Cisco WebEx Meetings Server Troubleshooting Guide

First Published: October 23, 2012

Last Modified: October 23, 2012

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

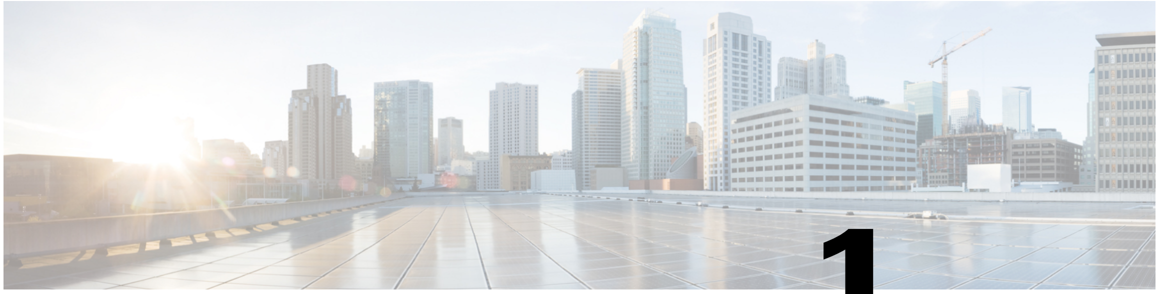
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

CONTENTS



CHAPTER 1

Alarms and Logs

This section includes troubleshooting topics about alarms and logs.

Log Capture Size Problems

Problem The log capture size can become too large.

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

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

CHAPTER 2

Certificates

This section includes troubleshooting topics about certificates.

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 Not Yet Valid Error

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

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

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

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

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

Expired Certificate Error

Problem You receive an expired certificate error.

Possible Cause The validity period of the certificate has ended.

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

Incorrect X.509 Certificate to Validate SAML Assertion

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

Possible Cause Your certificate or IdP is not valid.

Solution Validate your certificate or IdP as necessary.

Invalid Certificate Error

Problem You receive an invalid certificate error.

Possible Cause The certificate file is malformed.

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

- **Solution** Make sure the certificate is in a supported format.

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

Invalid Domain Error—Wildcard Certificate

Problem You receive an invalid domain error message.

Possible Cause The user uploaded a wildcard certificate. The domain in the CN does not match the domain of the site URL.

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

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

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

Invalid Domain Error—SAN Certificate

Problem You receive an invalid domain error message.

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

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

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

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

Key Decryption Error

Problem You receive a key decryption error.

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

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

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

Key Size Error

Problem You receive a key size error message.

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

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

Self-Signed Certificate After Upgrade

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

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

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

Third Party Certificates - Private-key Auto-Generated by the System is not Compatible with the Certificate

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

Possible Cause CUCM check X509 Extended Key Usage in certificate.

Solution Include this extension in CSR when applying for certificate. The third party certificate should have this extension:

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

Untrusted Connection

Problem You receive an untrusted connection message. This might be caused by the following:

- **Problem** A client-side error.
- **Problem** The client is not able to verify the Cisco WebEx Meetings Server certificate using its truststore.

Problem Microsoft Internet Explorer uses the operating system truststore. Mozilla Firefox uses its own built-in truststore. To view Windows trusted root certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx. To view Windows trusted root certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx. On a Windows system, select **Tools** > **Options**. Then select **Advanced** > **Encryption** > **View Certificates** > **Authorities**. On a Mac, select **File** > **Preferences**. Then select **Advanced** > **Encryption** > **View Certificates** > **Authorities**.

