



# Multilevel Administration

Multilevel Administration (MLA) は、Cisco CallManager Administration に対して複数のセキュリティ レベルを提供します。この手法により、選択されたユーザグループに必要な特権だけを与えることが可能になり、特定ユーザグループ内のユーザが実行できる設定機能を制限します。

MLA が使用可能になる前は、Cisco CallManager 設定に対して読み取りおよび書き込みアクセス権のある管理者であれば、Cisco CallManager Administration および Cisco CallManager Serviceability からアクセス可能なデータベース要素およびディレクトリ要素の一部またはすべてを変更することができました。ユーザはマウスを数回クリックしてアクセスする必要がないデータを誤って変更することにより、意図せずにシステム全体を使用不可にしてしまう場合があります。

次のトピックを使用して MLA を説明します。

- [主な機能 \(P.4-2\)](#)
- [ログイン認証 \(P.4-3\)](#)
- [機能グループ \(P.4-4\)](#)
- [ユーザグループ \(P.4-5\)](#)
- [ユーザグループのアクセス特権 \(P.4-6\)](#)
- [アクセスログ \(P.4-7\)](#)
- [MLA エンタープライズパラメータ \(P.4-8\)](#)
- [標準ユーザグループおよび標準機能グループ \(P.4-12\)](#)
- [参考情報 \(P.4-16\)](#)

## 主な機能

MLA は、Cisco CallManager Administration に対して複数のセキュリティ レベルを提供します。Cisco CallManager Administration 機能には、機能グループがあります。各機能グループは、さまざまなユーザ グループに対して異なるアクセス レベル（アクセス権なし、読み取り専用アクセス、およびフル アクセスなど）を持つことができます。また、MLA によって、ユーザ ログインの監査ログが提供され、Cisco CallManager 設定データに対するアクセスおよび変更が可能になります。

## ログイン認証

MLA が使用可能になる前は、Cisco CallManager 管理者はローカル NT 管理アカウントを使用してログインしました。MLA を使用すると、Lightweight Directory Access Protocol (LDAP) に保管されたディレクトリのユーザ名およびパスワードによって基本的なログイン認証が提供されます。MLA は、*CCMAdministrator* という定義済みのスーパー ユーザを作成します。

Windows レジストリは *CCMAdministrator* のユーザ ID および暗号化されたパスワードを保管します。したがって、ディレクトリが使用できない場合でも、*CCMAdministrator* はログインして対応策をとることができます。ユーザがブラウザに URL を入力して直接アクセスしようとすると、まずユーザを認証するためのログイン ウィンドウが表示されます。



(注) MLA は、Cisco CallManager Administration、Cisco CallManager Serviceability、Cisco CallManager Trace Analysis、Cisco CallManager Trace Collection Tool、Real Time Monitoring Tool (RTMT)、および Serviceability SOAP アプリケーションに認証機能を提供します。MLA が使用可能な場合、ログイン機能は、*CCMAdministrator*、または、MLA ユーザ グループに所属するその他の LDAP ユーザに対してだけ動作します。



(注) MLA が使用可能な状態で Cisco CallManager 3.3(x) または Cisco CallManager 3.2(x) から Cisco CallManager 4.1(x) にアップグレードした場合、スーパーユーザ *CCMAdministrator* のパスワードはリセットされます。アップグレードの最後に、新しい *CCMAdministrator* パスワードがメッセージ ボックスに表示されます。このパスワードを使用し、パスワードを固有の値に変更してください。

Cisco CallManager のインストーラが、MLA を使用できない以前のバージョンからのアップグレードである場合には、Enable MultiLevelAdmin エンタープライズパラメータを変更して MLA を使用可能にします。P.4-8 の「[MLA エンタープライズパラメータ](#)」の「[Enable MultiLevelAdmin](#)」を参照してください。

## 機能グループ

機能グループは Cisco CallManager システム管理機能を集めたものです。共通の管理メニューには、各機能グループが含まれます。機能グループには、デフォルトの機能グループである標準機能グループと、カスタム機能グループという 2 つのタイプがあります。標準機能グループは、MLA のインストールの一部として作成されます。ユーザはカスタム機能グループを定義することができます。



