ユーザ アクセスの管理

ユーザ アクセスの概要

次の項目を設定して、Cisco Unified Communications Manager に対するユーザ アクセスを管理します。

- [アクセス制御グループ（Access Control Groups）]
- [ロール（Roles）]
- [ユーザ ランク（User Rank）]

アクセス制御グループの概要

アクセス制御グループは、ユーザのリストと、それらのユーザに割り当てられているロールのリストです。エンド ユーザ、アプリケーション ユーザ、または管理者ユーザをアクセス制御グループに割り当てると、そのユーザは、そのグループに関連付けられているロールのアクセス権限を取得します。類似するアクセス権限を持つユーザを、必要なロールとアクセス許可のみを含むアクセス制御グループに割り当てることによって、システム アクセスを管理できます。

アクセス制御グループには、次の 2 つのタイプがあります。

- 標準アクセス制御グループ：これらは定義済みのデフォルト グループであり、一般的な導入ニーズを満たすロールが割り当てられています。標準グループ内のロール割り当てを編集することはできません。ただし、ユーザの追加または削除、ユーザのランク要件の編集

は可能です。標準アクセス制御グループのリストと、それらに関連付けられているロールについては、「標準ロールとアクセス制御グループ（18ページ）」を参照してください。

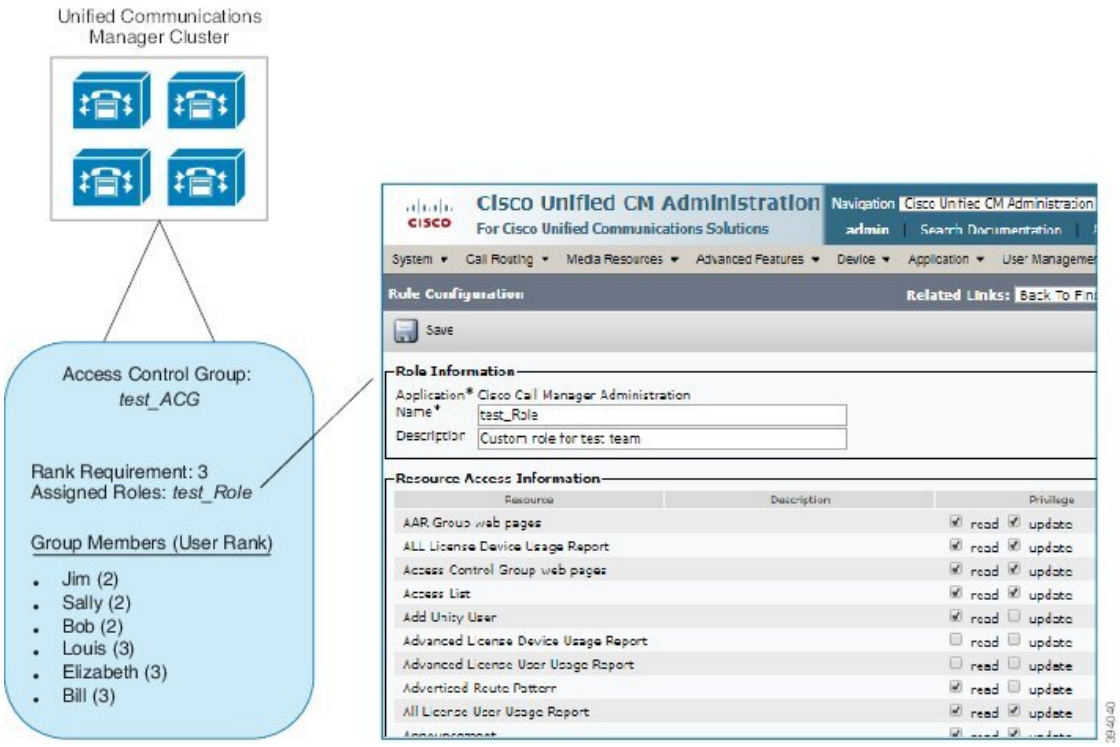
- カスタムアクセス制御グループ：必要条件を満たすロールの権限が標準のグループに含まれていない場合は、独自のアクセス制御グループを作成します。

