Managing Users

About Managing Users

You can add users individually by using the GUI or import user accounts stored in a comma-separated or tab-delimited (CSV) file. See Creating Comma- or Tab-Delimited Files, on page 3.

The system supports a lifetime maximum of 400,000 user accounts, the sum of both active and deactivated user accounts. (This lifetime maximum number of user accounts is large enough to accommodate the anticipated growth in the user database of any organization.)

You can add and deactivate user accounts, but you cannot delete them. A deactivated user can be reactivated as necessary. Reactivated user accounts regain access to the meetings, recordings, and other data that they had access to before they were deactivated.

User accounts are based on the email address of the user. If the email address of a user is changed outside the system, the user might not be able to use the system until the email address is reconciled.

To prevent unauthorized sign-in to the system, deactivate any users who leave your organization. You can deactivate users in the following ways:

- If your system does not use integrated SSO, you can deactivate users individually by using the GUI or by importing a CSV file with the ACTIVE field set to N for all the users you want to deactivate. See Activating or Deactivating Users or Administrators, on page 21 for more information.
- If your system uses integrated SSO you must deactivate users by removing them from the corporate directory in your SAML 2.0 IdP. This procedure cannot be performed through this product.
- Use the password configuration feature to deactivate users after a specified period of time. See General Password Settings for more information.

For Cisco WebEx Meetings Server Release 2.5, there are additional user roles: SSO Administrator, LDAP Administrator, and Auditor.

Auditor Role

Auditor Role

The Auditor role is added by using Adding Users, on page 17.

The Auditor role is a special role created for environments that need to audit sign-ins and configuration changes made by administrators. An auditor can configure log settings and generate Application Audit logs to meet company security and JITC-compliance requirements.

The First Administrator has Auditor privileges 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.
- An Auditor *does not have Host privileges* and cannot schedule meetings by using the Auditor account. An Auditor can attend meetings as a participant.
- If the Administrator and Auditor roles are not separated, only the Administrator role exists.
- 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. The First Administrator can create as many auditors as desired after the system has been deployed by using the Adding Users, on page 17 procedure..

- 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 can only see and configure settings on the Auditor tab.

The Auditor role is a unique role with the following aspects:

Note If an Auditor is not configured, all administrators have access to and can configure the Application Audit Log settings on the **Settings** > **Security** > **Application Audit Log** page and the Log Memory Usage alarm on the **Dashboard** > **Alarms** > **Edit Alarms** page. If an Auditor is configured, administrators can view these pages, but they cannot modify them.

Creating Comma- or Tab-Delimited Files

The system can import and export user account values contained in a comma- or tab-delimited (CSV) file. (A spreadsheet application, such as Microsoft Excel, can be used to manage CSV files.) If an account in an imported CSV file does not exist, the account is added. If the account exists, imported CSV account values replace the current values.

The system can export a CSV file containing user account values that can be modified and imported back into the system or a new system.

To successfully import a CSV file, the following criteria must be met:

- All fields listed in the table are required. We recommend that before importing a CSV file, that you export the current database to a CSV file to confirm the structure of the file. If a field is missing, an error message appears. For example,
  Incorrect file format. Custom10 is required.
- Field values can be empty, unless indicated otherwise.
- Valid characters in the CSV file are limited to those contained in UCS Transformation Format—8 bit (UTF-8).
- When adding a new user account, the **UserId** field can be blank if the **Email** field contains an email address that is not used by another user account. If the email address matches the email address in another user account, the user account in the CSV file is not added.
- When editing a user account, the **UserId** and **Email** values must match an existing user account. If they do not match a user account, none of the current values are changed to the CSV values.
- Up to ten **Tracking Code Groups** can be defined. Tracking code group names must be unique. Do not use predefined field names (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE, and so forth) for tracking codes.

Table 1: Field Names, Descriptions, and the Acceptable Values

Field Name	Description	Size and Type of Value
USERID	User ID. **Important** This field is generated by the system and must be left blank.	1 to 19 alphanumeric characters
ACTIVE	Indicate whether or not this user is active.	Y or N
FIRSTNAME	User's first name. This field cannot be empty.	1 to 32 character string
LASTNAME	User's last name. This field cannot be empty.	1 to 32 character string
EMAIL	User's email address.	1 to 192 alphanumeric character string
LANGUAGE	Language of the user. (See CSV File Field Values, on page 5.)	1 to 64 character string
HOSTPRIVILEGE	Host privileges.	ADMN or HOST If the import file does not specify a value, the system applies the default user account type. (**Settings** > **User Management** > **Default user account type**)
TIMEZONE	Time zone where the user is located. (See CSV File Field Values, on page 5.)	Time zone name
DIVISION	Tracking code group 1. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 21.)	1 to 128 character string
DEPARTMENT	Tracking code group 2. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 21.)	1 to 128 character string
PROJECT	Tracking code group 3. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 21.)	1 to 128 character string

