



Using Your Dashboard

- [About the Dashboard, on page 1](#)
- [Viewing and Editing Alarms, on page 4](#)
- [Viewing Meeting Trends, on page 6](#)
- [Scheduling a Maintenance Window, on page 14](#)
- [About Maintenance Mode, on page 16](#)
- [Using the HostID and ConfID to Locate a Meeting Recording, on page 19](#)

About the Dashboard

The dashboard is the home page of the administration site and provides several parameters and graphs key monitoring features.

The dashboard includes the following sections:

- System Monitor—Displays the system status and timestamp and includes the following subsections:
 - Meetings and Users—Status of meetings in progress and usage. Displays the number of meetings currently in progress and the number of unique participants (usage). The status mark indicates whether the meetings in progress and usage are under or over the configured alarm threshold. A green status mark indicates that the system is under a configured threshold. A red status mark indicates that the system is over a configured threshold. See [Viewing and Editing Alarms, on page 4](#) for more information.
 - Alarm icon—Select the Alarm icon to view and edit the alarm threshold settings. Alarm thresholds appear on the **Alarms** page in numerical form. By default, alarm thresholds appear as a percentage. See [Viewing and Editing Alarms, on page 4](#) for more information about configuring alarms.

You can configure alarms for the following:

- Meetings In Progress—the current meetings that are experiencing issues.
- Usage—the total number of distinct users using the system. Occasionally participants are in multiple sessions, but participants are only counted once.
- Storage—the amount of space used for storing avatar images, meeting recordings, and database backups. The storage alarm appears only if you have configured a storage server. See [Adding an NFS or SSH Storage Server](#) for more information. The system disables meeting recording if the storage usage is over the configured threshold.

- Log Partition—the amount of space used to store the Application Audit Log. If an Auditor is configured for your system, this alarm is only visible to the Auditor.
 - License Usage—the percentage of permanent licenses assigned to host users.
 - Grace Licenses—the number of grace host licenses that are assigned to users.
- Data Center—lists the name of each data center, whether Maintenance Mode is on or off, the amount of storage used for each data center, and the status of data replication. See [About the Data Center Information Displayed on the Dashboard, on page 3](#) for more details.
 - Meeting Trend—graph of the number of meetings held on the system during a specified time. Use the **From** and **To** fields to set the time for the meeting trend information and for the meetings displayed in the Meetings list. You can select a point on the **Meeting Trend** graph to list the meetings that occurred during the time specified on the graph. To view meetings that occurred during a specific time of day, mouse over the graph and select the desired time.
 - Meeting Search—finds a meeting by entering specific search criteria, such as the meeting number, meeting topic, or a date range.
 - Meetings—the total number of meetings that occurred during the selected time, the meeting topics, hosts, numbers of participants, and the state of the meeting. If a data point is not selected from the **Meeting Trend** graph, all meetings for the time period appear. You can sort each column of information in the **Meetings** list, and the meetings appear in order by state: **In progress**, **Ended**, and **Not started**.

Select a **Meeting Topic** from the list to display details about the meeting. Details include: the meeting number, start time, end time, general status, and whether the meeting has been analyzed in detail. Before the analysis, the **Status** parameter shows the overall status of the meeting as it relates to quality. Select **Analyze Meeting Detail** to perform a detailed analysis of the meeting and generate a log. After the log is compiled, the general **Status** of the meeting changes, based on the details gathered during the analysis. The system generates and displays the date and time log, and then sends you an email with the log file download information. You can also download the log from the dashboard by selecting **Download Log**.



Note If the meeting host doesn't attend the meeting, the system terminates the meeting 30 minutes after the last participant exits the meeting. The meeting ends regardless of the scheduled end time. The meeting shows as being in progress until this time expires.

- Maintenance—schedules an announcement indicating when Maintenance Mode will be turned on or off. See [Scheduling a Maintenance Window, on page 14](#) and [About Maintenance Mode, on page 16](#) for more information.
- Last System Backup—appears if you have configured a storage server. It notifies you if the backup failed and the date of the first backup attempt if one has not yet been created. A link to the backup is provided for each data center. The window shows:
 - Time and date that the last backup was created.
 - Filename.
 - File size.
 - Location of the backup.

- Date and time of the next backup.
- Link to configure the system backup.
- Users—displays the number of active users, whether Directory Integration is configured, the time of the next synchronization (if configured), and the selected type of authentication. Select **View More** to go to [Editing Users](#).
- Settings—Shows the maximum number of participants allowed in each meeting, audio type, and whether Webex HQ video is enabled. Select **View More** to go to [Configuring Settings](#).