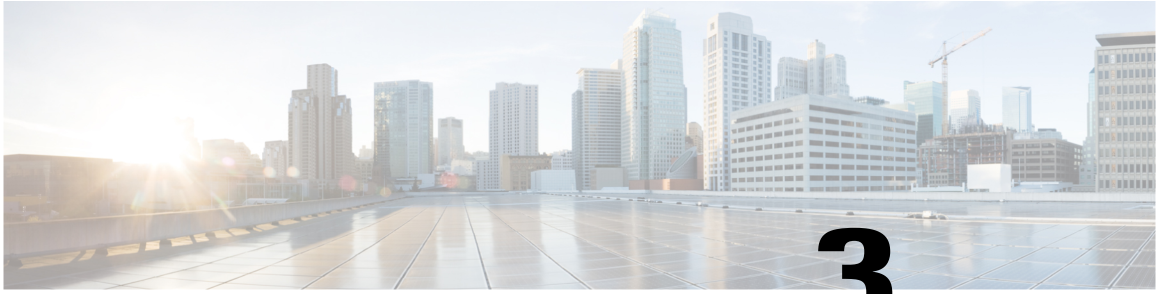
Possible Cause The system is using a self-signed certificate. This may occur because the system is a new installation or the customer had an existing certificate but performed an operation which invalidated that certificate and the system generated a self-signed certificate in its place.

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

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

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

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



CHAPTER 3

Downloading Applications

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

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

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

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

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

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

Signing into a SSO Site Using the Productivity Tools Fails

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

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

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

Cisco WebEx Meetings Fails to Launch

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

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

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

Solution Update your end-user Windows desktops to the latest Java version found on www.java.com. If this does not work, we recommend that you tell your users to manually install the Cisco WebEx Meetings application from the **Downloads** page. Alternatively users can download the Cisco WebEx Meetings application when they attempt to join the meeting for the first time.

Note **Solution** The above workarounds assume user PCs in your organization have administrator privileges. If they do not have administrator privileges, you can push the Cisco WebEx Meetings application to their PCs using the installation files provided on the **Download** page.

Error 1316 Received During Application Installation

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

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

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

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

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

CHAPTER 4

Emails

This section includes troubleshooting topics about emails.

Create Password Not Sent to User, FTE Not Complete

Problem A user has not received a create password email from the first administrator after completing the first-time experience wizard.

Possible Cause The incorrect email server information was entered.

1 **Solution** Go to the last page of FTE and select the **Resend email** link.

2 **Solution** Go back to FTE and navigate (using the back and forward buttons) to the email server configuration page and make sure it is correct. Then navigate back (using the forward button) to the last page in FTE and select the **Resend email** link.

Emails are not Being Received by Administrators and Users

Problem Emails are not being received by administrators and users.

Possible Cause Possible causes include:

- **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 Solutions include:

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

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

CHAPTER 5

Installation and Deployment

This section includes troubleshooting topics about installation and deployment issues.

Use of Forward Proxies in Your System

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

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

Performance Considerations

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

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

Functionality

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

Use of Reverse Proxies in Your System

Only the Internet Reverse Proxy provided with this product may be used in this system. Internet Reverse Proxies or web load balancers, supplied by other vendors, are not supported. The Internet Reverse Proxy provided with this product is optimized for handling real-time web, audio, and data-sharing traffic from external users joining meetings from the Internet.

Auto-Deployment Fails for error.deploy_summary.353

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

Possible Cause The previously downloaded OVA is corrupted.

- **Solution** Check to determine if the OVA downloaded from Cisco contains the correct checksum.
- **Solution** Make sure the datastore where new virtual machines are being deployed is available and not actively running any applications.
- **Solution** Make sure there are no visible storage alarms seen in VMware vCenter.

End User Download Page is Broken After Completing An Update

Problem End users are not able to access download link.

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

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

Unable to Install Cisco WebEx Meetings Server

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

Possible Cause Your version of VMware ESXi is not supported.

Solution Make sure you are using VMware ESXi 5.0. Version 4.x is not supported.

