



## Multilevel Administration Access

---

Multilevel administration access provides multiple levels of security to Cisco CallManager Administration. This technique permits granting only the required privileges for a selected group of users and limits the configuration functions that users in a particular user group can perform.

Prior to the availability of multilevel administration access, administrators with read/write access to Cisco CallManager configuration could change any or all the database/directory elements that are accessible through Cisco CallManager Administration and Cisco CallManager Serviceability. Users could inadvertently disable the entire system with a few mouse clicks by accidentally modifying the data to which they do not need access.

Use the following topics to understand multilevel administration access:

- [Key Features, page 4-2](#)
- [Login Authentication, page 4-2](#)
- [Functional Groups, page 4-3](#)
- [User Groups, page 4-3](#)
- [User Group Access Privileges, page 4-4](#)
- [Access Logs, page 4-5](#)
- [MLA Enterprise Parameters, page 4-6](#)
- [Standard User Groups and Functional Groups, page 4-8](#)
- [Where to Find More Information, page 4-13](#)

# Key Features

Multilevel administration access provides multiple levels of security to Cisco CallManager Administration. Cisco CallManager Administration functions comprise functional groups. Each functional group can have different access levels, such as no access, read-only access, and full access, to different user groups. Multilevel administration access also provides audit logs of user logins and access and modifications to Cisco CallManager configuration data.

## Login Authentication

Prior to the availability of multilevel administration access, Cisco CallManager administrators logged in using a local NT administration account. With multilevel administration access, directory user names and passwords stored in Lightweight Directory Access Protocol (LDAP) provide the basis for login authentication. Multilevel administration access creates a predefined super user called the *CCMAdministrator*.

The windows registry stores the CCMAdministrator's user ID and encrypted password. Thus, even when the directory is unavailable, CCMAdministrator can log in to take corrective action. When the user attempts direct access by entering a URL in the browser, a login window displays first to authenticate a user.

**Note**

---

MLA provides authentication for Cisco CallManager (CCM) Administration, CCM Serviceability, CCM Trace Analysis, CCM Trace Collection Tool, Real Time Monitoring Tool (RTMT), Admin Serviceability Tool (AST), and Serviceability SOAP applications. If MLA is enabled, login works only for the CCMAdministrator.

---

**Note**

---

or any other LDAP user belonging to a MLA usergroup. After upgrade to Cisco CallManager 4.0(x) from either Cisco CallManager 3.3(x) or Cisco CallManager 3.2(x) with multilevel administration access enabled, the password for the super user CCMAdministrator is reset. At the end of the upgrade, a message box displays the new CCMAdministrator password. Use this password and change it to a unique value.

---

If installation of Cisco CallManager 4.0(x) is an upgrade of a previous version for which MLA was not enabled, change the Enable MultiLevelAdmin enterprise parameter to enable multilevel administration access. Refer to [“Enable MultiLevelAdmin”](#) in the [“MLA Enterprise Parameters”](#) section on page 4-6.

---

## Functional Groups

A functional group includes a collection of Cisco CallManager system administration functions. All the web pages that compose each functional group belong to a common administrative menu. Two types of functional groups exist: standard functional groups, which are the default functional groups, and custom functional groups. Standard functional groups are created as part of multilevel administration access installation. Users may define custom functional groups.



### Note

---

All standard functional groups get created at installation. You cannot modify or delete standard functional groups.

---

The system creates the following standard functional groups at the time of installation:

- Standard System
- Standard RoutePlan
- Standard Service Management
- Standard Feature

For the complete listing of functional groups, see the [“Standard User Groups and Functional Groups”](#) section on page 4-8.

## User Groups

A user group comprises a collection of Cisco CallManager users that are grouped together for the purpose of assigning an access privilege level to the members in the user group.

Various named user groups that are predefined have no members assigned to them at install time. The Cisco CallManager super user or a user with access to user group configuration should add users to these groups and set the access rights for the user groups. The super user or a user with access to user group configuration can configure additional named user groups as needed.

The following user groups get created at the time of installation:

- SuperUserGroup
- ReadOnly
- PhoneAdministration
- GatewayAdministration

**Note**


---

The SuperUserGroup represents a named user group that always has full access permission to all named functional groups. You cannot delete this user group. You can only make additions and deletions of users to this group.

---

**Note**


---

CCAdministrator always represents a super user, even though CCAdministrator is not a member of the SuperUserGroup.

---

**Note**


---

You can delete standard user groups that are created at installation, except for the SuperUserGroup.