About the Data Center Information Displayed on the Dashboard

The System Monitor section of the dashboard displays status information for the data centers that comprise your system. If you have a single data center system, the data center name automatically assigned by the system is **CWMS System**, but the status information is dynamically updated for the single data center. In a multi-data center system, each data center is listed in a separate row by the name you entered during the join data center process and the status information is dynamically updated separately and displayed for each data center.

- Status—This column displays the status of each data center. Status can be Good, Partial Service, Blocked, or Down.
 - Good—All components of the data center are working properly. No system-generated email messages sent to the administrator.
 - Partial Service—Some of the components of the data center are not working properly, but the data center is providing service. The system sends an email to the administrator indicating that this data center needs attention.
 - Blocked—The system has blocked service on this data center and is redirecting all activity to another data center. The system sends an email to the administrator to indicate that service is down, data is being redirected to another data center, and this data center needs attention.
 - Down—The operation of a data center has degraded to the point where it can no longer provide reliable service and failover to an operational data center is in progress. The system sends an email to the administrator to indicate that service is down, data is being redirected to another data center, and this data center needs attention.
- In a Multi-data Center (MDC) environment, some components are capable of cascading, so the disabled service on this data center might be provided by another data center. This is not an indication of overall system status; it applies only to the status of this data center.
- Blocked or Down and Maintenance Mode is on—The data center status continues to show that the data center is blocked. When Maintenance Mode is turned off AND all components are again up and running, the status changes.
 - Unreachable—Another data centers cannot communicate with this data center. The system sends an email to the administrator asking them to check the network connectivity between the data centers.
 - Maintenance—Indicates whether a data center has Maintenance Mode turned On or Off.
 - Storage—The amount of storage used on the storage server connected to each data center. **Not Configured** displays If a storage server is not connected to the system.

- Data Replication—Indicates whether data replication is occurring between the data centers in an MDC system.

When a data center is in the Blocked or Down state, users might experience the following:

- In-progress meetings are automatically moved to an operational data center after a few minutes; similar to what happens in a failover situation. There is no impact on PCN or Blast Dial meetings.
- Previously scheduled meetings that have not started move to the operational data center. No other actions are required for the host or participants.
- Users sign in to a Webex site URL in the usual manner, but the system redirects the sign-in to the operational data center.
- Administrators can sign in to the blocked data center as well as the operational data center.
- Administrators receive a system-generated email which explains which data center is in the blocked state, and information explaining some of the possible causes.

Monitoring CPU, Memory, and Network Usage

To monitor CPU, memory, and network usage, we recommended that you use the performance tab of each CWMS virtual machine in vSphere client or vSphere Web client. The advantage to monitoring performance of CWMS virtual machines by using vSphere client or vSphere Web client is that each virtual machine can be monitored separately and for a specified period of time. If an issue that affects the system negatively exists, it is easier to precisely troubleshoot.

To monitor CPU usage refer to

<http://pubs.vmware.com/vsphere-51/index.jsp?topic=/2Fcom.vmware.vsphere.monitoring.doc/2FGUID-FC93B6FD-DCA7-4513-A45E-660ECAC54817.html>

Variations and spikes in CPU usage is expected; however, during general system use all levels should be less than 90 percent.

To monitor Memory usage refer to

<http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.monitoring.doc/GUID-C442423F-18CD-4F01-914E-286ED6C72BC6.html>

During normal operation Memory usage should be stable. Some variations are expected, but an increasing trend over a long period of time might indicate a pending issue that will soon affect system performance.

To monitor Network usage refer to

<http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.monitoring.doc/GUID-41B7E742-B387-4638-A150-CB58E2ADD89F.html>

Network usage can vary widely in reference to a CWMS virtual machine, and spikes in network usage (for example during a backup) are expected.

Viewing and Editing Alarms

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select the alarm **icon**.

The **Alarms** page appears.

Step 3 To modify, activate, or deactivate alarm thresholds, select **Edit**.

The **Edit Alarms** page appears. Select **Percentage %** to view the alarm threshold as a percentage or **Number #** to view the alarm threshold as a number. The default setting is **Percentage %**.

Step 4 Select the check boxes for the alarms that you want enabled and select the interval for each enabled alarm.