CHAPTER 6

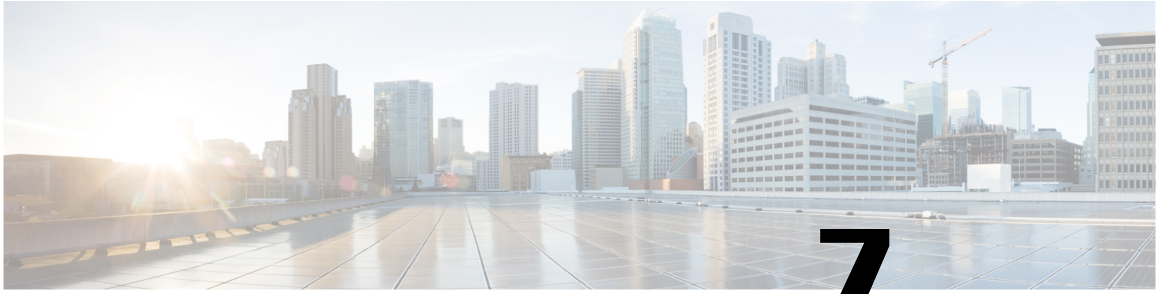
Licenses

Free Trial Alert Message Appears

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

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

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



CHAPTER 7

Maintenance Mode

This section includes troubleshooting topics about maintenance mode issues.

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 Uncertain. This is a known issue.

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

Request to Turn Maintenance Mode On or Off is Rejected

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

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

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

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

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

CHAPTER 8

Recordings

This section includes troubleshooting topics about recording issues.

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

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

Possible Cause Users are using unsupported Java versions.

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

Meeting Recordings Missing on Host Recordings Pages

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

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

Solution This is a known issue.

Record Button Generates Server Connect Error

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

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

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

Cannot Add a Storage Server

Problem You cannot add a storage server.

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

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

Meeting Recording Does Not Display for Host

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

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

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

The Record Button is Gray

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

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

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

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

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

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

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

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

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

Recording Panel Generates Error

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

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

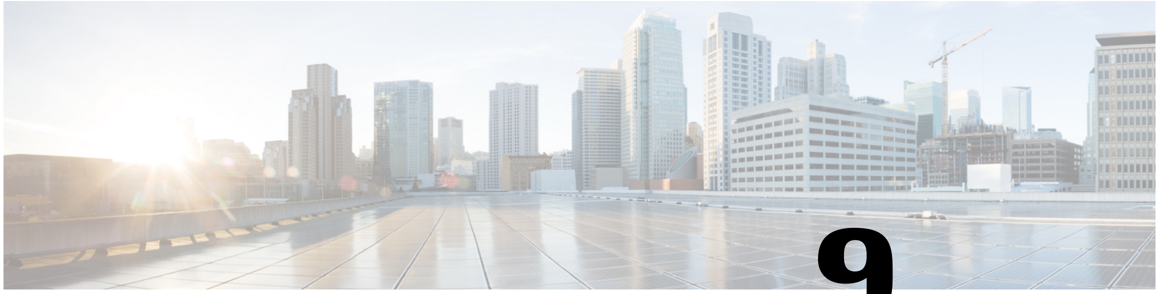
Solution Make sure that the mount point can be accessed and that Cisco WebEx Meetings Server can write to it.

Recordings Do Not Show Up on the Recordings Page

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

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

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



CHAPTER 9

Servers

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

SMTP Sends Failures When Administrator Email Uses an Underscore Character

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

Possible Cause Underscore characters are not supported for email addresses.

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

External Server Connection Issues

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

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

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

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

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

NTP-Provisioned Time out of Sync on Virtual Machines

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

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

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

2 **Solution** Confirm that all the virtual machines are using the same NTP host. Consult your vSphere documentation.

Cannot Add a Storage Server

Problem You cannot add a storage server to your system. You receive an error message that informs you that you do not have read/write privileges.

Possible Cause Your network-based recording (NBR) system will not read/write recording files to your storage server as the root user.

Solution Update your mount point 777 privileges by going to the CLI and using the command **chmod -R 777** (your mount point directory). Your users can now configure the storage server as described in Configuring a Storage Server.