Field Name	Description	Size and Type of Value
OTHER	Tracking code group 4. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 21.)	1 to 128 character string
CUSTOM5	Custom field 5. (See Configuring Tracking Codes, on page 21.)	1 to 128 character string
CUSTOM6	Custom field 6.	1 to 128 character string
CUSTOM7	Custom field 7.	1 to 128 character string
CUSTOM8	Custom field 8.	1 to 128 character string
CUSTOM9	Custom field 9.	1 to 128 character string
CUSTOM10	Custom field 10.	1 to 128 character string
COUNTRY	Country of user.	1 to 128 character string

The following topics provide additional information:

- Exporting All User Accounts to a CSV File, on page 16
- Importing User Accounts from a CSV File, on page 16
- Transferring User Accounts Between Systems by using a CSV File, on page 17
- Configuring Tracking Codes, on page 21

CSV File Field Values

Language Field Values

Following are examples of the LANGUAGE field values that you can use in a CSV file.

Field Value	Language
en-us	U.S. English
zh-cn	Simplified Chinese
zh-tw	Traditional Chinese
jp	Japanese
ko	Korean

Field Value	Language
fr	French
de	German
it	Italian
es-me	Castellon Spanish
es	Latin American Spanish
nl	Dutch
pt-br	Portuguese
ru	Russian

Time Zone Field Values

Following are the TIMEZONE field values that you can set in a CSV file.

Field Value	GMT
Marshall Islands	-12 hr
Samoa	-11 hr
Honolulu	-10 hr
Anchorage	-9 hr
San Francisco	-8 hr
Tijuana	-8 hr
Arizona	-7 hr
Denver	-7 hr
Chihuahua	-7 hr
Chicago	-6 hr
Mexico City	-6 hr
Saskatchewan	-6 hr
Tegucigalpa	-6 hr

Field Value	GMT
Bogota	-5 hr
Panama	-5 hr
New York	-5 hr
Indiana	-5 hr
Caracas	-4.5 hr
Santiago	-4 hr
Halifax	-4 hr
Newfoundland	-3.5 hr
Brasilia	-3 hr
Buenos Aires	-3 hr
Recife	-3 hr
Nuuk	-3 hr
Mid-Atlantic	-2 hr
Azores	-1 hr
Reykjavik	0 hr
London	0 hr
Casablanca	0 hr
West Africa	1 hr
Amsterdam	1 hr
Berlin	1 hr
Madrid	1 hr
Paris	1 hr
Rome	1 hr
Stockholm	1 hr

Field Value	GMT
Athens	2 hr
Cairo	2 hr
Pretoria	2 hr
Helsinki	2 hr
Tel Aviv	2 hr
Amman	2 hr
Istanbul	2 hr
Riyadh	3 hr
Nairobi	3 hr
Tehran	3.5 hr
Moscow	4 hr
Abu Dhabi	4 hr
Baku	4 hr
Kabul	4.5 hr
Islamabad	5 hr
Mumbai	5.5 hr
Colombo	5.5 hr
Ekaterinburg	6 hr
Almaty	6 hr
Kathmandu	6.75 hr
Bangkok	7 hr
Beijing	8 hr
Perth	8 hr
Singapore	8 hr

Field Value	GMT
Taipei	8 hr
Kuala Lumpur	8 hr
Tokyo	9 hr
Seoul	9 hr
Adelaide	9.5 hr
Darwin	9.5 hr
Yakutsk	10 hr
Brisbane	10 hr
Sydney	10 hr
Guam	10 hr
Hobart	10 hr
Vladivostok	11 hr
Solomon Islands	11 hr
Wellington	12 hr
Fiji	12 hr

Country Field Values

The COUNTRY field is *optional* and, if included, follows the TIMEZONE field. These are examples of the COUNTRY field values that you can use in a CSV file:

Afghanistan

Albania

Algeria

American Samoa

Andorra

Angola

Anguilla

Antarctica

Antigua (including Barbuda)

Argentina

Armenia

Aruba

Ascension Islands

Australia

Austria

Azerbaijan

Bahamas

Bahrain

Bangladesh

Barbados

Belarus

Belgium

Belize

Benin

Bermuda

Bhutan

Bolivia

Bosnia-Herzegovina

Botswana

Brazil

British Virgin Islands

Brunei

Bulgaria

Burkina Faso

Burundi

Cambodia

Cameroon

Canada

Cape Verde Island

Cayman Islands

Central African Republic

Chad Republic

Chile

China

Colombia

Comoros

Cook Islands

Costa Rica

Croatia

Cuba

Cyprus

Czech Republic

Democratic Republic of the Congo

Denmark

Diego Garcia

Djibouti

Dominica

Dominican Republic

Ecuador

Egypt outside Cairo

El Salvador

Equatorial Guinea

Eritrea

Estonia

Ethiopia

Faeroe Islands

Falkland Islands

Fiji Islands

Finland

France

French Depts. (Indian Ocean)