ユーザランクのフレームワークによって、ユーザの割り当てが可能なアクセス制御グループに対する一連の制御が提供されます。アクセス制御グループにユーザを割り当てるためには、そのグループの最小ランク要件をユーザが満たしている必要があります。たとえば、ユーザランクが 4 であるエンドユーザは、最小ランク要件が 4 ～ 10 であるアクセス制御グループにのみ割り当てることができます。最小ランクが 1 のグループには割り当てることができません。

例：アクセス制御グループを使用したロールの権限

次の例は、テストチームのメンバーがアクセス制御グループ **test_ACG** に割り当てられているクラスタを示しています。右側のスクリーンキャプチャには、このアクセス制御グループに関連付けられているロールである test_Role のアクセス設定が表示されています。このアクセス制御グループの最小ランク要件は3であることにも注目してください。このグループに参加するためには、すべてのグループ メンバーのランクが 1 ～ 3 でなければなりません。

図 *1:* アクセス制御グループを使用したロールの権限



ロールの概要

ユーザは、そのユーザがメンバーとなっているアクセス制御グループに関連付けられたロールを介して、システム アクセス権限を取得します。各ロールには、Cisco Unified CM Administration または CDR Analysis and Reporting などの特定のリソースまたはアプリケーションに割り当てられた一連の権限が含まれています。Cisco Unified CM Administration などのアプリケーションの場合、ロールには、アプリケーション内の特定の GUI ページを表示または編集できるアクセス許可が含まれている場合があります。リソースまたはアプリケーションに割り当てることができるアクセス許可には、次の 3 つのレベルがあります。

- [読み取り（Read）]：ユーザがリソースの設定を表示することを許可します。
- [更新（Update）]：ユーザはリソースの設定を編集できます。
- [アクセスなし（No Access）]：ユーザが読み取りと更新のどちらのアクセス権も持っていない場合、そのユーザは、特定のリソースの設定を表示も編集もできません。

ロール タイプ

ユーザをプロビジョニングする場合は、適用するロールを決定してから、そのロールを含むアクセス制御グループにユーザを割り当てる必要があります。Cisco Unified Communications Manager には、主に 2 つのロール タイプがあります。

- 標準ロール：一般的な展開のニーズを満たすように設計された、プレインストールされたデフォルトのロールです。標準ロールの権限を編集することはできません。
- カスタム ロール：必要な権限を持つ標準ロールがない場合に、カスタム ロールを作成します。さらに細かいレベルのアクセス制御が必要な場合は、高度な設定を適用して、管理者がキーのユーザ設定を編集できるように制御することができます。詳細については、該当する項を参照してください。

高度なロール設定

カスタマイズされたロールを作成する際に、**[アプリケーション ユーザ（Application User）]** と **[エンド ユーザ（End User）]** 設定ウィンドウで選択されたフィールドに、詳細レベルの制御を追加できます。

[高度なロール設定（Advanced Role Configuration）] ウィンドウでは、Cisco Unified CM Administration へのアクセスを設定する一方で、次のようなタスクの使用を制限できます。

- ユーザの追加
- パスワードを編集
- ユーザランクの編集
- アクセス制御グループの編集

次の表に、この構成で適用できるその他のコントロールを詳しく示します。

表 *1:* 高度なリソースアクセス情報

高度なリソース	アクセス コントロール
権限情報	アクセス制御グループを追加または編集する機能を制御します： • [表示（View）]：ユーザは、アクセス制御グループを表示することはできますが、追加、編集、または削除することはできません。 • [更新（Update）]：ユーザは、アクセス制御グループを追加、編集、または削除できます。 （注） 両方の値が選択されていないと、[権限情報（Permission Information）] セクションは使用できません。 （注） **表示 (View)**を選択すると、**ユーザが[ユーザ (user)]フィールドの権限情報を更新できるように いいえ (No)**に設定され、無効になります。このフィールドを編集できるようにする場合は、**アクセス許可情報**フィールドを**更新**するように設定する必要があります。
ユーザは自分のユーザの権限情報を更新できる	ユーザが自分のアクセス権を編集できるかどうかを制御します。 • **はい (Yes)**: ユーザは自分のアクセス権情報を更新できます。 • **いいえ (No)**: ユーザは自分のアクセス権情報を更新できません。ただし、ユーザは同じユーザまたは下位レベルのユーザのアクセス権情報を表示または変更できます。 （注） **[ユーザは自分のユーザの権限情報を更新できる（User can update Permissions Information for own user）]**フィールドが**いいえ (No)**に設定され、**権限情報(Permission information)**の**更新 (Update)** チェックボックスがオフになっている場合は無効になります。
ユーザランク	ユーザランクを変更する機能を制御します。 • [表示（View）]：ユーザは、ユーザ ランクを表示できますが、変更することはできません。 • [更新（Update）]：ユーザは、ユーザ ランクを変更できます。 （注） 両方の値が選択されていないと、[ユーザランク（User Rank）] セクションは使用できません。 （注） **表示 (View)**を選択すると、**ユーザが[ユーザ (user)フィールドのユーザランクを更新できるように いいえ (No)**に設定され、無効になります。このフィールドを編集できるようにする場合は、**ユーザランク**フィールドを**更新**するように設定する必要があります。