---

For the complete listing of user groups, see the [“Standard User Groups and Functional Groups”](#) section on page 4-8.

## User Group Access Privileges

One of the following access privileges applies to named user groups for access to the functional groups:

- No Access
- Read Only
- Full Access

For each user group, one of these privilege levels applies for access to each of the functional groups. The access privileges specify the following privileges:

- Access privilege *No Access* specifies that users in a user group with this privilege defined for a particular functional group can neither view nor change any pages that belong to that functional group. No access exists to pages in a functional group for which a user has access privilege *No Access*.
- Access privilege *Read Only* specifies that users in a user group with this privilege defined for a particular functional group can only view the pages that belong to that functional group, but cannot modify these pages. Access privilege *Read Only* limits access to pages in a functional group to read operations. Buttons such as **Insert**, **Delete**, **Update**, and **Reset** appear as grayed out to prevent modifications to database and directory data.
- Access privilege *Full Access* specifies that users in a user group with this privilege defined for a particular functional group can view and change any pages that belong to that functional group. Users with full access privilege can perform operations such as Insert, Delete, Update and Reset, as well as executive functions that can start or stop a process or service from the Cisco CallManager Administration and Serviceability pages.

Install assigns default access privileges to the user groups for the functional groups that are created at install time.

## Access Logs

Multilevel administration access generates a log with a record of login attempts. The log includes the user name, group name, date, time, and success or failure status of the login session.

The log also contains a file report of access/change attempts. That is, multilevel administration access generates a record of attempts to access or modify any directory or database component through the Cisco CallManager system administration. The change record includes the user name, date, time, menu accessed, web page from which the change was made, and the success or failure status of the update.

Find the log file under the Log directory in c:\Program Files\Cisco\Trace\MLA, filename Accessxx.log (where xx are numeric digits).

Additional data is stored in the ISAPI permission logs. Filenames are ISAPIFilter\*\*.exe and Permissions\*\*.exe.

# MLA Enterprise Parameters

Multilevel administration access uses the following enterprise parameters:

- User Group Base
- Administrative User Base
- Debug Level
- Effective Access Privileges For Overlapping User Groups
- Effective Access Privileges For Overlapping Functional Groups
- Enable MultiLevelAdmin

## User Group Base

The User Group Base enterprise parameter designates the user group base that multilevel administration access uses.

The User Group Base enterprise parameter includes the following default values:

- In DC Directory, User Group Base parameter is set to ou=MultiLevelAdmin, ou=Admins, <Cisco-base>.
- In Netscape Directory, User Group Base parameter is set to ou=MultiLevelAdmin, ou=CCN, <Cisco-base>.
- In Active Directory, User Group Base parameter is set to ou=MultiLevelAdmin, <Cisco-base>.

You can change this enterprise parameter to make use of the windows groups that are created in Active Directory.

## Administrative User Base

The Administrative User Base enterprise parameter designates the administrative user base that multilevel administration access uses.

The Administrative User Base enterprise parameter is set, by default, to the enterprise user base found in the system profile. You can change this enterprise parameter to make use of the windows groups that are created in Active Directory.

### Debug Level

The Debug Level enterprise parameter designates a value that is used to set debug level (None, Trace, or Debug) for MLA debug logs. Set this parameter to *None* to turn off debug, to *Trace* to generate trace information, and to *Debug* to generate debug information.

The Debug Level enterprise parameter specifies a default value of Trace. The debug log files are stored in the directory c:\Program Files\Cisco\Trace\MLA in filename DirAndUI\*\*.\*.log.

### Effective Access Privileges for Overlapping User Groups

The Effective Access Privileges For Overlapping User Groups enterprise parameter determines the level of user access for users that belong to multiple user groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping user groups.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping user groups.

The Effective Access Privileges For Overlapping User Groups enterprise parameter specifies the following default value: Maximum.

### Effective Access Privileges for Overlapping Functional Groups

The Effective Access Privileges For Overlapping Functional Groups enterprise parameter determines the level of user access for Cisco CallManager web pages that belong to multiple functional groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping functional groups.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping functional groups.

The Effective Access Privileges For Overlapping Functional Groups enterprise parameter specifies the following default value: Maximum.

### Enable MultiLevelAdmin

The Enable MultiLevelAdmin enterprise parameter designates whether multilevel administration access is enabled.

You can set this enterprise parameter to the following values:

- True—Multilevel administration access is enabled.
- False—Multilevel administration access is disabled.

The Enable MultiLevelAdmin enterprise parameter specifies the following default value: False.

