does not function after you perform disaster recovery on a Multi-data Center (MDC) system.

**Possible Cause** The Cisco Unified Communications Manager (CUCM) SIP trunk configuration is not updated. Before you perform the disaster recovery procedure, the application point and load balance point SIP trunks are configured with X.509 SIP trunk security profiles. At your primary data center, your SIP trunks are configured with X.509 SIP trunk security profiles in that data center. At your secondary data center, the 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.

**Possible Cause** After disaster recovery, the restored secondary data center is assigned the SIP trunk security profile URL of the primary 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

<table>
<thead>
<tr>
<th>SIP Trunk</th>
<th>SIP Trunk Security Profile: X.509 Subject Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP trunk for a load balance point at the first data center</td>
<td>Site URL for the first data center (FQDN format)</td>
</tr>
<tr>
<td>SIP trunk for an application point at the first data center</td>
<td>Site URL for the first data center (FQDN format)</td>
</tr>
</tbody>
</table>

### Table 2: Second Data Center Configuration before Disaster Recovery

<table>
<thead>
<tr>
<th>SIP Trunk</th>
<th>SIP Trunk Security Profile: X.509 Subject Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP trunk for a load balance point at the second data center</td>
<td>Site URL for the second data center (FQDN format)</td>
</tr>
<tr>
<td>SIP trunk for an application point at the second data center</td>
<td>Site URL for the second data center (FQDN format)</td>
</tr>
</tbody>
</table>
Solution Start CUCM and change the SIP trunk security profile for your secondary data center to the URL of the primary data center in the X.509 Subject field. See the table below for the required configuration of your secondary data center after disaster recovery. See the Cisco Webex Meetings Server Administration Guide for more information about disaster recovery. See the Cisco Webex Meetings Server Planning Guide for more information about CUCM configuration.


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

<table>
<thead>
<tr>
<th>SIP Trunk</th>
<th>SIP Trunk Security Profile: X.509 Subject Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP trunk for a load balance point at the second data center</td>
<td>Site URL for the first data center (FQDN format)</td>
</tr>
<tr>
<td>SIP trunk for an application point at the second data center</td>
<td>Site URL for the first data center (FQDN format)</td>
</tr>
</tbody>
</table>
CHAPTER 6

Downloading Applications

- The Cisco Webex Meetings Desktop Application Fails to Open, on page 17
- Error 1316 Occurs During Application Installation, on page 17

The Cisco Webex Meetings Desktop Application Fails to Open

**Problem** Users can't open the Cisco Webex Meetings desktop app for Windows, when they connect to their corporate intranet using Cisco Any-Connect VPN Client. This issue occurs only after users install the Cisco Webex Meetings desktop app, the first time that they join a meeting.

**Problem** This problem doesn't occur when the user attempts to join the meeting without VPN turned on. If you enable your Webex site for public access, external users can join meetings without using the VPN.

**Possible Cause** Users have an outdated version of Java.

**Solution** Update your end-user Windows desktops to the latest Java version. If the Java update doesn't work, have users manually install the Cisco Webex Meetings desktop app from the Downloads page. These workarounds assume that users have administrator privileges to install applications on their PCs. If they don't have administrator privileges, you can push the Cisco Webex Meetings desktop app to their PCs.

Error 1316 Occurs During Application Installation

**Problem** While installing one of the application downloads (Cisco Webex Meetings Desktop Application 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** Do one of the following actions:

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

- **Solution** Uninstall the existing application and reinstall it.
Error 1316 Occurs During Application Installation
Emails

- Administrators and Users Are Not Receiving Emails, on page 19
- SMTP Email Server Issues on a System with TLS-Based Authentication, on page 19
- Administrators Do Not Receive the Notification Emails for Reports, on page 20

Administrators and Users Are Not Receiving Emails

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 correctly, 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. See the Administration Guide for Cisco Webex Meetings Server for more information about how to configure an SMTP server.

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.
Administrators Do Not Receive the Notification Emails for Reports

**Problem** An administrator selects **Customize Reports** to request system logs, but the administrator does not receive email notification after the logs are collected.

**Possible Cause** The NTP server may be down or unreachable.

**Solution** Make sure that there is an NTP server configured properly on the ESXI hosts of your Cisco Webex Meetings Server with your virtual machines. Verify that the NTP server is operational and reachable. If your NTP server is operational, contact Cisco Technical Assistance Center (TAC) for further assistance.
General

- Text Fields Have Angled Corners Instead of Rounded Corners, on page 21

Text Fields Have Angled Corners Instead of Rounded Corners

**Problem** Text fields appear with angled corners instead of rounded corners.

**Possible Cause** You are using an outdated version of Microsoft Internet Explorer.

**Solution** Use Internet Explorer 10 or higher in standard mode (not compatibility mode). Do not use Internet Explorer 7.
Text Fields Have Angled Corners Instead of Rounded Corners
CHAPTER 9

Installation and Deployment

• Use of Forward Proxies in Your System, on page 23
• Use of Reverse Proxies in Your System, on page 24
• Auto-Deployment Fails with error.deploy_summary.353, on page 24
• Auto-Deployment Fails with error.deploy_summary.363 or error.deploy_summary.365, on page 25
• Deployment Fails with an "Unsupported Configuration" Error, on page 25
• The End User Download Page is Broken After Completing an Update, on page 25
• Invalid Passphrase URL Error, on page 25
• Unable to Install Cisco Webex Meetings Server, on page 26
• The System Displays a Pre-check Error During an Update or Upgrade, on page 26

Use of Forward Proxies in Your System

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 recommend you minimize such elements, because each intervening network element can introduce network latencies. Latency results in a poor user experience for aspects of Cisco Webex meetings, including Webex Video, Voice Connection using computer, and screen sharing. Intervening elements can also affect the contents of each networking packet in unpredictable ways that could break these features.

If your end users experience these issues, remove the intervening networking elements from your system. Check to see whether the problems are resolved.

Note
Using forward proxies can 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 for processing packets. Forwarding proxies that check the packet content may not be able to process packets in under 10 ms. Latency affects 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).
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 can bypass the Internet Reverse Proxy (for "internal" users). In this scenario, the forward proxy must allow the system to redirect HTTPS connections between the 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 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 Cisco Webex Meetings Server is supported. The Internet Reverse Proxy provided with this product is optimized for handling real-time web, audio, and data-sharing traffic from external users joining meetings from the Internet.

Internet Reverse Proxies or web load balancers supplied by other vendors, are not supported.