高度なリソース	アクセス コントロール
ユーザは自分のユーザのランクを更新できる	ユーザが自分のユーザランクを編集できるかどうかを制御します。 • **はい**: ユーザは自分のユーザランクを更新できます。 • **いいえ** : ユーザは自分のユーザランクを更新できません。ただし、ユーザは同じユーザまたは下位レベルのユーザのランクを表示または変更できます。 （注） **[ユーザは自分のユーザのランクを更新できる（User can update User Rank for own user）]** フィールドが**いいえ (No)** に設定され、**ユーザランク**の**更新 (Update)** チェックボックスがオフになっている場合は無効になります。
新規ユーザの追加	新しいユーザを追加する機能を制御します。 • [はい（Yes）] : ユーザは、新しいユーザを追加できます。 • [いいえ（No）] : [新規追加（Add New）] ボタンを使用できません。
パスワード	パスワードを変更する機能を制御します。 • **はい** - ユーザーは**アプリケーションユーザー情報**セクションでユーザーパスワードを変更できます。 • **いいえ** - **「アプリケーションユーザー情報」**セクションの**「パスワード」**および**「パスワードの確認入力」**は使用できません。

ユーザ ランクの概要

ユーザ ランクのアクセス制御では、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。

エンド ユーザやアプリケーション ユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。管理者は、各アクセス制御グループにもユーザ ランクを割り当てる必要があります。Conttrol グループにアクセスするユーザを追加する場合、管理者は、ユーザのユーザのランク要件がグループのランク要件を満たしているグループにのみユーザを割り当てることができます。たとえば、あるエンド ユーザのユーザ ランクが 3 の場合、3 ～ 10 のユーザ ランクが設定されているアクセス制御グループに割り当てることができます。ただし、管理者は、そのユーザを 1 または 2 のユーザランク要件を持つアクセス制御グループに割り当てることはできません。

管理者は、[ユーザ順位の**設定**] ウィンドウ内に独自のユーザランク階層を作成し、ユーザをプロビジョニングし、アクセス制御グループを使用して、その階層を使用することができます。ユーザランクの階層を設定しない場合や、ユーザをプロビジョニングするとき、または conrol グループにアクセスするときにユーザランクの設定を指定しない場合は、すべてのユーザとア

クセス制御グループにはデフォルトのユーザランク 1 (可能な限り高いランク) が割り当てられます。

ユーザ アクセスの前提条件

ユーザに必要なアクセス レベルを判断できるよう、ユーザのニーズを確認してください。ユーザが必要とするアクセス権限を与える一方で、ユーザがアクセスすべきではないシステムへのアクセス権を付与しないよう、ロールを割り当てる必要があります。

新しいロールとアクセス コントロール グループを作成する前に、標準のロールとアクセス コントロール グループの一覧を確認して、既存のアクセス コントロール グループに必要なロールとアクセス権限があるかどうかを確認します。詳細については、標準ロールとアクセス制御グループ （18 ページ） を参照してください。