Option	Description
Meetings In Progress	<p>Meetings in progress alarm threshold.</p> <ul style="list-style-type: none"> • If set to Percentage %, move the selector bar to set from 2 to 99 percent. • If set to Number #, enter a number from 2 to 99 percent. <p>Default: Selected with an interval of one hour.</p>
Usage	<p>System usage alarm threshold.</p> <ul style="list-style-type: none"> • If set to Percentage %, move the selector bar to set from 2 to 99 percent. • If set to Number #, enter the number of users. <p>Default: Selected with an interval of 12 hours.</p>
Storage	<p>Storage threshold in GB. The maximum storage threshold is calculated as (the total space–recording buffer size). The size of the recording buffer depends on the size of your system [50-user (1 GB), 250-user (5 GB), 800-user (16 GB), or 2000-user (40 GB)], the number of Cisco Webex meetings held, and the length of the recorded meetings. Larger user systems (800– and 2000–user systems) require more storage to accommodate larger database backups. In general, plan to provide enough storage space for three backup files.</p> <ul style="list-style-type: none"> • If set to Percentage %, move the selector bar to set from 2 to 99 percent. • If set to Number #, enter the number of gigabytes. <p>Default: Not selected. Interval is one hour.</p> <p>Note This section appears only if you have configured a storage server. If the storage usage exceeds this threshold, the system disables meeting recording and the uploading of new avatar images. See Adding an NFS or SSH Storage Server for more information.</p>
Log Memory Usage	<p>Amount of disk space used for logs.</p> <p>If a user is configured as an Auditor during system deployment, this alarm is visible and configurable only by the Auditor on the Auditing tab. If your system does not have an Auditor role, an Administrator, SSO Administrator, or LDAP Administrator can see and configure this alarm.</p> <ul style="list-style-type: none"> • If set to Percentage %, move the selector bar to set from 2 to 99 percent. • If set to Number #, enter the number of gigabytes. <p>Set the Interval to indicate how often the system checks log memory usage.</p>

Option	Description
License Usage	<p>Permanent license use.</p> <ul style="list-style-type: none"> • If set to Percentage %, move the selector bar to set from 2 to 99 percent. • If set to Number #, enter the number of gigabytes. <p>Set the Interval to indicate how often the system checks the number of assigned licenses.</p>
Grace Licenses	<p>Grace license use.</p> <p>Select Notification was sent to the Grace license holder to send notifications to users when one of the selected conditions is met:</p> <ul style="list-style-type: none"> • A user is assigned a Grace license. • A Grace license assigned to a user is expired. • All Grace licenses are assigned.

An email is sent to administrators when an alarm exceeds a threshold. The interval is used to suppress multiple alarms within the specified time to avoid sending too many emails about the same issue.

Step 5 Select **Save**.

Your alarm settings are saved and the **Alarms** page is updated with your changes.

Viewing Meeting Trends

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Above the **Meeting Trend** graph set a trend period by selecting the **From** and **To** date and time.

- You can view meeting trend data from the four previous months, the current month, and one month in the future.
- Meetings scheduled before midnight and extending to the following day are displayed on the graph by the meeting start date.
- If a meeting is disconnected due to a system problem and then reconnected, it is counted twice on the Meeting Trends graph.
- Meeting trend data for one-month and six-month views is based on Greenwich Mean Time (GMT) and is therefore not accurately displayed over a 24-hour period. For example, if your system hosts 200

meetings during a given day, the database records the occurrence of those meetings based on GMT and not local time. Meeting trend data for one-day and one-week views are based on the user's time zone.

- A green track indicates meetings that are in progress or that have ended. Future meetings are shown in yellow.
- If the selected time range is 24 hours, the data points for passed or in-progress meetings are in five-minute intervals and future meetings are in one-hour intervals.
- If the selected time range is longer than one day but shorter than or equal to one week, the data points for passed, in progress, or future meetings are in shown in one-hour intervals.
- If the selected time range is longer than one week, the data points for passed, in progress, or future meetings are shown in one-day intervals.

The **Meeting Trend** graph shows the total number of meetings that occurred during the selected time period. The **Meetings** list below the graph lists all the meetings during the selected trend period.

Note Some meeting trend entries might appear to be duplicated, because they have the same name. An entry is created every time a meeting is started. Therefore, if a meeting is started, stopped, and restarted, multiple entries with the same meeting name are shown.

Step 3 To view a list of meetings that occurred at a particular time:

- a) Click a particular location on the **Meeting Trend** graph to list the meetings that occurred within 5 minutes of the selected time in the **Meetings** list below the graph. See [Viewing the Meetings List, on page 7](#) for more information.
- b) Select the graph symbol below the **From** and **To** fields to display a list of date and times when meetings occurred between the From and To period. Then select a date from the drop-down list.

The data points shown in the drop-down menu are the same as those shown on the graph. They are made accessible primarily for the benefit of users with a keyboard and screen reader.

Mouse over the graph to see the total number of meetings that occurred at that time.

What to do next

- See [Viewing the Meetings List, on page 7](#) to view more information about a meeting.
- See [Finding a Meeting, on page 9](#) for more information about using the **Meeting Search** tab.

Viewing the Meetings List

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Above the Meeting Trend graph set a trend period by selecting the **From** and **To** date and time.

By default, the Meetings list displays the meetings for the current 24-hour period. See [Viewing Meeting Trends, on page 6](#) for more information.