Auto-Deployment Fails with 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
Ensure that the OVA downloaded from Cisco contains the correct checksum.

Solution
Ensure that the datastore is available and not actively running any applications.

Solution
Ensure that there are no visible storage alarms in VMware vCenter.
Auto-Deployment Fails with error.deploy_summary.363 or 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** Click **Start Over** to restart the deployment.

Deployment Fails with an "Unsupported Configuration" Error

**Problem** Cisco Webex Meetings Server system deployment fails with an "Unsupported Configuration" error.

**Possible Cause** Check the CPU and memory reservations for the virtual machines on the host server. Confirm that there are no other virtual machines on the host server other than the supported Cisco Webex Meetings Server virtual machines.

**Possible Cause** The hardware or storage might have issues resulting in the calibration test failure.


The End User Download Page is Broken After Completing an Update

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

**Possible Cause** Static resources are cached to enhance the performance of web pages. Javascript files might be cached where the Javascript files are loaded from the local machine instead from the server. Alternately, end users might be using an older version of their web browser.

**Solution** Have users clear their browser cache and try re-accessing the download page. Ensure that they are using supported browser versions.

Invalid Passphrase URL Error

**Problem** The "Invalid Passphrase" message can appear because the URL was entered incorrectly. Rebooting the primary or secondary Admin virtual machine during a deployment, or changing the deployment URL can also cause this error.

**Solution** If the error is a result of the Admin virtual machine reboot, delete the Admin virtual machine in the vCenter and restart the deployment from the beginning.

**Solution** If other virtual machines were connected during the deployment, you must also delete those virtual machines and redeploy them.
Unable to Install Cisco Webex Meetings Server

Problem: Unable to install Cisco Webex Meetings Server on a virtual machine.

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

Solution: Ensure that you are using a supported version of VMware ESXi. For more information, see the planning guide for your release of Cisco Webex Meetings Server.

The System Displays a Pre-check Error During an Update or Upgrade

Problem: During an update or upgrade, the Administration page displays an error indicating that the pre-check failed and the process fails.

Problem: When an administrator is asked to confirm an Update or an Upgrade, the process does not continue. The system displays the same page, asking you to confirm the update or the upgrade.

Possible Cause: The system caches static resources to enhance the performance of web pages. The data in the cache might be incorrect.

Solution: Clear the browser cache and re-try the process.
Licenses

- Cisco Webex Meetings Server Is Running in Evaluation Mode, on page 27

Cisco Webex Meetings Server Is Running in Evaluation Mode

**Problem** In Webex Administration, your system shows that it is running in Evaluation mode.

**Possible Cause** This behavior is by design. After you deploy your system, you have 90 days to purchase licenses and to register with the Smart Software Manager.

**Solution** Before the 90–day Evaluation period expires, purchase licenses and register with the Smart Software Manager.
Cisco Webex Meetings Server Is Running in Evaluation Mode
CHAPTER 11

Maintenance Mode

- The “Rebooting” Message Does Not Go Away after You Turn off Maintenance Mode, on page 29
- Request to Turn Maintenance Mode on or off is Rejected, on page 29

The “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 Webex Administration 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 attempted to turn on Maintenance Mode, or turn off Maintenance Mode, too quickly.

**Solution** Wait a few seconds and retry changing the status.

**Possible Cause** A system-altering change is not complete (for example, adding or removing High Availability).

**Solution** Wait 30 minutes, and then turn on Maintenance Mode, or turn off Maintenance Mode.
Recordings

- Cannot Start or Join Meetings, or View Recordings, on page 31
- Recordings Do Not Appear on the Host Recordings Pages, on page 31
- Meeting Recordings Do Not Appear on the Recordings Page, on page 32
- Clicking the Record Button Generates a Server Connect Error, on page 32
- Cannot Add a Storage Server, on page 32
- Meeting Recording Is Disabled, on page 32
- The Record Button is Disabled, on page 32
- Record Button Is Not Available After Secure Storage Is Restored, on page 33
- The Recording Panel Generates an Error, on page 33
- Some Users Do Not Receive Links to Their Meeting Recordings, on page 34

Cannot Start or Join Meetings, or View Recordings

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

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

**Solution** Upgrade to the latest Java version. You can also try reinstalling the Cisco Webex Meetings client and Network Recording Player.

Recordings Do Not Appear on the Host Recordings Pages

**Problem** Meeting recordings do not appear on the Recordings page for any host user, including those who enabled recording in meetings.

**Possible Cause** There is a permission issue for the storage server mount point.

**Solution** In Webex Administration, go to System > Servers > Storage Server Configuration. Ensure that the permissions are set correctly.
Meeting Recordings Do Not Appear on the Recordings Page

**Problem** The meeting host receives notifications that recordings are available, and more than 10 minutes have passed since the recorded meetings ended. However, the meeting recordings do not appear on the **Recordings** page.

**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 `chmod -R 777 mount point directory`. To recover the meeting records that were not generated on the **Recordings** page, contact Cisco TAC.

Clicking the Record Button Generates a Server Connect Error

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

**Possible Cause** The Tomcat user for Cisco Webex Meetings Server 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 Tomcat user for Cisco Webex Meetings Server 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 Is Disabled

**Problem** When Storage usage exceeds the threshold, the Storage status appears in red on the Administration Dashboard. You receive a Storage Alarm email notification (if Storage alarm is enabled), and the recording of new meetings is disabled.

**Possible Cause** The allocated storage space is insufficient for the number of meeting recordings.

**Solution** Set the storage threshold to the maximum, calculated as (the total space - recording buffer size) where the recording buffer size is 1 GB for micro, 5 GB for small, 16 GB for medium, or 40 GB for large systems.

The Record Button is Disabled

**Problem** Meeting hosts cannot record meetings because the **Record** button is disabled (dimmed).

**Possible Cause** NAS is not attached to Cisco Webex Meetings Server.
1. **Solution** Sign in to Webex Administration and go to **System > Servers**.

2. **Solution** Click **Add Storage Server**.

3. **Solution** Specify the NFS server and mount point.
   
   **Solution Example:** `170.70.80.90:/path to mount point on server`.
   
   **Possible Cause** Recording is not enabled on Cisco Webex Meetings Server.

1. **Solution** Sign in to Webex Administration and go to **Settings > Meetings**.

2. **Solution** Check **Record** under **Participant Privileges**.

   **Possible Cause** The storage server capacity is at the specified limit.

   **Solution** Increase the specified limit for storage capacity.

1. **Solution** Sign in to Webex Administration and go to **Dashboard > Alarms**.