When the Enable MultiLevelAdmin enterprise parameter value is modified, the CCMA administrator must perform the following steps to act on the modified value:

1. Go to **Start > Programs > Administrative Tools > Services**.
2. Select and right-click the Worldwide Web Publishing service.
3. Select **Stop**, then select **Start**.

## Standard User Groups and Functional Groups

This section provides the complete list of standard user groups and standard functional groups that become available when you enable Cisco CallManager multilevel administration access. This section comprises the following topics:

- [Standard Functional Groups, page 4-8](#)
- [Standard User Groups, page 4-9](#)
- [Standard User Group and Functional Group Privilege Mapping, page 4-9](#)

## Standard Functional Groups

Cisco CallManager multilevel administration access creates standard functional groups. The following functional groups comprise the standard functional groups:

- Standard Plugin
- Standard User Privilege Management
- Standard User Management
- Standard Feature

- Standard System
- Standard Service Management
- Standard Service
- Standard Serviceability
- Standard Gateway
- Standard RoutePlan
- Standard Phone

## Standard User Groups

Cisco CallManager multilevel administration access creates standard user groups at installation. The following user groups comprise the standard user groups:

- SuperUserGroup
- ReadOnly
- PhoneAdministration
- GatewayAdministration
- ServerMonitoring
- ServerMaintenance

## Standard User Group and Functional Group Privilege Mapping

[Table 4-1](#) provides the default mapping of privileges for the standard user groups and functional groups.

**Table 4-1 Standard User/Functional Group Mapping**

<b>User Group</b>	<b>Functional Group</b>	<b>Permission</b>
GatewayAdministration	Standard Feature	Read Only
	Standard Gateway	Full Access
	Standard Phone	Read Only
	Standard Plugin	Ready Only
	Standard RoutePlan	Full Access
	Standard Service	Read Only
	Standard Service Management	Read Only
	Standard Serviceability	Read Only
	Standard System	Read Only
	Standard User Management	Read Only
	Standard User Privilege Management	Read Only
PhoneAdministration	Standard Feature	Read Only
	Standard Gateway	Read Only
	Standard Phone	Full Access
	Standard Plugin	Read Only
	Standard RoutePlan	Read Only
	Standard Service	Read Only
	Standard Service Management	No Access
	Standard Serviceability	Read Only
	Standard System	No Access
	Standard User Management	Full Access
	Standard User Privilege Management	Read Only

**Table 4-1 Standard User/Functional Group Mapping (continued)**

<b>User Group</b>	<b>Functional Group</b>	<b>Permission</b>
ReadOnly	Standard Feature	Read Only
	Standard Gateway	Read Only
	Standard Phone	Read Only
	Standard Plugin	Read Only
	Standard RoutePlan	Read Only
	Standard Service	Read Only
	Standard Service Management	Read Only
	Standard Serviceability	Read Only
	Standard System	Read Only
	Standard User Management	Read Only
	Standard User Privilege Management	Read Only
ServerMaintenance	Standard Feature	Full Access
	Standard Gateway	Read Only
	Standard Phone	Read Only
	Standard Plugin	Full Access
	Standard RoutePlan	Read Only
	Standard Service	Full Access
	Standard Service Management	Full Access
	Standard Serviceability	Read Only
	Standard System	Full Access
	Standard User Management	Read Only
	Standard User Privilege Management	Full Access

**Table 4-1 Standard User/Functional Group Mapping (continued)**

<b>User Group</b>	<b>Functional Group</b>	<b>Permission</b>
ServerMonitoring	Standard Feature	Read Only
	Standard Gateway	Read Only
	Standard Phone	Read Only
	Standard Plugin	Read Only
	Standard RoutePlan	Read Only
	Standard Service	Read Only
	Standard Service Management	Read Only
	Standard Serviceability	Full Access
	Standard System	Read Only
	Standard User Management	Read Only
	Standard User Privilege Management	Read Only
SuperUserGroup	Standard Feature	Full Access
	Standard Gateway	Full Access
	Standard Phone	Full Access
	Standard Plugin	Full Access
	Standard RoutePlan	Full Access
	Standard Service	Full Access
	Standard Service Management	Full Access
	Standard Serviceability	Full Access
	Standard System	Full Access
	Standard User Management	Full Access
	Standard User Privilege Management	Read Only

# Where to Find More Information

## Related Topic

- [Multilevel Administration Access Configuration](#), *Cisco CallManager Administration Guide*

## Additional Cisco Documentation

- *Installing Cisco CallManager*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*

■ Where to Find More Information