By default the Meetings list displays meetings in the order of their scheduled start time. Meetings are displayed in order of status: In Progress, Ended, Not Started. Information displayed in the Meetings list includes:

- Time range selected in the trend chart
- Meeting Topic
- Host 's name
- Number of participants
- State of the meeting: In Progress, Ended, Not Started

Note A status icon displays in the first column to indicate the state of the meetings that are in-progress or have ended as *good (green)*, *fair (yellow)*, or *poor (red)*.

- Fair (yellow) indicates the audio/video delay or jitter taking place during the meeting has reached a minor threshold and should be monitored and investigated to determine the cause.
- Poor (red) indicates the audio/video delay or jitter taking place during a meeting has reached a major threshold.
- If the majority of the meetings displayed in the Meetings list indicate a status of poor, then contact the Cisco Technical Assistance group (TAC) for assistance.
- The following table provides more details for the different meeting status indicators.

Category	Good	Fair	Poor
Data Round Trip Time	Less than 3000 ms.	3000–5999 ms.	6000 ms. and higher
Audio Round Trip Time	Less than 100 ms.	100–299 ms.	300 ms. and higher
Audio Packet Loss	Less than 5 percent	5–9 percent	10 percent and higher
Audio Jitter	Less than 100 ms.	100–499 ms.	500 ms. and higher
Video Round Trip Time	Less than 100 ms.	100–499 ms.	500 ms. and higher
Video Packet Loss	Less than 20 percent	20–49 percent	50 percent and higher
Video Jitter	Less than 100 ms.	100–499 ms.	500 ms. and higher

Step 3 (Optional) Select a column heading to sort the meetings.

Step 4 Use the pagination function to view the next or previous page.

- A maximum of 10 meetings display on each page.

- You might see duplicate meeting entries in the Meetings list. A meeting entry is created every time a meeting is started. Therefore, if a meeting is started, stopped, and restarted, multiple meeting entries with the same name are displayed in the list.

Step 5 Select a **meeting topic** in the Meetings list to display more meeting information.

The list expands to show meeting details, such as the names of the participants, the start and end time, and the meeting status.

- Select **time stamp** to go to the **Meeting Analysis Report** page.
- Select **Download Log** to download the System Information Capture (Infocap) Log to your local drive.

Step 6 (Optional) To refine your search, select the **Meeting Search** tab. Additional search fields appear.

What to do next

- See [Viewing a Meeting Analysis Report, on page 10](#) for more detailed meeting information.
- See [Downloading Cisco Webex Meeting Logs, on page 12](#) to download a compressed file with several meeting logs. Use these logs to troubleshoot issues that participants experienced during a meeting.
- See [Finding a Meeting, on page 9](#) to refine your search results or find a specific meetings.

Finding a Meeting

Procedure

Step 1 Sign in to Webex Site Administration.

Step 2 In the **Meeting Trend** section, select the **Meeting Search** tab.

Step 3 Enter your search criteria.

Search for meetings by using some or all of the following fields:

- Meeting Number or Host Name
- Status—Select All, Good, Fair, or Poor from the drop-down menu.
- Meeting Topic—You can enter the first few letters of the meeting topic to find all meetings with similar topics.
- From Date and Time—Use the calendar icon and drop-down menu to select the date and time.
- To Date and Time—Use the calendar icon and drop-down menu to select the date and time.

Step 4 Select **Search**.

The **Search Results** lists the meetings that match the search criteria and the **Export** button appears.

Step 5 To export your search results to a .CSV file, select **Export**.

Step 6 To start another search, select **Clear**.

Step 7

The system clears the search fields, but the results from the previous search remain in the **Search Results**. Select a **meeting topic** in the Meetings list to display more meeting information.

The list expands to show meeting details, such as the names of the participants, the start and end time, and the meeting status.

- Select **time stamp** to go to the **Meeting Analysis Report** page.
- Select **Download Log** to download the System Information Capture (Infocap) Log to your local drive.

What to do next

To view additional meeting information, see [Viewing a Meeting Analysis Report, on page 10](#).

To download a zipped file with meeting logs, see [Downloading Cisco Webex Meeting Logs, on page 12](#).

Viewing a Meeting Analysis Report

Additional information about a Cisco Webex meeting and its participants is available on the **Meetings Analysis Report** page.

Before you begin

One or more meetings are displayed in the Meetings list on the **Meeting Trend** tab. See [Viewing the Meetings List, on page 7](#) for details.

Procedure**Step 1**

Select a **meeting topic** displayed in the Meetings list on the Meeting Trend tab.

Step 2

In the Meetings list, select **Analyze Meeting Detail**.

While the system is processing the information, the date and time the system started generating the information is displayed with a status of Pending. When the system is finished generating the information, the date and time become an active link and the Pending status changes to a Download log active link.