2. **Solution** Click **Edit**.

   **Solution Check Storage**.

3. **Solution** Drag the slider for the storage limit on **Edit Alarms** to increase the storage, and then click **Save**.

   **Solution** Alternatively, you can delete files from the storage server mount point to create more space.

   **Possible Cause** The storage server is stopped, or the NFS service on the NAS is stopped or restarting, preventing Cisco Webex Meetings Server from accessing the mount point.

1. **Solution** Sign in to Webex Administration and go to **System > Servers > Storage Server**.

2. **Solution** Reconfigure NAS.

---

### Record Button Is Not Available After Secure Storage Is Restored

**Problem** After restoring secure storage, the **Record** button does not appear during meetings.

- **Possible Cause** A Secure Storage (SFTP) server is configured as the CWMS storage server.
- **Possible Cause** SFTP goes down and becomes inaccessible.
- **Possible Cause** The administration page indicates that the storage server is unreachable.
- **Possible Cause** Secure storage comes back online and is reachable.
- **Possible Cause** Users start meetings and the **Record** button does not appear.

**Solution** Restart the system.

### The Recording Panel Generates an Error

**Problem** During a meeting that is being recorded, the recorder panel shows an error. When you mouse over the panel, it indicates an audio or video error.
Some Users Do Not Receive Links to Their Meeting Recordings

Problem Some users on the system do not receive the links to their meeting recordings. Recording appears to work normally during the meeting.

Possible Cause The system generates the files in the <current year> directory on NFS storage. However, the system does not create a directory and copy the files into the 1 directory on NFS, and therefore doesn't create the link.

Solution
- Set Anonymous to 65534 on NFS server and then remount it.
- Run `sudo /etc/init.d/rpcidmapd start` and then re-mount the remote file.
- Verify that everyone has full permissions on the NFS mount:
  - SSH to Admin VM. (Contact TAC if necessary.)
  - Run `chmod -Rf 777 /opt/cisco/webex/storage/nbr`.

References
- http://www.serverlab.ca/tutorials/windows/storage-file-systems/configuring-an-nfs-server-on-windows-server-2012-r2/
CHAPTER 13

Servers

- SMTP Sends Delivery Failure Replies, on page 35
- Users Are Seeing NTP Alerts, on page 35
- The Storage Server Is Not Backing up the System or the Recordings, on page 36
- Repeated Kernel Errors Appear in the Syslog, on page 36
- The CWMS System Fails to Boot up after an Update or Upgrade, on page 36

SMTP Sends Delivery Failure Replies

Problem A user sends an email to an administrator and the system sends a reply to notify them that their message is undeliverable.

Possible Cause This issue can occur if the administrator password contains a special character, such as ^, &*, (, _, +, or /.

Solution To resolve this issue, administrators must ensure that their passwords do not contain unsupported characters.

Users Are Seeing NTP Alerts

Problem An NTP alert appears at the top of the page, after the user logs in.

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

1. Solution Wait to see whether the message clears after the 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, see your VMware vSphere documentation.

3. Solution Confirm that the NTP Server is configured on the host (Configuration > Time Configuration).

4. Solution Confirm that NTP services are running.

5. Solution Ensure that Startup police is set to start and stop with the host (Configuration > Time Configuration > Properties > Option > General).
The Storage Server Is Not Backing up the System or the Recordings

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

**Possible Cause** Your storage server cannot connect with the virtual machines on your system.


**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. Determine whether mount/access is possible from a non-Cisco Webex Meetings Server machine. Ensure that your storage server is not full.

Repeated Kernel Errors Appear in the Syslog

**Problem** VMware does not support virtualized drive cache for the virtual disks that CWMS uses. When you configure CWMS to automatically report syslog errors, to a remote syslog server, each server in a CWMS cluster reports the messages every few minutes.

**Problem** kernel: sd 2:0:2:0: [sdc] Assuming drive cache: write through, kernel: sd 2:0:3:0: [sdd] Assuming drive cache: write through

**Problem** The system generates one of these messages for each disk, on each server, in the deployment. The errors also appear in the messages logged on the virtual machine.

**Possible Cause** CWMS checks to see whether some volumes are resized. When the Linux kernel tries to configure the maximum performance parameters, it detects that caching is not available, logs the issue, and the process continues.

**Solution** This is expected behavior. No action is required.

The CWMS System Fails to Boot up after an Update or Upgrade

**Problem** When you update or upgrade the CWMS system and attempt a restart, the system does not boot up.

**Possible Cause** This issue can occur if DNS entries are missing or changed.

**Solution** Shutdown guest on all virtual machines. Correct the DNS entries and power on the servers.
Sign in and Meeting Issues

• Account Activation Fails, on page 37
• Webex Meetings Desktop App Fails to Start Meetings, on page 38
• Missing Personal Room Tab, on page 38
• Missing Avatar for a Mobile User, on page 38
• Users Are Not Seeing 720p Resolution, on page 38
• Automatic Sign-in or Sign-out Problems Occur after Importing Cookies from Microsoft Internet Explorer, on page 39
• You Cannot Connect to the Webex Site or to Webex Administration, on page 39
• Forwarded Meeting Invitations Do Not Work after an Upgrade, on page 40
• Forgotten Password Audio Captcha Fails in IE, on page 40
• Graphics Quality Degrades During Application or Desktop Sharing, on page 40
• A Meeting Does Not Appear on the Meetings Page, on page 40
• The Start Button Still Appears after a Participant Joins the Meeting, on page 41
• Maximum Meeting Capacity Exceeded, on page 41
• Meeting Issues Email Received, on page 41
• Meeting Participants Cannot Dial out to Their Phones, on page 41
• Meeting Trend Data is One Hour Later on the One-Day and One-Week Charts, on page 42
• Unable to Start a Meeting on Mozilla Firefox or Google Chrome, on page 42
• A User Cannot Schedule Meetings with Webex Desktop Meetings Application, on page 42
• A User Cannot Host or Attend Meetings, on page 43
• Users Cannot Start or Join Meetings, on page 43
• URL Entered in Mixed Case, on page 43
• User Is Dropped from an Audio Conference, on page 43
• WBX*INPROGRESSMEETING Table Does Not Record Data When a Meeting Ends, on page 43

Account Activation Fails

**Problem** An administrator or user receives notification that their account is activated, but they cannot sign into the account.