French Guiana

French Polynesia

Gabon Republic

Gambia

Georgia

Germany

Ghana

Gibraltar

Greece

Greenland

Grenada

Guadeloupe

Guantanamo (U.S. Naval Base)

Guatemala

Guinea

Guinea-Bissau

Guyana

Haiti

Honduras

Hong Kong

Hungary

Iceland

India

Indonesia

Iran

Iraq

Ireland

Israel

Italy

Ivory Coast

Jamaica

Japan

Jordan

Kazakhstan

Kenya

Kiribati

Korea, North

Korea, South

Kuwait

Kyrgyzstan

Laos

Latvia

Lebanon

Lesotho

Liberia

Libya

Liechtenstein

Lithuania

Luxembourg

Macao

Macedonia

Madagascar

Malawi

Malaysia

Maldives

Mali

Malta

Marshall Islands

Mauritania

Mauritius

Mayotte Island

Mexico

Micronesia

Moldova

Monaco

Mongolia

Montenegro

Montserrat

Morocco

Mozambique

Myanmar

Namibia

Nauru

Nepal

Netherlands

Netherlands Antilles

New Caledonia

New Zealand

Nicaragua

Niger

Nigeria

Niue

Norfolk Island

Northern Mariana Islands

Norway

Oman

Pakistan

Palau

Panama

Papua New Guinea

Paraguay

Peru

Philippines

Poland

Portugal

Puerto Rico

Qatar

Republic of the Congo

Romania

Russia

Rwanda

San Marino

Sao Tome

Saudi Arabia

Senegal Republic

Serbia

Seychelles Islands

Sierra Leone

Singapore

Slovakia

Slovenia

Solomon Islands

Somalia

South Africa

Spain

Sri Lanka

St Helena

St Kitts and Nevis

St Lucia

St Pierre and Miguelon

St Vincent

Sudan

Suriname

Swaziland

Sweden

Switzerland

Syria

Taiwan

Tajikistan

Tanzania

Thailand

Togo

Tonga Islands

Trinidad and Tobago

Tunisia

Turkey

Turkmenistan

Turks and Caicos

Tuvalu

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States of America

Uruguay

Uzbekistan

Vanuatu

Vatican City

Venezuela

Vietnam

Wallis And Futuna Islands

Western Samoa

Yemen

Zambia

Zimbabwe

Exporting All User Accounts to a CSV File

You can export selected users to a CSV file.

Step 1 Sign in to 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 **Users** > **Import/Export Users**.

Step 3 Select **Export**.
Your user data is exported as a CSV file. The system emails the administrator a link to the exported file download. A **Download exported csv file** link appears in the window.

Step 4 Select the link to download the file and follow the instructions.

Importing User Accounts from a CSV File

To import a CSV file to the system:

Before You Begin

Prepare a comma- or tab-delimited (CSV) file containing the user account information. You can export the current system user account values to a CSV file, modify the file, and import it to add or change user accounts. See Exporting All User Accounts to a CSV File, on page 16 and Creating Comma- or Tab-Delimited Files, on page 3 for more information.

Step 1 Sign in to 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 **Users** > **Import/Export Users**.
The **Import/Export Users** page appears.

Step 3 Select **Import**.
The **Import Users** page appears.

Step 4 Select **Browse** and then select the CSV file to be imported.

Step 5 Select **Comma** or **Tab** to indicate which type of CSV file you are importing, comma-delimited or tab-delimited.

Step 6 Select **Import**.
The file is imported and the system sends an email indicating how many user accounts were imported successfully and how many accounts failed to be added or modified.

What to Do Next

Select **Users** to view the user accounts and verify that the values were imported correctly.

Transferring User Accounts Between Systems by using a CSV File

To transfer user accounts from one system to another by using a CSV file:

Step 1 Sign in to the Administration site on the system that contains the source of the user accounts to be transferred.

Step 2 Select **Users** > **Import/Export Users**.

Step 3 Select **Export**.
Your user data is exported as a CSV file. The system emails the administrator a link to the exported file download. A **Download exported csv file** link appears in the window.

Step 4 Optionally, open the exported CSV file, modify the user account values as needed, and save the CSV file. (See Creating Comma- or Tab-Delimited Files, on page 3 for more information.)

Step 5 Sign in to the target system Administration site.

Step 6 Select **Users** > **Import/Export Users**.
The **Import/Export Users** page appears.

Step 7 Select **Import**.
The **Import Users** page appears.

Step 8 Select **Browse** and then select the CSV file to be imported.

Step 9 Select **Comma** or **Tab** to indicate which type of CSV file you are importing, comma-delimited or tab-delimited.

Step 10 Select **Import**.
The file is imported and the system sends an email indicating how many user accounts were imported successfully and how many accounts failed to be added or modified.