Step 3

Select the **date and time** link to view the **Meeting Analysis Report** page.

The following information displays:

- Meeting Topic
- Host's email address
- Status—Current status of the meeting. Values: Not Started, In-Progress, Ended.
- Start Time—Date and time the meeting started.
- End Time—Date and time the meeting ended.
- Online Meeting ID—The meeting ID assigned to the online portion of the meeting.
- Join Before Host—Indicates whether participants are allowed to join the meeting before the meeting host.

- **Data Center**—Shows the name of the data center used for the meeting. In a single data center environment, the name is always CWMS System.
- **Meeting Number**—A 9-digit number assigned to the meeting.
- **Health**—The general health of the meeting. Values can be Normal, Fair, or Poor.
- **Scheduled Start Time**—The date and time the meeting was scheduled to begin.
- **Scheduled End Time**—The date and time the meeting was scheduled to end.
- **Audio Meeting ID**—The meeting ID assigned to the audio portion of the meeting.
- **Audio Meeting Started First**—Indicates whether the audio portion of the meeting was started before the online portion of the meeting.

Note When the system refreshes the window, the meeting details are closed. Select the meeting topic again to display the date and time or Download log links.

Step 4 Select the **Meeting Messages** tab to display the Function, Time, and Messages generated during a meeting.

Step 5 Select the **Participants** tab to display the following information for each meeting participant:

- Participant's name
- Join Time
- Browser
- Client IP address—IP address of the Webex site.
- Leave Time—Time the participant left the meeting.
- Leave Reason—Reason for leaving a meeting. Values are Normal or Timeout.
- Phone Number—Number of the phone that participants use to attend the meeting.
- VoIP Latency
- Audio QoS—Quality of the audio during the meeting. Values are Normal or Bad.
- Video QoS—Quality of the video during the meeting. Values can be Normal or Bad.
- Client Latency—Latency from the meeting client to the Data Meeting server. Values can be Normal or Bad.
- Hosting Server—Name of the virtual machine that hosted the meeting. It is part of the fully-qualified domain name (FQDN) of the virtual machine that hosted the meeting. For example, if a micro VM FQDN is `susmicro-vm.orionqa.com`, `susmicro-vm` appears in the report.

What to do next

See [Downloading Cisco Webex Meeting Logs, on page 12](#) to download a compressed file with several meeting logs.

Downloading Cisco Webex Meeting Logs

While a Cisco Webex meeting is in-progress or when a meeting has ended, you can download system-generated meeting logs that provide information for troubleshooting an issue users experienced during a meeting.

Procedure

- Step 1** Sign in to the Administration site.
 - Step 2** Select the Meeting Trend tab, then select a **From** and **To** range to display a graph of meetings that occurred during the selected time frame.
 - Step 3** Click a particular location on the **Meeting Trend** graph to list the meetings that occurred within 5 minutes of the selected time in the **Meetings** list below the graph.
 - Step 4** Select a **meeting topic** in the **Meetings** list.
Information about the selected meeting display below the meeting topic.
 - Step 5** Select **Download logs**.
-

What to do next

See [About Meeting Logs, on page 12](#) for more information about the downloaded meeting logs.

About Meeting Logs

Your downloaded Meeting Logs compressed file contains the following logs:

Data Conference Log

This log contains information about the online portion of a meeting.

- Conference ID
- Meeting ID
- Scheduled Start Time
- Start Time
- End Time
- Host Email Address
- Site URL
- Meeting Type—Meeting client
- Meeting Name—The meeting topic.
- Primary Call-in Number
- Secondary Call-in Number
- Delete Meeting When Ended—Indicates whether this meeting is deleted from the Meetings details page when the meeting ends.

- Meeting Status
- Application Sharing—indicates whether the application sharing feature was used during a meeting.
- Regular Telephony—Indicates whether participants called the meeting using telephones.
- Hybrid Telephony
- Eureka Video
- Eureka VoIP
- MMP VoIP
- Hybrid VoIP
- MMP Video
- NBR2
- Mobile
- Audio Broadcast
- Audio Broadcast for Mobile

Multimedia Log

This log provides information about audio streaming, audio switching, and SVC stream adaptation to the meeting client as it relates to MMP.

- Meeting Name
- Conference ID
- Session Type
- Participants
- Total Join
- MCS Server
- Start Time
- End Time
- Duration

Teleconference Log

This log contains information about a teleconference meeting.

- TeleConf ID
- App Server
- Callers
- Callback

- Call-in
- Start Time
- End Time
- Duration
- Description
- Account Type

Web Join Event Log

This log contains information about the web join events.