(注)

---

すべての標準機能グループはインストール時に作成されます。標準機能グループは変更も削除もできません。

---

インストール時に次の標準機能グループがシステムによって作成されます。

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

機能グループの全リストについては、[P.4-12](#) の「標準ユーザグループおよび標準機能グループ」を参照してください。

## ユーザグループ

ユーザグループとは、アクセス特権レベルをユーザグループ内のメンバーに割り当てるために、グループ化された Cisco CallManager ユーザの集まりです。

あらかじめ定義されたさまざまな名前のユーザグループがありますが、インストール時にはどのグループにもメンバーが割り当てられません。

Cisco CallManager スーパーユーザか、またはユーザグループ設定にアクセスできるユーザが、これらのグループにユーザを追加して、そのユーザグループにアクセス権を設定する必要があります。スーパーユーザ、またはユーザグループ設定にアクセスできるユーザは、必要に応じて追加の名前付きユーザグループを設定することができます。

インストール時に次のユーザグループが作成されます。

- SuperUserGroup
- ReadOnly
- PhoneAdministration
- GatewayAdministration



(注) SuperUserGroup は、すべての名前付き機能グループに対するフル アクセス権限を常に持つ名前付きユーザグループです。このユーザグループは削除できません。このグループに対してはユーザの追加および削除だけが可能です。



(注) CCMAAdministrator は CCMAAdministrator が SuperUserGroup のメンバーではない場合も、常にスーパーユーザを表します。



(注) インストール時に作成される標準ユーザグループは削除することができます。ただし、SuperUserGroup は削除できません。

ユーザグループの全リストについては、[P.4-12](#)の「標準ユーザグループおよび標準機能グループ」を参照してください。

## ユーザ グループのアクセス特権

機能グループにアクセスするため、次のアクセス特権のいずれかが名前付きユーザ グループに適用されます。

- No Access
- Read Only
- Full Access

各機能グループにアクセスするために、これらの特権レベルのいずれかが各ユーザ グループに割り当てられます。アクセス特権によって次の特権が指定されま

- アクセス特権 *No Access* は、この特権が特定機能グループに定義されているユーザ グループ内のユーザが、その機能グループに属するすべてのウィンドウについて表示も変更もできないことを指定する。アクセス特権 *No Access* を持つユーザには、機能グループ内のウィンドウへのアクセス権がありません。
- アクセス特権 *Read Only* は、この特権が特定機能グループに定義されているユーザ グループ内のユーザが、その機能グループに属するウィンドウを表示することだけはできるが、ウィンドウの変更はできないことを指定する。アクセス特権 *Read Only* は、機能グループ内のウィンドウへのアクセスを読み取り操作に限定します。**Insert**、**Delete**、**Update** および **Reset** などのボタンは、データベースおよびディレクトリ データが変更されないようにするため、グレー表示されます。
- アクセス特権 *Full Access* は、この特権が特定機能グループに定義されているユーザ グループ内のユーザが、その機能グループに属するすべてのウィンドウを表示および変更できることを指定する。フルアクセス特権を持つユーザは **Insert**、**Delete**、**Update** および **Reset** などの操作を行うことができ、**Cisco CallManager Administration** および **Serviceability** からプロセスやサービスを開始あるいは停止できる管理機能も実行できます。

インストールではデフォルトのアクセス特権が、インストール時に作成される機能グループのユーザ グループに対して割り当てられます。

## アクセス ログ

MLA はログインを試行した記録の入ったログを生成します。このログには、ユーザ名、グループ名、日付、時刻、および成功または失敗のログインセッション状況が含まれます。

また、試みたアクセスおよび変更に関するファイル レポートも含まれます。つまり、MLA は **Cisco CallManager Administration** を使用してディレクトリまたはデータベース コンポーネントにアクセスまたは変更を試みた記録を生成します。変更記録には、ユーザ名、日付、時刻、アクセスされたメニュー、変更で使用されたウィンドウ、および成功または失敗の更新状況が含まれます。

c:\Program Files\Cisco\Trace\MLA の Log ディレクトリの下にあるログ ファイルを検索します。ファイル名は Accessxx.log (xx は数字) です。