**Possible Cause** The account activation period has expired. After an account is activated, administrators have two days and end-users have three days to sign in, before the account deactivates.
Solution Go to the sign-in page and click the Forgot Password link. When you receive the email, follow the instructions to reset your password and sign into your account.

Webex Meetings Desktop App Fails to Start Meetings

Problem The Webex Meetings desktop app fails to start meetings.

Possible Cause There might be a communication issue between the application and the Cisco Unified Communications Manager.

Solution Gather the following information and contact TAC:
- Steps to reproduce the issue, with screenshots
- Outlook version
- Outlook Event logs (optional)
- Exchange server version
- Webex Meetings desktop app version
- Webextracer logs.

Solution Help > Send Problem Report
- Fiddler logs (get API response)

Missing Personal Room Tab

Problem After signing in to the Webex site, users cannot see the Personal Room tab in Modern View.

Possible Cause You have not enabled Personal Room for your site.

Solution Sign in to Webex Administration and check the settings: Settings > Meetings
- Enable both Enable Modern View and Enable Personal Room.

Missing Avatar for a Mobile User

Problem A user uploads a new avatar, but the avatar does not appear on their mobile device.

Possible Cause The URL for the avatar on the server might not be correct.

Solution Use GetUserXML API to check the URL for the avatar. Look for use: avatar - use:url. Copy the URL and paste it into a web browser to see whether the URL points to the avatar image.

Users Are Not Seeing 720p Resolution

Problem Users are not seeing 720p resolution in meetings.

Possible Cause The feature is not enabled for your site.
**Sign in and Meeting Issues**

**Automatic Sign-in or Sign-out Problems Occur after Importing Cookies from Microsoft Internet Explorer**

**Problem** A user signs in to Cisco Webex Meetings Server using Microsoft Internet Explorer, and checks **Remember me**. If the user subsequently imports all cookies from Internet Explorer to Mozilla Firefox, they automatically sign in every time they start Firefox. Signing out manually does not resolve the issue.

**Problem** If an administrator changes the authentication key in Webex Administration, or upgrades to a new version, every time the user starts Firefox they automatically sign out of the Webex site. This occurs even if they checked **Remember me** the last time they signed in to the Webex site.

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

**Solution** Have users clear their Firefox cookies manually.

**You Cannot Connect to the Webex Site or to Webex Administration**

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

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

---

**Solution** Sign in to Webex Administration and go to **Settings > Video**. In the Webex Video section, ensure that 720p is selected.

**Possible Cause** The user's system might not support 720p.

**Solution** Ensure that end user systems meet the following minimum requirements:

- **Solution** CPU: Duo core 2.8; Quad core
- **Solution** Memory: 1G
- **Solution** Camera: HD camera support at least 15fps

**Possible Cause** Insufficient available network bandwidth can affect video performance.

**Solution** 720p resolution requires the following bandwidth:

- **Solution** Sending traffic: 1750–2380 kbps
- **Solution** Receiving traffic: 1260–1820 kbps

**Possible Cause** Cisco Webex Meetings Server is at full capacity usage.

**Solution** This is by design. There are two scripts that you can use to check the 720p status on server side:

- **Solution** QuickCheckMediaVMLog.sh—Checks all MCS logs and gathers resolution received statistics.
- **Solution** mmpVideoSummary.sh—Checks the MCS writing logs and gathers resolution received statistics.

---

**Automatic Sign-in or Sign-out Problems Occur after Importing Cookies from Microsoft Internet Explorer**

**Problem** A user signs in to Cisco Webex Meetings Server using Microsoft Internet Explorer, and checks **Remember me**. If the user subsequently imports all cookies from Internet Explorer to Mozilla Firefox, they automatically sign in every time they start Firefox. Signing out manually does not resolve the issue.

**Problem** If an administrator changes the authentication key in Webex Administration, or upgrades to a new version, every time the user starts Firefox they automatically sign out of the Webex site. This occurs even if they checked **Remember me** the last time they signed in to the Webex site.

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

**Solution** Have users clear their Firefox cookies manually.
Solution Disable FIPS.

Forwarded Meeting Invitations Do Not Work after an Upgrade

Problem A user schedules a meeting and then forwards the invitation to other participants. The participants can use the forwarded invitations to attend meetings initially. However, after a system upgrade the forwarded invitations do not work and participants see the following message: "The meeting does not exist or has already ended."

Possible Cause The upgrade procedure invalidates the meeting.

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

Forgotten Password Audio Captcha Fails in IE

Problem The audio captcha "Hear an audio challenge" to reset a forgotten password fails to play in some versions of Internet Explorer (IE). Also the message, “The file you are attempting to play has an extension (.) that does not match the file format. Playing the file may result in unexpected behavior.” might appear.

Possible Cause When using audio captcha, the audio file downloads over a secure connection and an exchange of certificates occurs. This issue can occur with an IE browser, if the CWMS server certificate is not trusted.

Solution When the message appears, click Yes. To permanently resolve this issue, accept the CWMS certificate as trusted.

Graphics Quality Degrades During Application or Desktop Sharing

Problem During application sharing or desktop sharing, the graphics quality degrades.

Possible Cause During application sharing or desktop sharing, 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 the disabled graphics settings.

A Meeting Does Not Appear on the Meetings Page

Problem A meeting configured with the “Join before host” option enabled does not appear on the Meetings page.

Possible Cause A participant joined the meeting and then left before the host joined. On the Dashboard and Meeting Trends page, the meeting appears 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 does not appear on the Meetings page.
The Start Button Still Appears after a Participant Joins the Meeting

**Problem** A meeting participant has joined a meeting by telephone, and the **Start** button still appears on the **Meetings** page.

**Possible Cause** The Host enabled one or both of the following options for the meeting: JMBH (join meetings before host) and JTBH (join teleconference before host).

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

Maximum Meeting Capacity Exceeded

**Problem:**
The following error message appears when a participant attempts 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 appears 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. After the maximum number of concurrent users have joined the Webex meeting, the remaining users can dial in to the meeting and listen. 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 in to Webex Administration and go to the **Dashboard**. Click the **Meetings** chart to see the **Meeting Trend** page. Examine the meetings that occurred at the same date and time, at which 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 Cannot 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 Webex Administration, and go to Settings > Audio > CUCM. Ensure that 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.

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.

Unable to Start a Meeting on Mozilla Firefox or Google Chrome

Problem A user attempts to start a meeting using Mozilla Firefox or Google Chrome and receives an error message such as the following:

Problem "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."

Problem Restarting the browser does not fix the issue.