CHAPTER 10

Sign In and Meeting Issues

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

Browser Compatibility Issues

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

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

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

Call Dropped on TLS High-Availability System

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

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

Solution Participants must manually rejoin their meeting.

Call-In Issues

- **Problem** Users hear a reorder tone before or after the complete number is dialed.
- **Problem** The "Your call cannot be completed as dialed" message is played by the annunciator.
- **Problem** During call-back, a user's call terminates after pressing **1** to join the meeting.
- **Problem** During call-in, a user's call terminates after entering the meeting ID followed by #.

Possible Cause You need to reconfigure your CUCM servers.

Solution Do one of the following:

- **Solution** Reconfigure your CUCM settings as follows: Use the "<NONE>" partition and "<NONE>" CSS (Calling Search Space) for all Cisco WebEx Meetings Server related entities in CUCM (for example, route patterns, SIP route patterns, SIP trunks, etc.).

- **Solution** Use one partition and one CSS specifically assigned for all Cisco WebEx Meetings Server related entities. For more information refer to the system guide for your CUCM version.

Cannot Connect to WebEx Site or Administration Site

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

Possible Cause FIPS is enabled which blocks SSL 3.0.

Solution Disable FIPS.

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

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

Possible Cause Users are using unsupported Java versions.

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

Join Before Host Meeting not Shown on Meetings Page

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

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

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

Meeting Issues Email Received

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

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

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

Meeting Participants are Unable to Dial Out to Their Phones

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

Possible Cause Your CUCM settings are configured incorrectly.

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

Meeting Status is Incorrect

Problem A meeting participant has joined a meeting but the Start button is still displayed on the **Meetings** page.

Solution This is a known issue. Incorrect status on the **Meetings** page does not affect your ability to participate in the meeting.

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

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

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

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

Meeting Participants Can Not Connect to Outside Phones

Problem Participants in meetings are unable to dial out to their phones. Participants receive a" failed to connect" error.

Possible Cause Check the CUCM settings in the audio settings (sign in to the Administration site and select **Settings** > **Audio** and select the **Edit** link under CUCM Settings), for the correct IP address, Transport and Port settings.

Solution Make sure that the port number and transport type match the corresponding settings on your CUCM servers.

Users are Unable to Host or Attend Meetings

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

Possible Cause The user has restricted PC permissions.

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

Unable to Start a Meeting

Problem Unable to start a meeting.

Possible Cause Your port numbers are not configured correctly.

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

User Calls are Dropped After Failover

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

Possible Cause Your system has TAS 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.

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.

User Cannot Access Product

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

Possible Cause Under Windows 7 32-bit and IE 8 environments, the local security setting has the following option:

Possible Cause Use FIPS compliant algorithms for encryption, hashing, and signing enabled.

Possible Cause The option path: gpedit.msc | Computer Configuration | Windows Settings | Security Settings | Local Policy | Security Options

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

User is Dropped from Audio Conference

Problem A user is dropped from an audio conference.

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

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

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

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

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

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

Cisco WebEx Meetings Fails to Launch

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

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

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

Solution Update your end-user Windows desktops to the latest Java version found on www.java.com. If this does not work, we recommend that you tell your users to manually install the Cisco WebEx Meetings application from the **Downloads** page. Alternatively users can download the Cisco WebEx Meetings application when they attempt to join the meeting for the first time.

Note **Solution** The above workarounds assume user PCs in your organization have administrator privileges. If they do not have administrator privileges, you can push the Cisco WebEx Meetings application to their PCs using the installation files provided on the **Download** page.

CHAPTER 11

Single Sign-On

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

SSO Fails After Completing Disaster Recovery Operation

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

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

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

SSO Protocol Error

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

Possible Cause The following are possible causes for this error message:

Possible Cause

- **Possible Cause** Your SSO administration site or IdP configuration contains errors.
- **Possible Cause** SSO is not enabled.

- **Possible Cause** Some or all of the required IdP attributes are not configured: firstname, lastname, email.
- **Possible Cause** The NameID parameter of your SAML is not set to email.