What to Do Next

Select **Users** to view the user accounts and verify that the values were imported correctly.

Adding Users

Step 1 Sign in to 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 **Users** > **Add User**.

Step 3 Select the account type (**Auditor**, **Host**, or **Administrator**).
The Auditor option is visible, but is an available option only for the First Administrator.

Step 4 Complete the fields with the user information. Fields marked with an asterisk are required fields.

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.

Step 5 Check the **Session Type Allowed** in the Privileges section assigned to the user.
Selecting one of the highlighted session types shows the Session Type Features.

Step 6 Select the audio types (Telephony Privilege) allowed for this user.
Call-in teleconferencing allows the user to host a teleconference that participants can attend by calling a telephone number.

Call-back teleconferencing allows the user to host a session in which participants receive a telephone call from the WebEx service to join the teleconference. Each participant calls a telephone number and then hangs up the call. The service then calls that participant's telephone number.

Integrated VoIP allows the user to host as session that includes an Internet telephone (voice-over-IP) access to the teleconference.

Step 7 Select **Save**.
Cisco WebEx Meetings Server sends an Email to the user with a **Create Password** link. A user must create a password before signing in to the WebEx Common site.

The Create Password link expires after 72 hours. If the link has expired, the user can select the **Forgot Password** link to receive a new email message that gives them another opportunity to create a password.

The user is added to the system.

Editing Users

Change user account information or reserve a permanent host license for this user.

Important Users are identified to the system by Email address. If using SSO and a user Email address is changed and that user remains active, we recommend that you change the Email address on CWMS or that user will not receive notifications until the systems are synchronized.

After making a change to an existing user's email address, that user must wait until the Exchange server, Outlook, and CWMS server are synchronized before the scheduling of a meeting by a delegate (proxy) user hosted by that user with the modified email. Also attempting to schedule an alternate host with a recently modified email address will fail. The address book in Outlook is synchronized with the Exchange server once a day. When an email address is changed on the Exchange server, that change is not immediately propagated to Outlook. If, prior to synchronization, a user attempts to schedule a meeting for a user with a modified email address or identify them as an alternate host, the system receives the old email address and issues a notice that the user cannot be found. Manually synchronizing the systems does not solve this issue. Note that this is not a CWMS issue, but a result of the way Outlook and Exchange are designed.

Step 1 Sign in to 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 **Users**.
The default number of users shown on each page is 50. Use the **Users Per Page** drop-down menu to change the setting.

The list of users appears.

Step 3 Select the user to edit by double-clicking the user name.

Step 4 Select an **Account Type**.
Auditor separates administrative actions from system monitoring. (An existing user account cannot be changed to an Auditor account. The Auditor must be created by the First Administrator. See Auditor Role, on page 2 for more information.)

Host can schedule meetings and start meetings if they have an assigned license. A host can start up to two simultaneous meetings, but will receive an error when attempting to start a third meeting.

Attendee Only can attend meetings, but not schedule, start, host, or be an alternate host.

Administrators are created on the Add User page. Administrators can configure settings during system deployment and can make other users Hosts, Administrators, SSO Administrators, or LDAP Administrators. If an Auditor is configured on a system, an administrator cannot configure the Application Audit Log settings.

SSO or LDAP Administrators can change configuration settings after the system is operational. These users are synchronized into the system when the system is an SSO-integrated system or an LDAP-integrated system. Only the option that applies to your system appears as an account type. SSO and LDAP Administrators sign-in to the WebEx site URL and select the **Administration Site** link to connect to the Administration site. This type of administrator can add other administrators on the Add User page, can make users hosts, or make other users (synchronized on an SSO integrated or LDAP integrated system) SSO Administrators or LDAP Administrators..

Step 5 Make changes to the editable fields in the **Account Information** section. Fields marked with an asterisk are required.

Step 6 (Optional) Select **Reserve license** to provide this user with a permanent license to host meetings.
Typically, if available, a host license is granted when a user hosts a meeting for the first time. This option reserves an available license in the license pool and assigns it to the user without the user having to host a meeting. See About Host Licenses for details.

Step 7 (Optional) Select **Require user to change password at next sign in**.
If SSO or LDAP is enabled on your system, this feature is disabled for host accounts. It is available only for administrator and auditor passwords used to sign-in to the Administration site. Administrator and auditor continue to use the SSO or LDAP credentials to sign-in to their WebEx site.

Step 8 Check the **Session Type Allowed** in the Privileges section assigned to the user.
Selecting one of the highlighted session types shows the Session Type Features.

Step 9 Select the audio types (Telephony Privilege) allowed for this user.
Call-in teleconferencing allows the user to host a teleconference that participants can attend by calling a telephone number.

Call-back teleconferencing allows the user to host a session in which participants receive a telephone call from the WebEx service to join the teleconference. Each participant calls a telephone number and then hangs up the call. The service then calls that participant's telephone number.