その他のデータは、ISAPI アクセス許可のログに保管されます。ファイル名は ISAPIFilter\*.txt および Permissions\*.txt (\* はトレース ファイル番号) です。

## MLA エンタープライズ パラメータ

MLA では次のエンタープライズ パラメータを使用します。

- 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 Cache Flush Timeout (Minutes)

### User Group Base

User Group Base エンタープライズ パラメータは、MLA で使用するユーザ グループの基本要素を指定します。

User Group Base エンタープライズ パラメータには次のデフォルト値が含まれます。

- DC Directory で User Group Base パラメータは次のように設定される。  
ou=MultiLevelAdmin, ou=Admins, <Cisco-base>
- Netscape Directory で User Group Base パラメータは次のように設定される。  
ou=MultiLevelAdmin, ou=CCN, <Cisco-base>
- Active Directory で User Group Base パラメータは次のように設定される。  
ou=MultiLevelAdmin, <Cisco-base>

このエンタープライズ パラメータは、Active Directory で作成される Windows グループを使用するように変更することができます。

### Administrative User Base

Administrative User Base エンタープライズ パラメータは、MLA で使用する管理ユーザの基本要素を指定します。

デフォルトで Administrative User Base エンタープライズ パラメータは、システムプロファイル内で検出されたエンタープライズ ユーザ基本要素に設定されます。このエンタープライズ パラメータは、Active Directory で作成される Windows グループを使用するように変更することができます。



## Debug Level

Debug Level エンタープライズ パラメータは、MLA デバッグ ログのデバッグ レベル設定値 (None、Trace、または Debug) を指定します。このパラメータを *None* に設定するとデバッグがオフになり、*Trace* に設定するとトレース情報が生成され、*Debug* に設定するとデバッグ情報が生成されます。

Debug Level エンタープライズ パラメータのデフォルト値は Trace です。デバッグ ログ ファイルは、ディレクトリ c:\Program Files\Cisco\Trace\MLA に、ファイル名 DirAndUI\*\*.log で保管されます。

## Effective Access Privileges For Overlapping User Groups

Effective Access Privileges For Overlapping User Groups エンタープライズ パラメータは、複数のユーザ グループに所属し競合する特権を持つユーザのアクセス レベルを決定します。

このエンタープライズ パラメータは次の値に設定することができます。

- **Maximum** : 有効な特権は、重複するすべてのユーザ グループで最大限の特権になる。
- **Minimum** : 有効な特権は、重複するすべてのユーザ グループで最小限の特権になる。

Effective Access Privileges For Overlapping User Groups エンタープライズ パラメータのデフォルト値は Maximum です。

## Effective Access Privileges For Overlapping Functional Groups

Effective Access Privileges For Overlapping Functional Groups エンタープライズ パラメータは、複数の機能グループに所属し競合する特権を持つ Cisco CallManager ウィンドウに対するユーザ アクセス レベルを決定します。

このエンタープライズ パラメータは次の値に設定することができます。

- **Maximum** : 有効な特権は、重複するすべての機能グループで最大限の特権になる。
- **Minimum** : 有効な特権は、重複するすべての機能グループで最小限の特権になる。

Effective Access Privileges For Overlapping Functional Groups エンタープライズ パラメータのデフォルト値は Maximum です。

### Enable MultiLevelAdmin

Enable MultiLevelAdmin エンタープライズ パラメータは MLA を使用可能にするかどうかを指定します。

このエンタープライズ パラメータは次の値に設定することができます。

- True : MLA は使用可能
- False : MLA は使用不可

Enable MultiLevelAdmin エンタープライズ パラメータのデフォルト値は False です。

True を選択した場合は、プロンプト「New password for CCMAdministrator」で新しいパスワードを入力し、プロンプト「Confirm password for CCMAdministrator」でそのパスワードを再入力します。