ユーザ アクセスの設定タスク フロー

以下のタスクを実行して、ユーザ アクセスを設定します。

始める前に

デフォルトのロールとアクセス制御グループを使用する場合は、カスタマイズされた役割を作成するタスクをスキップし、制御グループにアクセスできます。ユーザーを既存のデフォルトのアクセス制御グループに割り当てる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ ランク階層の設定 （7 ページ）	ユーザ ランク階層を設定します。このタスクをスキップすると、すべてのユーザとアクセス コントロール グループには、デフォルトのユーザ ランク 1（最高ランク）が割り当てられます。
ステップ 2	カスタム ロールの作成 （7 ページ）	必要なアクセス権限がデフォルト ロールに割り当てられていない場合は、カスタムロールを作成します。
ステップ 3	管理者の高度なロール設定 （9 ページ）	これはオプションです。カスタムロールの高度な権限を使用すると、主な設定に対する管理者の編集権限を制御することができます。
ステップ 4	アクセス制御グループの作成 （9 ページ）	デフォルトのグループに必要なロールが割り当てられていない場合は、カスタム

	コマンドまたはアクション	目的
		アクセス コントロール グループを作成します。
ステップ 5	アクセス制御グループへのユーザの割り当て （10 ページ）	標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。
ステップ 6	アクセス制御グループの重複する特権ポリシーの設定 （11 ページ）	これはオプションです。この設定は、権限が競合する複数のアクセスコントロール グループにユーザが割り当てられている場合に使用します。

ユーザ ランク階層の設定

カスタムのユーザ ランク階層を作成するには、この手順を使用します。

（注） ユーザ ランク階層を設定しない場合は、すべてのユーザおよびアクセス制御グループにデフォルトで 1（最高ランク）が割り当てられます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザランク（User Rank）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ユーザランク（User Rank）] ドロップダウン メニューから、1 ～ 10 のランク設定を選択します。最も高いランクは 1 です。

ステップ 4 [ランク名（Rank Name）] と [説明（Description）] を入力します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 ユーザ ランクをさらに追加するには、この手順を繰り返します。
ユーザおよびアクセス制御グループにユーザ ランクを割り当てることで、ユーザをどのグループに割り当てることができるかを制御できます。

カスタム ロールの作成

カスタマイズされた権限で新しいロールを作成するには、この手順を使用します。必要な権限を備えた標準のロールがない場合に、この方法を使用できます。ロールを作成する方法は2つあります。

- 新規のロールを白紙の状態から作成して設定するには、[新規追加（Add New）] ボタンを使用します。
- 必要なアクセス権限に近いアクセス権限が既存のロールにある場合は、[コピー（Copy）] ボタンを使用します。既存のロールの権限を、編集可能な新しいロールにコピーできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）]** をクリックします。

ステップ 2 次のいずれかを実行します。

- 新しいロールを作成するには、**[新規追加（Add New）]** をクリックします。このロールを関連付ける [アプリケーション（Application）] を選択し、[次へ (Next)] をクリックします。
- 既存のロールから設定をコピーするには、[検索（Find）] をクリックして、既存のロールを開きます。[コピー（Copy）] をクリックし、新しいロールの名前を入力します。[OK] をクリックします。

ステップ 3 このロールの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 リソースごとに、該当するチェックボックスをオンにします。

- ユーザがリソースの設定を表示できるようにする場合には、[読み取り（Read）]チェックボックスをオンにします。
- ユーザがリソースの設定を編集できるようにする場合は、[更新（Update）] チェックボックスをオンにします。
- リソースに対するアクセスを提供しない場合は、両方のチェックボックスをオフにします。

ステップ 5 この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与（Grant access to all）] ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない（Deny access to all）] をクリックします。

（注） リソースのリストが複数のページにわたって表示される場合、このボタンは、現在のページに表示されるリソースに限り適用されます。他のページのリストにあるリソースのアクセス権を変更するには、それらのページを表示し、表示されたページでこのボタンを使用する必要があります。

ステップ 6 **[保存（Save）]** をクリックします。

管理者の高度なロール設定

[高度なロール設定（Advanced Role Configuration）] を使用すると、カスタム ロールの権限をより細かいレベルで編集できます。[**エンドユーザの設定（End User Configuration**）] ウィンドウおよび [**アプリケーションユーザの設定（Application User Configuration**）] ウィンドウで、次の主な設定に対する管理者の編集権限を制御することができます。