Integrated VoIP allows the user to host as session that includes an Internet telephone (voice-over-IP) access to the teleconference.

Step 10 Select **Save**.
The changes are saved. Saving the parameters does not alter the status of the account. (See Activating or Deactivating Users or Administrators, on page 21.)

Unlocking an Account

To prevent unauthorized access, the system can automatically lock out an account holder account. This feature is off by default. The conditions that would cause an account holder to be locked out, such as number of failures or the period of inactivity, and how many minutes the account remains locked are configurable. When an account is locked, the system sends the locked account holder and all administrators an email indicating that the account is locked.

The following sections describe how to unlock an account.

Unlocking an Account from an Email

An administrator can select **Unlock Account** in the email to unlock their account. This option is off by default.

Unlocking an Account from a User Profile

An administrator that is not locked out of the system can select the locked-out account holder from the list on the **Users** tab to display the **Edit User** page and then select the **Unlock** link in the message displayed at the top of that page to unlock the account and notify the account holder that the account has been unlocked. This option is always on.

When an administrator account is locked, another administrator can select the **Unlock** link in the message that appears at the top of the **Edit User** page to unlock the account on behalf of the locked-out administrator.

Waiting Until the Timer Expires

When an account is locked and the optional timer is set, the account holder can log in when the timer expires.

Activating or Deactivating Users or Administrators

Use this feature to activate deactivated accounts or reactivate inactive accounts. The only accounts that cannot be deactivated are the Auditor accounts. Alternatively, you can activate an account by setting the parameter in a CSV file and importing it. See Importing User Accounts from a CSV File, on page 16 for more information.

Note

Step 1 Sign in to 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 **Users**.

Step 3 Select the check boxes for any inactive users you want to activate. Or select the check boxes for any active users you want to deactivate.

Step 4 Select **Actions** > **Activate** or **Actions** > **Deactivate**.
The selected accounts are modified and the status for each account reflects the updated status.

Finding Users

You can sort users by type, for example active or host, or by the type of license assigned to hosts. In addition to sorting users, you can also search users by first, last, or full name and by email address. The search results display user profile and license information.

Step 1 Sign in to the Administration site.

Step 2 Select **Users**.

Step 3 Select a category from the drop-down menu to sort users.

Step 4 (Optional) Use the **Expire in** drop-down to sort users with temporary licenses by license expiration (expired, 1 month, 3 months, 6 months).

Step 5 Type a user's name (first, last, or full name) or email address in the search field and select **Search**.

Configuring Tracking Codes

Use tracking codes to categorize meeting usage, such as breaking out the data for a project or a department. The tracking codes appear as options when you add or edit users.

Configure the following parameters for each tracking code:

- **Tracking code group–**Active groups can be chosen when you add or edit users.
- **Input mode–**Controls how the tracking code parameters appear when creating or editing a user.
- **Usage–**Prevents the group from displaying, being an optional entry, or a required entry.

Step 1 Sign in to 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 **Users** > **Tracking Codes**.

Step 3 (Optional) Enter the name of each group you want to configure in the **Tracking code group** column.
The default group names are Division, Department, Project, Other, and Custom5 through Custom10. Any of the group names can be changed.

Note Tracking code group names should be unique and you should not use predefined field names (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE).

Step 4 Select **Text Input** or **Dropdown Menu** for each tracking code in the **Input mode** column.

- Select **Text Input**. The administrator enters the tracking code in a text field creating or editing a user.
- Select **Dropdown menu**. An **Edit list** link appears next to the **Input mode** field. Select the **Edit list** link to configure the values for this tracking code. See Editing Tracking Codes, on page 22 for more information.

Step 5 Select **Not used** to prevent the tracking code from displaying when that user is created or edited. Select **Optional** to display, but not require a tracking code. Select **Required** to make assigning a tracking code to a user a requirement.

Step 6 Select **Save**.
Your tracking code parameters are saved.

Editing Tracking Codes

A list of tracking codes can be associated with a specific group that displays when adding or editing a user. This feature manages the tracking codes that display when those codes are selected from a drop-down menu.

Step 1 Sign in to 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 **Dropdown Menu** in the **Input mode** column for the group that you want to list tracking codes in the drop-down menu.
If you select **Text Input**, an input field displays next to the group where the administrator can enter any valid string.

Step 3 (Optional) If you chose **Dropdown Menu**, select **Edit list** to configure the values for this tracking code. The **Edit Tracking Code List** dialog box appears.

In addition to creating, editing, or deleting codes, you can deactivate or activate the code and indicate that a code in the list is the default code.