- Meeting Name—Displays the meeting topic.
- Conference ID—Data conference instance ID.
- Site ID—The name of the Cisco Webex site.
- Participants—Total number of participants that joined the meeting from a Web browser.



Note The host that starts the meeting is not included in this total.

- Total Join—The total number of people who joined the meeting.
- Start Time—Starting date and time of the meeting.
- End Time—Ending date and time of the meeting.
- Duration—Amount of time, in minutes, the meeting lasted.
- End Reason—Reason the meeting ended.

Scheduling a Maintenance Window

When you turn on Maintenance Mode, all in-progress meetings end and the Meet Now function becomes unavailable. Before you perform system maintenance for a Single Data Center system, schedule a maintenance window and notify users in advance. Inform users that during a maintenance window, meetings currently in progress are terminated and that they cannot schedule meetings that overlap the maintenance window. If you are running a Multi-data Center system and only one system is put into Maintenance Mode, meetings transparently failover to the active system and there is no need to notify users.

For example, an administrator wants to bring a Single Data Center system down for one hour for maintenance. The administrator can try to schedule a time when no meetings appear to be scheduled. If meetings are scheduled, the administrator should notify the meeting hosts about the maintenance window. Hosts can then reschedule their meetings for another time, outside of the maintenance window. If a host tries to hold a scheduled meeting anyway, it will be terminated.

If the planned tasks require an extended period of time to complete, such as uploading a new Certificate Authority (CA) certificate, schedule a longer maintenance window. For example, when you schedule your

maintenance window, specify a start time of 30 minutes before you plan to turn on Maintenance Mode. This allows a grace period for all meetings to end gracefully. Also we recommend that you add an hour to any maintenance window. The extra time allows the system to become functional after the reboot that might occur. You might also want to start one or more instant meetings to test the modified settings, before the users attempt to schedule or host meetings.

While some system maintenance tasks do not require that you turn on Maintenance Mode, the tasks that do require extra time to complete a restart or a reboot, after you turn off Maintenance Mode. A system restart takes only a few minutes (approximately 3-5 minutes), but a reboot takes approximately 30 minutes. See [Turning Maintenance Mode On or Off, on page 18](#) for more details.

Procedure

- Step 1** Sign in to Webex Site Administration.
- In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.
- Step 2** Select **Schedule Maintenance**.
The **Schedule Maintenance Window** displays.
- Step 3** Use the calendar tool and the time drop-down menu to select the date and start time for the maintenance window.
- Step 4** Enter the duration of the maintenance window by specifying the number of hours and minutes.
- Step 5** Select **Schedule**.

When the maintenance window begins, users receive an error message if they attempt to schedule a meeting that falls within the scheduled maintenance window. Scheduling a maintenance window does not automatically put the system into Maintenance Mode; that must be done by an administrator.

The scheduled maintenance window date, start time, and duration displays in the Maintenance pane.

What to do next

See [Emailing Users](#) for details about notifying users of system maintenance events.

Changing a Scheduled Maintenance Window

After you schedule a maintenance window, you can reschedule the date and time or delete it.

Procedure

- Step 1** Sign in to Webex Site Administration.
- In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.
- Step 2** Select **Dashboard**.
- Step 3** Select the displayed system maintenance date and time.

Step 4 On the **Schedule Maintenance Window**, you can:

- Enter a different start date and time.
- Modify the duration hour and minutes.
- Select **Delete** to remove the maintenance window.

If you finish your system maintenance early, you can either reduce the duration time or select **Delete** on the **Schedule Maintenance Window**.

What to do next

Turn on Maintenance Mode before you modify system properties. See [About Maintenance Mode, on page 16](#) for information about which system properties require Maintenance Mode to be turned on.

About Maintenance Mode

Many configuration changes require that you put your system into Maintenance Mode. Maintenance Mode shuts down all conference functionality on a data center, so you should alert users by scheduling the maintenance windows (see [Scheduling a Maintenance Window, on page 14](#)).

For more information, see [Turning Maintenance Mode On or Off, on page 18](#).

Putting a data center in Maintenance Mode does the following:

- Disconnects users and closes all meetings. If you put a data center that is part of a Multi-data Center (MDC) system into Maintenance Mode, meetings in progress fail over to the active data center.
- Prevents users from signing in from web pages, the Outlook plug-in, and mobile applications. Emails are automatically sent when the system is taken out of Maintenance Mode.
- Stops access to meeting recordings.
- Prevents users from scheduling or hosting meetings.

The system continues to send automatic notification emails to users and administrators.

Use the following table to help determine which tasks require you to turn on Maintenance Mode and the action your system performs after you turn off Maintenance Mode, so you can plan the downtime. When Maintenance Mode is required, the system provides reminder messages if you attempt to perform a task without turning on Maintenance Mode.