Enable MultiLevelAdmin エンタープライズ パラメータ値を変更した場合、CCMAdministrator は次の手順を実行して変更した値を有効にする必要があります。

1. **Start > Programs > Administrative Tools > Services** の順に選択します。
2. **Worldwide Web Publishing service** を選択して右クリックします。
3. **Stop** を選択してから、**Start** を選択します。

### User Cache Flush Timeout (Minutes)

User Cache Flush Timeout エンタープライズ パラメータは、ユーザの資格情報を含む MLA キャッシュをフラッシュする間隔 (分単位) を指定します。MLA は、キャッシュをフラッシュするたびに、統合エンタープライズ ディレクトリ サーバからの最新のユーザ資格情報と MLA 自身を同期化します。

このパラメータの値を大きくするほど、最後のフラッシュ以降にユーザの資格情報 (エンタープライズ ディレクトリ内) が変更され、キャッシュされた値と一致なくなっている可能性が高くなります。つまり、ユーザはキャッシュされた資格情報に基づいて認証されますが、実際には、値が不一致のために認証が拒否されることがあります。

このパラメータの値を小さくすると、Real Time Monitoring Tool (RTMT) などの外部ポーリング アプリケーションのパフォーマンスが低下する可能性が高くなります。

このパラメータの適切な値は、ポーリング アプリケーションの許容可能なパフォーマンス レベルを維持しながら、セキュリティ リスクを最小限に抑えることのできる値です。

このエンタープライズ パラメータは次の値に設定することができます。

- No Caching (キャッシュしない)
- 5
- 10
- 20
- 30
- 45
- 60

User Cache Flush Timeout エンタープライズ パラメータのデフォルト値は、5 分間です。

## 標準ユーザ グループおよび標準機能グループ

ここでは、Cisco CallManager MLA を有効にすると使用できるようになる、標準ユーザ グループと標準機能グループの完全なリストを提供します。この項の構成は、次のとおりです。

- [標準機能グループ \(P.4-12\)](#)
- [標準ユーザ グループ \(P.4-12\)](#)
- [標準ユーザ グループおよび標準機能グループの特権マッピング \(P.4-13\)](#)

### 標準機能グループ

Cisco CallManager MLA によって標準機能グループが作成されます。標準機能グループは、次の機能グループで構成されます。

- 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

### 標準ユーザ グループ

Cisco CallManager MLA によってインストール時に標準ユーザ グループが作成されます。標準ユーザ グループは、次のユーザ グループで構成されます。

- SuperUserGroup
- ReadOnly

- PhoneAdministration
- GatewayAdministration
- ServerMonitoring
- ServerMaintenance

## 標準ユーザグループおよび標準機能グループの特権マッピング

表 4-1 は、標準ユーザグループと標準機能グループの特権を対象としたデフォルトのマッピングを示しています。

表 4-1 標準ユーザグループと標準機能グループのマッピング

ユーザグループ	機能グループ	アクセス権
GatewayAdministration	Standard Feature	Read Only
	Standard Gateway	Full Access
	Standard Phone	Read Only
	Standard Plugin	Read 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

## ■ 標準ユーザグループおよび標準機能グループ

表 4-1 標準ユーザグループと標準機能グループのマッピング (続き)

ユーザグループ	機能グループ	アクセス権
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
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

表 4-1 標準ユーザグループと標準機能グループのマッピング (続き)

ユーザグループ	機能グループ	アクセス権
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
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

表 4-1 標準ユーザグループと標準機能グループのマッピング (続き)

ユーザグループ	機能グループ	アクセス権
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

## 参考情報

### 関連項目

- 『Cisco CallManager アドミニストレーションガイド』の「Multilevel Administration Access の設定」

### 参考資料

- Cisco CallManager インストレーションガイド*
- Cisco CallManager アドミニストレーションガイド*
- Cisco CallManager Serviceability システムガイド*
- Cisco CallManager Serviceability アドミニストレーションガイド*