- Select **Show active codes only** to display only active tracking codes. Deselect this option to show all tracking codes. You cannot select this option the first time you configure tracking codes.
- Enter the drop-down menu code in the **Code** text box. This string is limited to 128 characters. If there are no empty tracking codes shown, select **Add 20 more lines** to add 20 more configurable tracking codes. The maximum number of tracking codes is 500 lines.
- Select **Default** to make a code the default selection.
- **Active** is selected by default. Uncheck **Active** to make a tracking code inactive. Inactive tracking codes do not appear on this tracking code group drop-down menu.
- Select **Update** to associate the codes with the group. You are returned to the **Tracking Codes** window.

Step 4 Select **Save** to save your settings.

Configuring Directory Integration

Directory integration enables your system to populate and synchronize your Cisco WebEx Meetings Server user database with the CUCM user database that is then integrated with an LDAP directory.

Directory integration simplifies user profile administration in the following ways:

- Imports user profiles from CUCM to Cisco WebEx Meetings Server.
- Periodically updates the Cisco WebEx Meetings Server database with new or modified user attributes in the CUCM database including each user's first name, last name, and email address. Cisco WebEx Meetings Server differentiates users by their email addresses, so if users have the same first name and last name but different email addresses, Cisco WebEx Meetings Server treats them as different users.
- Periodically checks the CUCM database for inactive user entries and deactivates their user profiles from the Cisco WebEx Meetings Server database.
- Enables the system to use LDAP authentication to authenticate Cisco WebEx Meetings Server directory integration users against the external directory.
- Supports fully encrypted LDAP integration when Secure LDAP (SLDAP) is enabled on CUCM and the LDAP server.
- All users configured in CUCM are synchronized to Cisco WebEx Meetings Server and their accounts are activated. You can optionally deactivate accounts after the synchronization is complete. All active users in CUCM are synchronized into Cisco WebEx Meetings Server. Inactive users are not imported into Cisco WebEx Meetings Server. (Users can be manually added into CUCM for environments where LDAP/AD is not available or configured in CUCM.)

Before You Begin

Make sure the following prerequisites are met before you proceed with directory integration:

- In Site Administration **Settings** > **User Management**, set the **Default user account type** to **Host** or to .
- Schedule synchronization during off-peak hours or on weekends to minimize the impact on your users.
- Verify that you have a supported version of Cisco Unified Communications Manager (CUCM). Refer to the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-configure.html for more information.
- Obtain CUCM administrative user credentials (required to add a CUCM server for directory integration).
- Configure AXL and LDAP directory service on CUCM. CUCM is required to import users into your Cisco WebEx Meetings Server system. Use CUCM to do the following:
    - Enable Cisco AXL Web Service
    - Enable Cisco directory synchronization
    - Configure LDAP integration
    - Configure LDAP authentication

  See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 28 and Using CUCM to Configure LDAP Integration and Authentication, on page 29. Refer to the http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html for additional information.
- Make sure that all users who require host privileges are available in CUCM. Any user not in CUCM will not be able to host meetings (all users can join as a guest). If necessary, create CUCM groups or filters, which include only the users that you want to import from CUCM.

Note If you do not use CUCM groups, the system imports all active CUCM users during the first directory synchronization. Inactive CUCM users are not imported. The system imports only active new and modified users during subsequent synchronizations. Deactivate user accounts that you do not want to give host access to. Note that a host license is only consumed in Cisco WebEx Meetings Server when a user actually hosts a meeting. Accounts that do not host meetings do not consume licenses. See "Managing Licenses" in Managing Host Licenses for more information about license consumption.

- Users without email address are not imported.
- If users have multiple accounts that use the same first name and last name but are assigned different email addresses on CUCM, when these users are imported to Cisco WebEx Meetings Server these addresses are treated as different users. CUCM users are unique by username so an administrator can create multiple user accounts with the same email address. However, accounts on the Cisco WebEx Meeting Server are unique by email address. Therefore, if multiple CUCM user accounts have the same email address, the administrator for CUCM should manually edit these user accounts to make the email addresses unique before importing those accounts to the Cisco WebEx Meetings Server.
- When LDAP authentication is enabled, Cisco WebEx Meetings Server uses port 8443 to connect to CUCM when you select the **Synchronize Now**, or check the **Next synchronization** option and enter a date and time.

- Cisco WebEx Meetings Server supports passwords up to 64 characters. When creating a user on CUCM, ensure that a password is no more than 64 characters. Users with passwords greater than 64 characters will not be able to sign into Cisco WebEx.

Step 1 Sign in to 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 (Optional) **Turn On Maintenance Mode**.
Maintenance mode is *not required* to perform directory integration but a large synchronization can affect system performance. You can put your system into maintenance mode to prevent users from using the system during a synchronization.

Step 3 Select **Users** > **Directory Integration**.

Step 4 (Optional) Select the server (under CUCM) to enter your CUCM server information if you have not done so already:

- IP Address or fully qualified domain name (FQDN)
- Username
- Password

The username and password can be your CUCM administrator or AXL username and password. After you configure your CUCM information, the IP address or FQDN of your CUCM server appears under the CUCM icon.