Task	Reference	Maintenance Mode Required	Reboot or Restart
Adding or removing High Availability	Adding a High Availability System	Y	Reboot
Adding or removing public access	Adding Public Access to Your System by using IRP or Removing Public Access	Y	Restart
Change the system default language	Configuring Company Information	Y	Restart

Task	Reference	Maintenance Mode Required	Reboot or Restart
Changing your host or admin account URLs	Changing Your Webex Site Settings	Y	Restart
Changing your mail server	Configuring an Email (SMTP) Server	N	N/A
Changing your virtual IP address	Changing the Private and Public Virtual IP Addresses	Y	Reboot
Configuring and changing branding settings	Configuring the Branding Settings	N	N/A
Configuring and changing many of the audio settings	Configuring Your Audio Settings	Y	Restart
Configuring and changing the Call-In Access Numbers, Display Name, and Caller ID audio settings.	Modifying Audio Settings	N	N/A
Configuring and changing quality of service settings	Configuring Quality of Service (QoS)	N	N/A
Configuring and changing SNMP settings	Configuring Your SNMP Settings	Y	Restart
Configuring certificates	Managing Certificates	Y	Restart or Reboot
Configuring disaster recovery settings	Disaster Recovery by Using the Storage Server	Y	Restart
Configuring FIPS-compatible encryption	Enabling FIPS Compliant Encryption	Y	Restart
Configuring storage servers	Adding an NFS or SSH Storage Server	Y	Restart
Configuring virtual machine security	Configuring Virtual Machine Security	Y	Reboot
Expanding system size	Preparing for System Expansion	Y	Restart
Performing updates or upgrades	Upgrading Your System	Y	Restart
Updating shared keys	Managing Certificates	Y	Restart
Using the System Resource test	Using the System Resource Test	Y	Restart

Each of your virtual machines has a console window that indicates when it is in Maintenance Mode. You can open the console windows in the vCenter inventory bar (for navigation). The console windows provide the URL of the system, type of system (primary, high availability, or public access), type of deployment (50 user, 250 user, 800 user, or 2000 user system), and the current system status including the time and date of the status change. The time displayed is configured in your **Company Info** settings. See [Configuring Company Information](#) for more information.

Completing System Maintenance Tasks

After you finish modifying your system configuration you can turn off Maintenance Mode. The system monitors the modifications and automatically makes the determination as to whether a restart or a reboot is required. The system displays a message to indicate the requirement:

- The changes that you made require a system restart that takes only a few minutes.
- The changes that you made require a system reboot that takes approximately 30 minutes, depending on the size of your system. During this time, conference functionality is unavailable.

When Maintenance Mode is off, the **Dashboard** page refreshes. Your system is ready for users to successfully start meetings when all of the virtual machines, listed on the **System Properties** page, display a status of Good (green). See [Turning Maintenance Mode On or Off, on page 18](#) for more information.

If Maintenance Mode is off but the scheduled maintenance window is still in effect, users will be able to host and attend previously scheduled meetings, but will not be able to schedule new meetings until after the maintenance window ends.

Related Topics

[Scheduling a Maintenance Window, on page 14](#)

[Turning Maintenance Mode On or Off, on page 18](#)

Turning Maintenance Mode On or Off

Turning on Maintenance Mode for all active data centers shuts down conference functionality and prevents users from signing in to the Webex site, scheduling or joining meetings, and playing meeting recordings. Some actions do not require that all data centers in a Multi-data Center (MDC) environment be put into Maintenance Mode. If you put all of data centers are put into Maintenance Mode, meetings in progress will end. When you turn off Maintenance Mode, the system determines whether a restart (takes approximately 3 to 5 minutes), or a reboot (takes approximately 30 minutes), is required and displays the appropriate message. See [About Maintenance Mode, on page 16](#) for information about which system tasks require Maintenance Mode to be turned on.

Before you begin

Schedule a maintenance window and notify users about the scheduled system maintenance time. See [Scheduling a Maintenance Window, on page 14](#) for details.

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

- Step 2** From the **Dashboard**, select **Manage Maintenance Mode**. The **Manage Maintenance Mode** dialog displays.
- Step 3** Select the data center to put into Maintenance Mode, or deselect the data center to be taken out of Maintenance Mode.
- Step 4** Select **Save**.
- Step 5** (Optional) Back up your virtual machines.
- Step 6** (Optional) To determine if the system is fully operational, select **Dashboard > System > View More** (in the System section).
- Conferencing functions can resume when the **Status** for all of the listed virtual machines is **Good** (green).
-

Using the HostID and ConfID to Locate a Meeting Recording

You can use the HostID and the ConfID values for a meeting to locate the path to the recording for that meeting.

Before you begin

Familiarize yourself with the Network File System (NFS) directory structure.