Possible Cause The ActiveTouch General Plugin Container might be disabled in the web browser.

Solution On Mozilla Firefox, go to Tools > Add-ons > Plugins, and enable ActiveTouch General Plugin Container.

Solution On Google Chrome, go to the URL, "chrome://plugins" and enable ActiveTouch General Plugin Container.

Solution After enabling ActiveTouch General Plugin Container, restart the browser.

A User Cannot Schedule Meetings with Webex Desktop Meetings Application

Problem A user has the Webex Meetings Desktop Application, but cannot schedule meetings from Microsoft Outlook.

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

Solution Have the user remove the extra accounts and keep only the account that matches their Cisco Webex profile.

Possible Cause The user uses a Mac and Microsoft Outlook for Mac.
Solution Scheduling meetings is not supported with Outlook for Mac. Have the user schedule, edit, or start meetings from the Webex site.

A User Cannot 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 the Webex Meetings Desktop Application to the desktops. In Webex Administration, go to Settings > Downloads and select Manually push application to users' desktops.

Users Cannot Start or Join Meetings

Problem Users cannot start or attend meetings.

Possible Cause The network ports are not configured correctly.

Solution Ensure that your firewall or load balancing solution redirects requests to the correct ports.

URL Entered in Mixed Case

Problem Site or Webex 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 Webex Administration URL must be entered in lowercase.

User Is Dropped from an 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 a Meeting Ends

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 workaround.
CHAPTER 15

Single Sign-On

- SSO Carriage Return Failure, on page 45
- SSO Fails after Completing a Disaster Recovery Operation, on page 45
- SSO Protocol Error, on page 45
- SSO Redirection Failed Error, on page 46
- SSO Error Codes, on page 47
- SSO Does Not Work with iOS Devices, on page 48

**SSO Carriage Return Failure**

Problem The Security Assertion Markup Language (SAML) response with a carriage return is not supported.

Possible Cause If the SAML response has a carriage return in any of the fields, then the auto update account creation authentication fails. Although the SAML provider calculates the digital signature with the carriage return, Cisco Webex Meetings Server (CWMS) removes the carriage return causing the digital signature to be invalid.

Solution Remove the carriage return from all fields.

**SSO Fails after Completing a Disaster Recovery Operation**

Problem After completing a disaster recovery operation, SSO fails.

Possible Cause The SSL certificates are expired.

Solution Replace the expired certificates. For more information, see the "Generating SSL Certificates" section of the Administration Guide for Cisco Webex Meetings Server. Import the new 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.

Possible Cause The Active Directory Federation Services (ADFS) Token-Signing certificate has expired and should be updated.

• Solution Verify that the required IdP attributes are configured.

• Solution Verify that the following IdP attributes are set to the user email address: uid, SAML_SUBJECT

• Solution Export a Primary Token-signing certificate from ADFS Server > ADFS Management Console > Service > Certificate and upload it to the CWMS SSO certificate.

Solution If you cannot determine the cause of the SSO protocol error, generate a log and contact the TAC for further assistance.

SSO Redirection Failed Error

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 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 45 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 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 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 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 Update user privilege failed or user is not allowed to update user privilege. Contact your administrator for further support.


SSO Error Codes

<table>
<thead>
<tr>
<th>Error Description</th>
<th>Error Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO protocol error</td>
<td>1</td>
</tr>
<tr>
<td>No user name found in SAML assertion</td>
<td>2</td>
</tr>
<tr>
<td>No user account found in the system</td>
<td>3</td>
</tr>
<tr>
<td>Error Description</td>
<td>Error Code</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>No X.509 certificate found in the system</td>
<td>4</td>
</tr>
<tr>
<td>Only POST request is supported</td>
<td>5</td>
</tr>
<tr>
<td>Incorrect SAML SSO POST data</td>
<td>6</td>
</tr>
<tr>
<td>The site is not allowed to use SSO</td>
<td>7</td>
</tr>
<tr>
<td>Incorrect X.509 certificate to validate SAML assertion</td>
<td>8</td>
</tr>
<tr>
<td>Loading configuration error</td>
<td>9</td>
</tr>
<tr>
<td>The value of NameQualifier does not match site URL</td>
<td>10</td>
</tr>
<tr>
<td>Unable to reach Assertion Party</td>
<td>11</td>
</tr>
<tr>
<td>Failed to resolve SAML Artifact</td>
<td>12</td>
</tr>
<tr>
<td>Invalid SAML assertion</td>
<td>13</td>
</tr>
<tr>
<td>Recipient does not match webex.com</td>
<td>14</td>
</tr>
<tr>
<td>X.509 certificate has expired</td>
<td>15</td>
</tr>
<tr>
<td>User account is locked</td>
<td>16</td>
</tr>
<tr>
<td>User account is expired</td>
<td>17</td>
</tr>
<tr>
<td>User account has been deactivated</td>
<td>18</td>
</tr>
<tr>
<td>SAML assertion is expired</td>
<td>19</td>
</tr>
<tr>
<td>SAML assertion is unsigned</td>
<td>20</td>
</tr>
<tr>
<td>User role is not allowed to login</td>
<td>21</td>
</tr>
<tr>
<td>Invalid RequestedSecurityToken</td>
<td>22</td>
</tr>
<tr>
<td>Invalid digital signature</td>
<td>23</td>
</tr>
<tr>
<td>Untrusted Issuer</td>
<td>24</td>
</tr>
<tr>
<td>Name Identifier format is incorrect</td>
<td>25</td>
</tr>
<tr>
<td>Unable to generate AuthnRequest</td>
<td>26</td>
</tr>
<tr>
<td>Unable to generate Logout Request</td>
<td>27</td>
</tr>
<tr>
<td>InResponseTo does not match the request ID</td>
<td>28</td>
</tr>
<tr>
<td>Invalid Response message</td>
<td>29</td>
</tr>
<tr>
<td>Invalid Request message</td>
<td>30</td>
</tr>
<tr>
<td>Auto Account Creation failed</td>
<td>31</td>
</tr>
<tr>
<td>Auto Account Update failed</td>
<td>32</td>
</tr>
</tbody>
</table>

SSO Does Not Work with iOS Devices

Problem Single Sign-On (SSO) is not working with a user's iOS device.
Possible Cause There is a known issue with Apple iOS 6.x, where SSO does not work for internal users of iPad/iPhone who are using the Safari 6 web browser. This is due to an Apple defect that is fixed in iOS 7. The Safari bug ID is 13484525.