Solution If you are unable to determine the cause of your SSO protocol error, generate a log and contact the Cisco TAC for further assistance. If you believe the cause is one of the above, you can perform the following actions to address the problem:

Solution

- **Solution** Make sure SSO is enabled.

- **Solution** Make sure the required IdP attributes are configured.

- **Solution** Make sure the following IdP attributes are set to the user's email address: uid, SAML_SUBJECT.

SSO Redirection Has Failed

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

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

- **Possible Cause** SSO protocol error. Contact your administrator for further support. See SSO Protocol Error, on page 35 for more information.
- **Possible Cause** No user account found in the system. Contact your administrator for further support.
- **Possible Cause** No X.509 certificate found in the system. Contact your administrator for further support.
- **Possible Cause** X.509 certificate has expired. Contact your administrator for further support.
- **Possible Cause** User account is locked. Contact your administrator for further support.
- **Possible Cause** User account is expired. Contact your administrator for further support.
- **Possible Cause** User account has been deactivated. Contact your administrator for further support.
- **Possible Cause** SAML assertion is expired. Contact your administrator for further support.
- **Possible Cause** Invalid Response message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed, on page 45 for more information.

- **Possible Cause** Auto Account Update failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed, on page 45 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** 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** 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** 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 4 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** 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** SAML assertion is unsigned. Contact your administrator for further support.
- **Possible Cause** User role is not allowed to login. Contact your administrator for further support.
- **Possible Cause** Invalid RequestedSecurityToken. Contact your administrator for further support.
- **Possible Cause** Invalid digital signature. Contact your administrator for further support.
- **Possible Cause** Untrusted Issuer. Contact your administrator for further support.
- **Possible Cause** Name Identifier format is incorrect. Contact your administrator for further support.
- **Possible Cause** Unable to generate AuthnRequest. Contact your administrator for further support.
- **Possible Cause** Unable to generate Logout Request. Contact your administrator for further support.

- **Possible Cause** InResponseTo does not match the request ID. Contact your administrator for further support.
- **Possible Cause** Invalid Response message. Contact your administrator for further support.
- **Possible Cause** Invalid Request message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support.
- **Possible Cause** Auto Account Update failed. Contact your administrator for further support.
- **Possible Cause** Update user privilege failed or user is not allowed to update user privilege. Contact your administrator for further support.

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

SSO Redirection Issues

SSO redirection issues can occur due to configuration issues with your SSO URL API or your IdP settings. The following topics address SSO redirection error messages you might encounter, the issues that might cause those error messages, and how to troubleshoot them.

CHAPTER 12

Using Single User Mode for Troubleshooting

This section includes troubleshooting topics about using single user mode.

Accessing Single User Mode For Your System

Caution Only complete this procedure when instructed to do so by Cisco TAC for troubleshooting. Do not complete this procedure by yourself without assistance from Cisco TAC.

SUMMARY STEPS

1. Sign in to the vSphere client and select your VMware vCenter.
2. Select the Admin virtual machine for your system.
3. Open the virtual machine console window.
4. Power on the Admin virtual machine.
5. Once the virtual machine boots and you see the splash screen, then select the **Ctrl + Alt + Backspace** keys to get to the command-line prompt.
6. Select the **Restart Guest** button.
7. Select **Yes** to confirm the reboot. Quickly click the mouse in the console window (the black area) to set the keyboard focus to the virtual machine console. Quickly press "any key" and continue to press it about once every second, to get to the GNU GRUB boot loader menu. After a minute or two, you will see the following message: `Booting Cent OS (<string_numbers_letters>) in <number> seconds...`
8. Press any key once more to interrupt the boot process and display the GNU GRUB boot loader menu.
9. Press **e** to edit the commands before booting the virtual machine.
10. Press the down arrow key to select the "kernel" line then press **e** to edit this kernel line.
11. Enter **single**.
12. Press the Enter key to save your changes and return to the previous menu.
13. Press **b** to boot into single user mode.
14. Once the virtual machine boots and you see the splash screen, then select the **Ctrl + Alt + Backspace** keys to get to the command-line prompt.