Procedure

- Step 1** Obtain the full name of the meeting host, the date and time of the meeting, and the meeting number.
- Step 2** In CWMS Site Administration, go to **Users > Import/Export Users** and click **Export**. The system sends you an email with the **users.csv** file attached.
- Step 3** In CWMS Site Administration, go to **Reports > Customize your report**, and then select a time period that includes the date and time when the meeting took place. The system sends you an email with the **CustomReport.zip** file attached.
- Step 4** Extract **MeetingInformation.csv** from the **CustomReport.zip** file.
- Step 5** Open the **users.csv** file and use the name of the host to find the **User ID** for the host (first column of the file). The **User ID** is the same as the **HostID** used in the directory structure.
- Step 6** Open the **MeetingInformation.csv** file, and sort the data by date.
- Step 7** Search for the **Meeting Number** and ensure that the details you gathered in Step 1 match.
- Step 8** Find the **Meeting ID** value. The **Meeting ID** is the same as the **ConfID** used in the directory structure.
- Step 9** Use the information that you gathered to construct the path for the recording:
NFSstorageIPaddressorFQDNpath/1/HostID%1000/HostID/ConfID%1000/ConfID.
- Example:** Where UserID=2711 and MeetingID=49782
HostID%1000 of 2711 = 711
HostID = 2711

ConfID%1000 of 49782 = 782

ConfID = 49782

Full path = NFSstorageIPaddressorFQDNpath/1/711/2711/782/49782

Related Topics

[Network File System Storage](#), on page 20

Network File System Storage

The Network File System (NFS) storage structure is organized into five directories (folders):

1—This directory contains all consolidated recordings and the following sub-directory structure:

- **HostID%1000**—If the host ID is larger than three digits, this sub-directory name is based on last three digits of the host ID.
- **HostID**—This sub-directory name matches the full host ID and is unique to each user.
- **ConfID%1000**—If the conference ID is larger than three digits, this sub-directory name is based on last three digits of the conference ID.
- **ConfID**—This sub-directory name matches the full conference ID and is unique to each conference. This sub-directory includes the following sub-directories:
 - **RecordingData**—This directory contains all of the consolidated recording files required for streaming the recording. Files present are `wbxcbr.dat`, `wbxcbr.idx`, `wbxcbr.conf`, `Wbxcbr_tel.wav`, `wbxmcsr.dat`, `wbxmcsr.idx`, and `public.wbxcbr`.
 - **RecordingPac**—The system creates this directory only after a host downloads the recording file from the Webex Site. This directory contains an ARF recording file that people can play locally on their PC by using NBR Player.

Table 1: Determining the HostID%1000 or the ConfID%1000 Sub-directory Names

Condition	First Sub-directory Name
The host ID or full conference ID is 6534. ¹	534
The host ID or full conference ID is 23045. ²	45
The host ID or full conference ID is 35000. ³	0
The host ID or full conference ID is 42. ⁴	42

¹ The host ID or full conference ID contains more than three digits, the sub-directory name is based on the last three digits of the ID.

² If the last three digits of the host ID or full conference ID contain leading zeros, the system strips them from the sub-directory name.

³ If the last three digits of the host ID or full conference ID are all zeros, the sub-directory name is 0.

⁴ If the host ID or full conference ID contains fewer than three digits, the sub-directory name matches it.

Calendar year named directory —For the year 2017 the directory name is 2017. The system creates a new folder for each year. If you have had the CWMS solution for a few years, you can see other directories such as 2016, 2015, and 2014 directories. The system uses this directory to temporarily store meeting recording files during meetings. After a meeting ends, the system consolidates the associated files from this directory and moves them into the directory named 1. This directory contains the following sub-directory structure:

- **Month (by number) named directory**—The system creates a directory for every month of that year (1 to 12).
- **Conf ID directory**—This directory contains the following sub-directories:
 - **Action**—This directory contains the .dct recording files for the associated meeting (Conf ID).
 - **Data**—This directory contains the .dat and .idx recording files for the associated meeting (Conf ID).

Avatars—The system stores all images for avatars inside this folder.

nfskeepalive—This folder contains files that contain information about the regular checks of component access to NFS storage. There are two types of files in this directory and both are for system use only:

- **Files with number names**—These files are empty.
- **Files with .nkl extension**—Files with names beginning with wbxcb or wbxmcs and having .nkl extensions contain 0.

Snapshot_folder—These directories store the daily backups of the system. The system can create more than one Snapshot_folder. The system takes a backup before running a MINOR update, and these backup files are not automatically deleted from the NFS storage. For every MINOR update run on the system, the system creates a Snapshot_folder with backups taken just before the update was run.

Related Topics

[Using the HostID and ConfID to Locate a Meeting Recording](#), on page 19