Note After you have configured your CUCM information, changing it is a complex procedure that can cause user synchronization problems and is not recommended.

Step 5 Select **CUCM User Groups for Filtering** to add only those users in the selected CUCM User Groups in to Cisco WebEx Meeting Server.

Step 6 (Optional) Select **Full Synchronization** to synchronize all users in the selected CUCM groups. When it is not selected, the system synchronizes only the users updated or added to the selected CUCM groups since the most recent update of the Directory Service user profile.
This option affects only the Synchronize Now option in the next step; it does not affect a scheduled (Next) synchronization.

We recommend that this action be performed as part of events such as, the CUCM server has been changed on CWMS, the email addresses of users have been changed on CUCM, or a user is deleted from the group on CUCM.

Depending on the size of the CUCM user database, system performance could be impacted when you chose to synchronize the entire database.

Step 7 Synchronize your Cisco WebEx Meetings Server system with your LDAP directory service. You can perform your synchronization in the following ways:

- Select **Synchronize Now** to perform a synchronization immediately. You cannot cancel synchronization once it starts. You are sent an email when the synchronization is complete. The other administrators on your system are not notified after a **Synchronize Now**.
- Select **Next synchronization** and enter a date and time to schedule synchronization. You can chose to **Repeat** synchronization at regular intervals.

In an MDC system, the synchronization of each data center should be performed either at different times or it should be active on only one of the data centers to avoid the degradation of system performance.

If you select **Synchronize Now**, your system immediately performs a synchronization. If you schedule a synchronization, it occurs at the specified date and time. All administrators receive an email after a scheduled synchronization is complete. If you want to prevent future synchronization, you can deselect **Next synchronization**.

The following attributes are mapped during the synchronization process:

CUCM Attribute	Cisco WebEx Meetings Server Attribute
First Name	First Name
Last Name	Last Name
Mail ID	Email Address

Note The first name and last name in Cisco WebEx Meetings Server are components of the full name that is displayed to users.

Mapped attributes in Cisco WebEx Meetings Server cannot be updated by end users.

If your synchronization fails, an error message appears on the page and an email with detailed information about the error is sent to the administrator. Select **View Log** to see a detailed explanation of the error. The logs provided include a deactivated user report, failed user report, and a summary.

After you have performed at least one synchronization, a summary of your last synchronization appears indicating whether or not it was completed, the time and date it was completed (using the time and date configured in your Company Info settings), and a listing of user changes including the following:

- Added—The number of new users added.
- Deactivated—The number of users who were deactivated.

Step 8 Select **Save** if you have configured or changed your synchronization schedule or your administrator notification settings.

Step 9 Select the **Users** tab and make sure that the correct users have been synchronized.

a) Select **Remote users** on the drop-down menu to filter the user list. Make sure that the users you wanted synchronized are present in the list. Remote users are imported into Cisco WebEx Meetings Server through a directory synchronization. If a user is created locally first and is overwritten by a directory synchronization, this user will become a remote user, not a local user.

b) Select **Local users** to see which users were not included in the synchronization. Local users are created locally by a Cisco WebEx Meetings Server administrator. Local users can be added manually or imported using a CSV file.

Step 10 Make sure your CUCM and Cisco WebEx Meetings Server synchronization schedules are sequential. Your CUCM synchronization must occur first and your Cisco WebEx Meetings Server synchronization should occur immediately afterward.

Step 11 (Optional) Select or deselect **Notify administrators when synchronization completes** and then select **Save**. This option is selected by default and only informs administrators after a *scheduled* synchronisation.

Step 12 Select **Enable LDAP Authentication**.

Note If your system is configured to use SSO, you must first disable SSO. See Disabling SSO for more information. If your system is not configured to use SSO, it uses its default authentication until you enable LDAP authentication.

After enabling LDAP we recommend that administrators use Active Directory server for user management including adding, disabling, and modifying users. After enabling LDAP authentication, all participants must use their LDAP credentials to sign in to the WebEx site.

Step 13 Make sure that your users can sign into the system with their AD domain credentials.

Step 14 (Optional) If you put your system in maintenance mode **Turn Off Maintenance Mode**.

Step 15 (Optional) If you have performed a synchronization, you can select **Notify Now** to notify users by email that accounts have been created for them on your Cisco WebEx Meetings Server system or when their accounts have been changed. You can optionally select **Automatically send out notifications**, which automatically sends an email to your newly added users after each synchronization. After any change to the authentication settings (for example, enabling LDAP), the Users–Password Changed email is sent to affected users.
When you select **Notify Now**

- All users receive only one notification in their lifetime. Subsequent synchronization do not cause additional emails to be sent.
- "Users that require notification" indicates all users that are active and have not been notified yet.
- Inactive users or local users are not sent any notification.
- Adding a local user on Cisco WebEx Meetings Server sends an email to this user. However, this user must be added on your CUCM Active Directory server before he can sign in to the WebEx site.
- You can only send notifications to users who were added using the synchronization feature.
- It might take a few minutes for your email notifications to be sent to your users. This delay is caused by several factors that are external to your Cisco WebEx Meetings Server system including your email server, network connectivity issues, and spam catchers on individual email accounts.