Solution Use a different web browser. For a list of supported browsers, see the section of the Cisco Webex Meetings Server Planning Guide and System Requirements.
Telephony

- Call Drops on a TLS High-Availability System, on page 51
- Call-In Issues, on page 51
- Call-Back Issues, on page 52
- Cannot Enter Meeting, on page 52
- EETone Does Not Play as Expected, on page 52
- Users Cannot Set EETone for Their Meetings, on page 53
- Caller ID Missing for Call-in Users, on page 53
- User Calls Drop after a Failover, on page 54
- Voice Activity Detection Support Issues, on page 54
- Secure Teleconferencing Works Only on One Data Center, on page 55

Call Drops on a TLS High-Availability System

**Problem** In a large high-availability environment that is configured for TLS (security encryption conferencing), a conference call drops.

**Possible Cause** The network connection between the primary and high-availability virtual machines drops for a few minutes, and then recovers during the meeting.

**Solution** Participants can manually rejoin the meeting.

Call-In Issues

**Problem** Users hear a reorder tone before or after they dial the complete number.

**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.
Call-Back Issues

**Problem** Users try to have the system call their phone numbers, but the phone does not ring and they 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.

Cannot Enter Meeting

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

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

**Possible Cause** 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. Verify that they each have the partition listed configured for the SIP Route Pattern for Cisco Webex Meetings Server.

EETone Does Not Play as Expected

**Problem** The Entry and Exit Tone for meetings does not play as expected.

**Possible Cause** The EETone parameters are not set correctly, or not set to pass to telephony.

**Solution** Check the following:

- Data from the database:

  ```
  selectconfid,paramname,paramvalue fromwbxmmconfparamwhereconfid=(selectconfid frommtgconferencewheremeetingtoolsid=?)andparamname='Orion_EntryExitTone';
  ```

  meetingtoolsid is the number (ID) for the meeting.

  - Check the return value for SQL:

    - 0: beep
    - 1: announce name
    - 2: no tone

    If it returns NULL, the meeting failed to set the EETone.

  - Check the trace log (wbxtra*.wbt) and search for **RollCall**:
Users Cannot Set EETone for Their Meetings

**Problem** Users cannot set the Entry and Exit Tone (EETone) at the meeting level.

**Possible Cause** Personal Conference meetings and Personal Room meetings do not support setting the EETone at the meeting level. These meetings follow the user-level setting for EETone.

**Solution** Check the meeting type. By design, Personal Conference meetings and Personal Room meetings follow user-level settings. Modern View does not support setting EETone when schedule meeting.

Caller ID Missing for Call-in Users

**Problem** Call-in users join meetings, and appear in the Participants list as Call-in User_X, instead of Call-in User_X (first name last name phone number ****).

**Possible Cause** This feature may not be enabled for your site.
Solution Sign into Webex Administration and go to Settings > Meetings. Ensure that Display Caller ID on Participants panel for Call-in Users joining by phone only.

Solution If the problem persists, gather the following information and contact TAC for assistance:

- **Solution** CUCM log (must include a SIP trace)
  - **Solution** Use the CUCM RTMT tool.
- **Solution** CWMS SIP log
  - **Solution** Check the CWMS meeting log for a particular meeting, or check the Overall System log.

*Note* If you need to check call ID text, you will need assistance from the CUCM TAC team.

## User Calls Drop after a Failover

**Problem** Calls drop after a 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 Webex Administration and go to Settings > Audio.

**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 Support Issues

**Problem** Cisco Webex Meetings Server does not recognize the remote peer Voice Activity Detection (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. Cisco Webex Meetings Server disables VAD.

**Possible Cause** By disabling VAD, codec bandwidth consumption does not exceed the standard bandwidth requirements for that codec. For example, the bandwidth consumption for G.711 is 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** Cisco Webex Meetings Server does not support VAD negotiation through SDP.
Secure Teleconferencing Works Only on One Data Center

**Problem** Secure teleconferencing in a MDC system works only on one data center; calls to other data centers fail.

**Possible Cause** Cisco Unified Communications Manager (CUCM) cannot import multiple certificates with a common name and both data centers are using the global site URL in the certificate common name (the default behavior).

**Solution** Generate or purchase a new certificate for each data center that uses the Local Site URL as the common name:

1. **Solution** Select Settings > Security > Certificates > certificates on datacentername > Generate CSR. The Generate CSR window appears.
2. **Solution** In the Common Name drop down, select the local site URL of the data center.
3. **Solution** Generate a CSR and submit to your Certificate Authority.
4. **Solution** Install the certificate on the data centers and import it into CUCM.
Secure Teleconferencing Works Only on One Data Center
CHAPTER 17

Upgrade, Update, and Expansion Issues

• Internal Server Error after Starting an Update, on page 57
• No Confirmation Message Received After Performing an Update, on page 58
• Unable to Connect to ISO Image in the CD/DVD Drive, on page 58
• No System Updated Message or the Restart Button Does Not Appear, on page 58
• Update Failure, on page 59
• The Update System Process is Stuck, on page 59
• The Upgrade Button Is Dimmed, on page 59
• Expansion Fails, on page 60
• Upgrade Credentials Are Incorrect, on page 60
• Upgrade and Original Admin VMs Are Not on the Same ESXi, on page 60
• Upgrade and Original Admin VMs Not On the Same Subnet, on page 60
• Transfer of Archived Data Failed, on page 61
• Upgrade to Incorrect Version Attempted, on page 61
• Upgrade Original HA System Connection Failure, on page 61
• Upgrade Failed to Get Data, on page 61
• Upgrade Failed Disk Space Check, on page 62
• Upgrade Failed to Join Virtual Machines, on page 62
• Update Failed the NTP Verification Check, on page 62
• Upgrade Virtual Machine Disk Format Failed, on page 63
• Upgrade System Size Mismatch, on page 63
• Original System Size Changed During Upgrade, on page 63
• Upgrade Session In Progress, on page 63
• Failed to Connect to the Original Admin Site, on page 63
• Original System Admin URL Changed during Upgrade, on page 63
• Original System Site URL Changed during Upgrade, on page 64
• Original System Version Changed during Upgrade, on page 64

Internal Server Error after Starting an Update

Problem  After starting an update, an in-progress pop up page 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.
**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 Webex Administration sign-in page and your Dashboard shows the old version.

**Possible Cause** A Webex Administration 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** During an update attempt, the system is unable to connect to the ISO image on a CD/DVD drive.

