Configuring Your Mail Server, Time Zone, and Locale

Configuring an Email (SMTP) Server

Configure an Email server to enable your system to send meeting invitations and other communications to users.

It is important that the Email server is always operational. Email is the primary method of communication with your users including recording notifications, meeting information changes, account status, and many other important announcements. (See also Adding Users.)

Important Users are identified to the system by Email address. If a user Email address is changed and the user remains active, the Email address on CWMS must also be changed or that user will not receive notifications.

Note Turning on Maintenance Mode is not required to change these properties.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Select **System** and select **View More** in the Servers section.

Step 3 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.

Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

Turning on Maintenance Mode on all active data centers shuts down conferencing activity and prevents users from signing in to the WebEx site, scheduling meetings, joining meetings, or playing meeting recordings. If this data center is part of a Multi-data Center (MDC) system and another data center is active, in-progress meetings will fail over to the active data center. This might cause a brief interruption in active meetings. See About Maintenance Mode for information about which system tasks require Maintenance Mode to be turned on.

Step 4 In the **SMTP Server** section, select **Edit**.

Step 5 Enter the fully qualified domain name (FQDN) of a mail server that the system will use to send emails.

Step 6 (Optional) Select **TLS enabled** to enable Transport Layer Security (TLS). (Basic authentication is enabled by default.)

Step 7 (Optional) Edit the **Port** field to change the default value.
The SMTP default port numbers are 25 or 465 (secure SMTP port).

Note The Web node and Admin node send SMTP requests to the configured Email server. If there is a firewall between the internal Web and Admin virtual machines and the Email server, the SMTP traffic might be blocked. To ensure Email server configuration and Email notification work properly, port 25 or 465 (secure SMTP port number) must be open between the Email server and the Web and the Admin virtual machines.

Step 8 (Optional) Enable mail server authentication, select **Server authentication enabled**. If you enable authentication, enter the **Username** and **Password** credentials necessary for the system to access the corporate mail server.
Emails from the system are sent by `admin@<WebEx-site-URL>`. Ensure that the mail server can recognize this user.

For micro, small, or medium systems, email notifications come from the administration virtual machines (either the primary or high-availability system).

For large systems, email notifications come from the web virtual machines (either on the primary or high-availability system). In a large system, there are three web virtual machines on the primary system and one web virtual machine on the high-availability system.

Step 9 Select **Save**.

What to Do Next

See Activating or Deactivating Users and Administrators from the Users Page, Adding Users, and Editing Users.

Setting the Time Zone, Language, and Locale

Before You Begin

If you are running Windows 7 and have your Cisco WebEx site open in an Internet Explorer 10 browser, you may want to select the document Internet Explorer 10 standards to make sure all the buttons in the application work properly.

- Select **Tools** > **Developer Tools**.

- At the top of the Developer Tools window, select **Document Mode: IE7 Standards** > **Internet Explorer 10 Standards**.

Step 1 From the Administration web site, navigate to **Settings** > **Company Info**

Step 2 Select the local **Time Zone** for this system from the drop-down list.

Step 3 Select the **Language**.

Step 4 Select the country **Locale**.

Step 5 Select **Save**.

Creating Administrator Accounts

The system creates a First Administrator account. This administrator must sign into the system, create a password, and add other administrators. Until then, no other administrator can have access to the system. As part of the process, the First Administrator can create an Auditor account, separating the administrator and auditor. This can be done as part of the deployment process or the First Administrator can create an Auditor (**Users** > **Edit Users**). (See Adding an Auditor Role, on page 3.)

Before You Begin

A mail server for the system to use to send emails to administrators must be configured. See Configuring an Email (SMTP) Server, on page 1 for instructions.

Step 1 Enter the first and last names of the administrator.

Step 2 Enter the complete administrator email address and confirm it by entering it again.

Step 3 (Optional) Select **Create an auditor account** to add an Auditor to the system.

Step 4 Select **Next** to create the initial password.

Step 5 Enter a password and confirm it by entering it again.

Step 6 Select **Submit** to sign in to the WebEx Administration site.

Step 7 Sign into the system and add administrators and users. Upon creation of each new account, the system sends an email to that person, welcoming them and asking that user to sign in and change the initial password.
Upon initial sign in, each administrator is offered a tutorial of the system. The administrators can view the tutorial immediately or view it on demand.

Adding an Auditor Role

The First Administrator has the Auditor role by default, and is the only one who can activate the Auditor role for another user. When doing so, the Auditor privileges are taken away from the First Administrator. If an Auditor is also a System Administrator, that person has a System Auditing role.

The Auditor role separates administrative actions from system monitoring as follows:

- Turn auditing on or off.
- Configure CWMS to synchronize with the remote syslog servers.
- Perform log purging.
- Configure alarms for the log partition.
- Generate log captures.

- If the Administrator and Auditor roles are not separated, only Administrator and Hosts roles exist; administrators have all the authority.
- If the Administrator and Auditor roles are separated when the system is deployed, a First Administrator role is created (described as the *emergency account*). After system deployment, only the First Administrator emergency account can create an Auditor, taking the Auditor privileges away from administrators. The First Administrator can create as many auditors as desired after the system has been deployed.
- The Auditor is local only; it cannot come from synchronization with any external user base.
- Auditor parameters (such as the name) can be modified, but once created the Auditor role cannot be deactivated or reassigned to another user ID.
- An Auditor cannot modify user parameters.
- An Auditor does not have Host privileges and cannot schedule meetings by using the Auditor account. An Auditor can attend meetings as a participant.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Select **Users**.

Step 3 Select a user.
The **Edit Users** window appears.

Step 4 Select the **Auditor** account type.

Step 5 Select **Save**.
Auditor is sent a welcome email.

About System Testing

Most of the system test are accomplished by using the CWMS system, for example by Using the Meetings Test and Using the System Resource Test.

When testing an upgraded system, you can keep the original system until you have finished testing the upgraded system (but because they share some parameters, such as IP addresses, you cannot power on both systems at the same time). Once you are satisfied with the results of the upgraded system tests, you can remove (forever)

the original system. Be sure your upgraded system is running when removing the original system. This prevents accidental removal of the base virtual machine disk (VMDK) file that must be accessed by the upgraded system.

Some of the recommended tests to run on the system are.

- Add, edit, activate, and deactivate users. (See Managing Users.)
- Schedule and hold a meeting.
- Reschedule an existing meeting.
- Delete a series of scheduled meetings.
- Add and open a meeting attachment from the meeting invitation.
- Record a meeting and play back the recording.

The system can also be tested by:

- Confirming that the Network is Configured Correctly
- Checking the System
- Confirming that the primary system will failover to the HA system by removing the physical connection to the primary system and verifying that Cisco WebEx is running on the HA system.