Your system sends the following emails:

- The AD Activation Email is sent to each user the first time they are imported into your system in a synchronization. Users do not receive this email on subsequent synchronization.
- The User Password–Changed email is sent to users who were created locally on your system.

See "About "Email Templates (v2.6 and Earlier)" for information on customizing these email templates.

Note If you are using Directory Integration with LDAP authentication, users configured in CUCM are synchronized into Cisco WebEx Meeting Server as hosts and use their LDAP credentials to sign in to their WebEx site. However, if you change an imported user account type from **host** to **administrator**, the user receives an email with a Create Password link. A user selects this link and enters a new password for Cisco WebEx Meetings Server. The user will use this newly created password to sign in to the Administration site, but will continue to use the LDAP credentials to sign in to their WebEx site.

Synchronizing User Groups

Administrator can create groups of users in CUCM. For example, an administrator might create a user group consisting of users who will be allowed to use Cisco WebEx Meetings Server. From CWMS, the administrator can filter and import certain users by selecting specific user groups.

Before You Begin

Use CUCM to create groups of users. Refer to the "User Management Configuration" section in the *Cisco Unified Communications Manager Administration Guide* http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html for more information.

Step 1 Sign in to 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 **Users** > **Directory Integration**.

Step 3 Select the **CUCM Groups for Filtering** link.

Step 4 Check the user groups to be synchronized.

Note If no groups are selected, directory integration synchronizes all user groups.

Step 5 Select **Save**.

Step 6 Select Synchronize Now to perform the synchronization. The time this process takes varies depending on the number of users being synchronized.

Note The system remembers which user groups were previously synchronized. If you do not select a user group that was previously synchronized, the users in the unselected user group will be deactivated during the synchronization process.

When the synchronization is finished, the system displays the number of users added and deactivated.

Step 7 Select **View Log** for summary information about the users who were imported or deactivated during the synchronization process.

Using CUCM to Configure AXL Web Service and Directory Synchronization

Use CUCM to configure AXL Web Service and directory synchronization.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 23 for more information.

Step 1 Sign in to your CUCM account.

Step 2 Select **Cisco Unified Serviceability** from the top right dropdown menu and then select **Go**.

Step 3 Select **Tools** > **Service Activation**.

Step 4 Select **Cisco AXL Web Service** and **Cisco DirSync** and then select **Save**.

Note If a Cisco Unified Call Manager (CUCM) failover condition occurs in a data center that is part of a Multi-data Center (MDC) system, the CUCM administrator credentials should work for all CUCMs in that data center.

What to Do Next

Use CUCM to configure LDAP integration and authentication if you have not already done so. See Using CUCM to Configure LDAP Integration and Authentication, on page 29 for more information.

Using CUCM to Configure LDAP Integration and Authentication

Use CUCM to configure LDAP integration and authentication.

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 If CUCM is configured for Directory Integration, you can choose to use SSO, LDAP, or local authentication.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 23 for more information.

Step 1 Sign in to your Cisco Unified Call Manager (CUCM) account.

Step 2 Select **Cisco Unified CM Administration** from the top right drop-down menu and then select **Go**.

Step 3 Select **File** > **LDAP** > **LDAP System**.

Step 4 Select **Enable Synchronizing from LDAP Server**, select **Microsoft Active Directory** for the LDAP Server Type, select **sAMAccountName** for the LDAP Attribute for User ID, and select **Save**.

Step 5 Select the check box for your LDAP server and then select **Add New**.

Step 6 Complete the fields on the LDAP Directory page and then select **Save**.

Step 7 On the LDAP Authentication page, select the **Use LDAP Authentication for End Users** check box, complete the fields on the page, and then select **Save**.

What to Do Next

Use CUCM to configure Cisco AXL Web Service and Cisco Directory Sync if you have not already done so. See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 28 for more information.

Emailing Users

Step 1 Sign in to 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 To send email notifications to users, select **Users** > **Email Users**.

Step 3 Enter a target user email address or an email alias in the **To** field, or leave the field blank to send email to all users.

Step 4 (Optional) Enter email addresses or an email alias in the **BCC** field.

Step 5 Enter the subject in the **Subject** field.

Step 6 Enter a message in the **Message** field.

Step 7 Select **Send**.
It might take a few minutes for your emails to be received by the users. This delay might be caused by several factors that are external to your Cisco WebEx Meetings Server system, including your email server, network connection speed, and spam catchers on individual email accounts.

Your email is sent.