**Problem** The drive status does not progress past **Connecting**.

**Possible Cause** You might be attempting to connect to the wrong virtual machine or the connection is slow (possibly caused by activity in VMware vCenter).

**Solution** Connect the ISO image by using the vSphere client. Check that the ISO image is connected to the correct virtual machine. Webex Administration displays the hostname of the virtual machine. Ensure that it matches. It is typically the primary Administration virtual machine unless you are updating a High Availability system that is not yet attached to a primary system. If the CD/DVD drive status is **Connecting**, wait until it is finished.

**Solution** In addition, it might be necessary to close and reopen the vSphere client.

**No System Updated Message or the Restart Button Does Not Appear**

**Problem** The update completes successfully, but you do not see a **System Updated** message 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 update package archive.
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 the 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 forth.

**Solution** Roll back all virtual machines to the backup version taken before you attempted your update and retry the update.

The 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.

The Upgrade Button Is Dimmed

**Problem** The System page in Webex Administration does not have an Upgrade button or the button is dimmed.

**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 Webex Administration, start a new browser session, and then sign in again. If the issue persists, ensure that the primary administration process is still running.

**Problem** Some changes require system restart or exit from Maintenance Mode. A virtual machine is experiencing issues.
Solution  Finish the change to the system and exit Maintenance Mode prior to the update. Ensure that all virtual machines are reachable and in good (green) state.

Expansion Fails

Problem  Your 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 the expansion.

Upgrade Credentials Are Incorrect

Problem  While attempting an automatic upgrade, the original system administrator login, or the vCenter credentials, or both were found to be incorrect.

Possible Cause  The upgrade process does not have an authenticated connection that includes the vCenter credentials so that it can perform pre-checks before beginning an upgrade.

Solution  Enter the correct credentials and continue the upgrade.

Solution  Connect to the original system Admin dashboard and login. If the attempts fail, you might be asked to reset the password or authenticate with a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Once the login credentials are validated on the original system, retry the upgrade with the corrected credentials. If the vCenter credentials fail multiple times, contact the vCenter administrator to verify the credentials before retrying the upgrade.

Upgrade and Original Admin VMs Are Not on the Same ESXi

Problem  The original and the upgraded Admin virtual machines are not on the same ESXi host.

Possible Cause  The upgrade Admin virtual machine was not deployed on the same ESXi host as the original Admin virtual machine.

Solution  Delete any virtual machines created by the upgrade. Do not attempt to continue the upgrade process. Start the upgrade from the beginning and deploy both virtual machines on the same ESXi.

Upgrade and Original Admin VMs Not On the Same Subnet

Problem  The original and the upgraded Admin virtual machines are not on the same subnet.

Possible Cause  The upgrade Admin virtual machine was not deployed on the same subnet as the original Admin virtual machine.

Solution  Delete any virtual machines created by the upgrade. Do not attempt to continue the upgrade process. Start the upgrade from the beginning, with both systems on the same subnet.
Transfer of Archived Data Failed

**Problem** Transfer of archived data fails. Upgraded system has snapshots.

**Possible Cause** At least one virtual machine vCenter snapshot exists.

**Solution** Delete all the snapshots on all upgraded system virtual machines and continue.

Upgrade to Incorrect Version Attempted

**Problem** Attempt to upgrade to an incorrect version.

**Note** The error message might indicate a connection failure.

**Possible Cause** Attempted an upgrade to the wrong version.

**Possible Cause** Attempted to upgrade to the wrong type of system, such as attempting to upgrade an Audio Encrypted (AE) system with an Audio Unencrypted (AU) image or vice versa.

**Possible Cause** Attempted to perform an upgrade while expanding the system.

**Possible Cause** Attempted an upgrade with system redeployment that is not supported for this version.

**Possible Cause** Chosen upgrade path is not supported.

**Solution** Upgrade to the correct version.

Upgrade Original HA System Connection Failure

**Problem** Attempting to connect to the original High Availability Admin fails.

**Note** The error message might indicate a mismatch version instead of a connection failure.

**Possible Cause** The original High Availability system is up.

**Possible Cause** For a Manual Upgrade, the original system might not be shut down.

**Possible Cause** For Automatic Upgrade, the original system was brought up after the upgrade process shutdown that system.

**Solution** Bring down the original High Availability system and continue the upgrade.

Upgrade Failed to Get Data

**Problem** The attempt to get data from the original system failed.

**Possible Cause** Multiple attempts to perform *Prepare For Upgrade* on the original system.
Possible Cause The deployment data could not be validated.
Possible Cause Deployment data initialization failed.
Possible Cause Unable to complete archiving data on original system.
Possible Cause An error occurred while transferring archived data to the upgrade system.
Possible Cause Unable to complete the validation of archived data.

Solution Exit Maintenance Mode on the original system and after that system is in a normal state, retry the upgrade.
Solution Re-enter the Admin URL and continue the upgrade.

Upgrade Failed Disk Space Check

Problem During an automatic upgrade, the disk space check fails.

Possible Cause Not enough disk space to deploy the virtual machines during automatic upgrade. Sufficient disk space to support the upgrade must be available on each of the datastores that are used by the original system. For each virtual machine, the upgrade system automatically uses the same datastores as the original system.


Upgrade Failed to Join Virtual Machines

Problem Joining the virtual machines failed.

Possible Cause One or more of the virtual machine checks, such as power up, version, type, size, or state, failed.

Solution Correct the issue and continue the upgrade.

Update Failed the NTP Verification Check

Problem CWMS update fails with an error message indicating that the verification failed or the system is not in a good state for updating.

Possible Cause NTP might not be running on all UCS hosts.

Solution Shutdown all virtual machines on the hosts. Configure the NTP server on the UCS hosts under Configuration > Time Configuration. We recommend that you select Start and Stop with Host under the NTP server settings. When the NTP configuration is complete, power on the virtual machines.

Solution (See also Users Are Seeing NTP Alerts.)
Upgrade Virtual Machine Disk Format Failed

**Problem** The VMware Virtual Machine Disk (VMDK) format failed.

**Possible Cause** The VMDK failed.

**Solution** Keep the Admin virtual machine powered off. Delete the VMDK files from the upgrade Admin virtual machine and replace them with the corresponding files from the original Admin virtual machine. Continue with the upgrade.

Upgrade System Size Mismatch

**Problem** You receive a System Size Mismatch error during an upgrade.

**Possible Cause** The size of the upgraded system does not match the size of the original system.

**Solution** In the vCenter, power down the upgrade Admin virtual machine and delete it. Redeploy the OVA and select the upgrade Admin virtual machine for the correct size.