DETAILED STEPS

Step 1 Sign in to the vSphere client and select your VMware vCenter.

Step 2 Select the Admin virtual machine for your system.

Step 3 Open the virtual machine console window.

Step 4 Power on the Admin virtual machine.

Step 5 Once the virtual machine boots and you see the splash screen, then select the **Ctrl + Alt + Backspace** keys to get to the command-line prompt.

Step 6 Select the **Restart Guest** button.

Step 7 Select **Yes** to confirm the reboot. Quickly click the mouse in the console window (the black area) to set the keyboard focus to the virtual machine console. Quickly press "any key" and continue to press it about once every second, to get to the GNU GRUB boot loader menu. After a minute or two, you will see the following message: `Booting Cent OS (<string_numbers_letters>) in <number> seconds...`

Step 8 Press any key once more to interrupt the boot process and display the GNU GRUB boot loader menu.

Step 9 Press **e** to edit the commands before booting the virtual machine.

Step 10 Press the down arrow key to select the "kernel" line then press **e** to edit this kernel line.

Step 11 Enter **single**.
This word is automatically added to the end of the kernel line.

Step 12 Press the Enter key to save your changes and return to the previous menu.

Step 13 Press **b** to boot into single user mode.

Step 14 Once the virtual machine boots and you see the splash screen, then select the **Ctrl + Alt + Backspace** keys to get to the command-line prompt.
You will not see any of the usual text on this splash screen.

The command-line window is displayed with the single user prompt `sh-3.2#`.

What to Do Next

Cisco TAC will provide you with the root credentials and further instructions. Once you complete your tasks, enter **reboot** or select the **Restart Guest** button in the virtual machine console window.

CHAPTER 13

Upgrade, Update, and Expansion Issues

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

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

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

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

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

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

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

Update System Process is Stuck

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

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

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

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

Upgrade Button Grayed Out

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

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

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

Upgrade or Expansion Fails

Problem Your upgrade or expansion attempt fails.

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

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

CHAPTER 14

User Management

This section includes troubleshooting topics about user management issues.

Auto Account Creation or Auto Account Update Has Failed

Problem You receive one of the following error messages:

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

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

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

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

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

- **Solution** If the tracking code is configured as **Required**, the attribute value must be one of the active values in the dropdown menu.

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

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

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

Note **Solution**

- **Solution** We recommend that you map the *Name_ID* to the email address.

- **Solution** The attribute name is case sensitive. Make sure the user's attribute value is not empty.

- **Solution** We recommend that you do not configure your tracking codes as **Required**.

- **Solution** We recommend that you do not configure the input mode of your tracking codes as dropdown menu.

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

SSO URL API Reference

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

Argument	Value	Description
firstname	String	User's first name is required with a maximum length of 32 characters.
lastname	String	User's last name is required with a maximum length of 32 characters.
email	String	User's email address is required with a maximum length of 64 characters.
TC1	String	User's tracking code 1. Optional/required (configured in the Administration site. Refer to the Administration Guide for more information on user management. The maximum length is 132 characters. • 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:
    - Administration site: Select **Users** > **Edit User** to display the user account fields.
    - End-user site: Select **My Account** to display the user account fields.
- Tracking code configuration:

- Administration site: Select **Users** > **Tracking Codes** and set your **Input mode** to **Dropdown menu** and configure your **Usage** setting. Then select **Edit list** to configure your dropdown menu settings.

No User Account Found in the System

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

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

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

CHAPTER 15

Virtual Machine issues

This section includes troubleshooting topics about virtual machine issues.

Virtual Machine Crashes

Problem Your virtual machine crashes and does not resume functioning.

Possible Cause

Solution Attempt to perform the following solutions:

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

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

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

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

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