Original System Size Changed During Upgrade

**Problem** The size of the original system has been changed since the start of the Automatic Upgrade process.

**Possible Cause** Changes were made to the original system after the Auto-Upgrade process was initiated.

**Solution** Remove the virtual machines from the upgrade system and start the Automatic Upgrade process from the beginning.

Upgrade Session In Progress

**Problem** An upgrade session is already in progress.

**Solution** The browser automatically refreshes and displays the current status.

Failed to Connect to the Original Admin Site

**Problem** During an upgrade, failed to connect to the original Admin site.

**Possible Cause** The original system might be in a transient state.

**Solution** Verify that the original system is in healthy state and then retry the automatic upgrade.

Original System Admin URL Changed during Upgrade

**Problem** The Admin URL of the original system has changed since the start of the Automatic Upgrade process.

**Possible Cause** Changes were made to the original system after the Auto-Upgrade process was initiated.
Original System Site URL Changed during Upgrade

**Problem** The Site URL of the original system has changed since the start of the Automatic Upgrade process.

**Possible Cause** Changes were made to the original system after the Auto-Upgrade process was initiated.

**Solution** Remove the virtual machines of the upgrade system and start the Automatic Upgrade process from the beginning.

Original System Version Changed during Upgrade

**Problem** The version of the original system has been changed since the start of the Automatic Upgrade process.

**Possible Cause** Changes were made to the original system after the Auto-Upgrade process was initiated.

**Solution** Remove the virtual machines of the upgrade system and start the Automatic Upgrade process from the beginning.
User Management

- Auto Account Creation or Auto Account Update Failed, on page 65
- Importing Users with a CSV File Fails, on page 67
- No User Account Found in the System, on page 68

Auto Account Creation or Auto Account Update 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 (\textit{SAML\_SUBJECT} is not required in ADFS 2), the following mapping is required:

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail-Addresses</td>
<td>Name_ID</td>
</tr>
<tr>
<td>E-Mail-Addresses</td>
<td>email</td>
</tr>
</tbody>
</table>
### LDAP Attribute

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given-Name</td>
<td>firstname</td>
</tr>
<tr>
<td>Surname</td>
<td>lastname</td>
</tr>
</tbody>
</table>

#### Note

- **Solution** We recommend that you map the Name_ID to the email address.
- **Solution** The attribute name is case sensitive. Ensure that 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 a dropdown menu.

### SSO URL API Reference

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firstname</td>
<td>String</td>
<td>User's first name is required with a maximum length of 32 characters.</td>
</tr>
<tr>
<td>lastname</td>
<td>String</td>
<td>User's last name is required with a maximum length of 32 characters.</td>
</tr>
<tr>
<td>email</td>
<td>String</td>
<td>User's email address is required with a maximum length of 64 characters.</td>
</tr>
<tr>
<td>Argument</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>TC1</td>
<td>String</td>
<td>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.</td>
</tr>
</tbody>
</table>

- If the tracking code is configured as required, then you must provide the value.
- If the input mode for current tracking code is **Dropdown menu**, then if you provide the value that you configure in the dropdown menu.

**Note** The value must be active in the dropdown menu.

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

- **User configuration:**
  - Webex Administration: Go to Users > **Edit User** to display the user account fields.
  - End-user site: Click **My Account** to display the user account fields.

- **Tracking code configuration:**
  - Webex Administration: Go to Users > Tracking Codes and set your **Input mode** to Dropdown menu. Configure your Usage setting. Then click **Edit list** to configure the dropdown menu.

---

**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** Modify the CSV file by using a spreadsheet, such as Excel (recommended, with tab delimiters), or a text tool, such as Notepad.

**Solution** Save the file as unicode UTF-16 (*.txt) or as a comma-separated value (*.csv) file.
Solution If the file extension is anything other than *.csv, rename the file.

Solution Import the corrected CSV file into Cisco Webex Meetings Server, selecting the tab delimited file option.

Solution The Auditor role cannot be transferred by using the CSV file.

Problem The Auditor role does not transfer with the CSV file.

Possible Cause This is by design.

### No User Account Found in the System

**Problem** A user receives 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** Ensure that you have added the user on the system and that auto account creation is turned on.
CHAPTER 19

Virtual Machine Issues

- Administration Virtual Machine on Your Primary or High-Availability System is Down, on page 69
- NIC Teaming Issues, on page 69
- A Virtual Machine Does Not Boot up after Deployment, on page 70
- A Virtual Machine Fails and Cannot Be Recovered, on page 70
- Virtual Machine Issues and Crashes, on page 70
- Virtual Machine Is Unreachable, on page 71
- Virtual Machine Repeatedly Reboots, on page 71
- A Virtual Machine Repeatedly Reboots after a Power Outage, on page 71

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

**Problem** The 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.

### A Virtual Machine Does Not Boot up after Deployment

**Problem** A 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.

### A 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. For more information, see the *Cisco Webex Meetings Server Administration Guide*. 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. For more information, see the *Cisco Webex Meetings Server Administration Guide*. For any other virtual machine, rebuild your system using the Disaster Recovery feature. For more information, see the *Cisco Webex Meetings Server Administration Guide*.

### Virtual Machine Issues and Crashes

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

**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** 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.
Virtual Machine Issues

Virtual Machine Is Unreachable

**Problem** The primary virtual machine is unreachable. Users cannot access the Administration site and cannot access the Webex site to start or schedule meetings. Administrators cannot make a SSH connection to the virtual machine. Fail over to the High Availability system does not occur.

**Possible Cause** The disk hosting the primary Admin virtual machine is inaccessible because it has failed.

**Solution** Using VMware vCenter, shut down the inaccessible virtual machine. By doing this, the failover process to the HA system completes successfully. When the hardware problem is resolved, contact Cisco TAC for assistance in restoring your primary virtual machine.

Virtual Machine Repeatedly Reboots

**Problem** The virtual machine on which the Cisco Webex Meetings Server OVA is deployed, 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.

A Virtual Machine Repeatedly Reboots after a Power Outage

**Problem** A virtual machine is stuck in a reboot loop, after a power outage. The operating system does not load. No SSH or GUI access is available.

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

**Solution** When the affected virtual machine boots, look for the following message on the console: **Booting CentOS (<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**.

• **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](http://www.cisco.com/cisco/web/support/index.html)
A Virtual Machine Repeatedly Reboots after a Power Outage