- ユーザ ランクの編集
- アクセス コントロール グループの割り当ての編集
- 新規ユーザの追加
- ユーザ パスワードの編集

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ロール（Role）]**を選択します。

ステップ 2 [**検索（Find**）] をクリックしてカスタムロールを選択します。

ステップ 3 [**関連リンク（Related Links**）] で、[**詳細なロール設定（Advanced Role Configuration**）] を選択し、[**Go（移動**）] をクリックします。

ステップ 4 [**リソース（Resource**）**Web ページ**] で、[**アプリケーション ユーザ（Application User**）**Web ページ**] または [**ユーザ（User**）**Web ページ**] を選択します。

ステップ 5 設定の編集フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 6 **[保存（Save）]** をクリックします。

アクセス制御グループの作成

新しいアクセス制御グループを作成する必要がある場合に、この手順を使用します。必要なロールとアクセス権限を持つ標準のグループがない場合に、この方法を使用できます。カスタマイズされたグループを作成する方法には、次の 2 つがあります。

- **[新規追加（Add New）]** ボタンを使用して、scatch から新しいアクセス制御グループを作成および設定します。
- 必要な内容に近いロールが既存のグループ割り当てられてい場合は、[コピー（Copy）] ボタンを使用します。既存のグループから、新しい編集可能なグループに設定をコピーできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス制御グループ（Access Control Group）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいグループを最初から作成するには、**[新規追加（Add New）]** をクリックします。
- 既存のグループから設定をコピーするには、**[検索（Find）]**をクリックして、既存のアクセス制御グループを開きます。[コピー（Copyt）] をクリックして、新しいグループの名前を入力します。[OK] をクリックします。

ステップ 3 アクセス制御グループの**名前**を入力します。

ステップ 4 **[ユーザで利用できるユーザランク（Available for Users with User Rank as）]** ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。デフォルトのユーザランクは 1 です。

ステップ 5 **[保存]** をクリックします。

ステップ 6 アクセス制御グループにロールを割り当てます。選択したロールは、グループのメンバーに割り当てられます。

a) **[関連リンク（Related Links）]** から、**[アクセス制御グループへの権限の割り当て（Assign Roles to Access Control Group）]** を選択して **[実行（Go）]** をクリックします。
b) **[検索（Find）]** をクリックして、既存のロールを検索します。
c) 追加するロールをオンにして、**[選択の追加 (add Selected)]** をクリックします。
d) **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのユーザの割り当て （10 ページ）

アクセス制御グループへのユーザの割り当て

標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。.

（注） ユーザのランクがアクセス制御グループの最低ユーザ ランクと同じかそれより上のユーザのみを追加できます。

（注） 会社のLDAPディレクトリから新しいユーザを同期する場合に、適切な権限を持つランク階層とアクセス制御グループが作成される場合、LDAP同期の一部としてグループを同期ユーザに割り当てる場合があります。LDAP ディレクトリ同期の設定方法については、『*Cisco Unified Communications Manager* システム構成ガイド』を参照してください。

手順

ステップ 1 **[ユーザ管理(User Management)]** > **[ユーザ設定(User Settings)]** > **[アクセスコントロールグループ(Access Control Group)]** を選択します。

[アクセスコントロールグループの検索/一覧表示(Find and List Access Control Group)] ウィンドウが表示されます。

ステップ 2 [検索（Find）] をクリックして、ユーザ リストを更新するアクセス制御グループを選択します。

ステップ 3 **[ユーザで利用できるユーザランク（Available for Users with User Rank as）]** ドロップダウンから、このグループに割り当てるために必要なユーザのランク要件を選択します。

ステップ 4 **[ユーザ]**セクションで、**[検索（Find）]** をクリックして、ユーザリストを表示します。

ステップ 5 エンド ユーザまたはアプリケーション ユーザをアクセス制御グループに追加するには、次の手順を実行します。

a) [エンド ユーザをアクセス制御グループに追加（Add End Users to Access Control Group）] または [アプリケーション ユーザをアクセス制御グループに追加（Add App Users to Access Control Group）] をクリックします。
b) 追加するユーザを選択します。
c) [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 アクセス制御グループからユーザを削除するには、次の手順を実行します。

a) 削除するユーザを選択します。
b) [選択項目の削除（Delete Selected] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

アクセス制御グループの重複する特権ポリシーの設定

Cisco Unified Communications Manager がアクセス制御グループの割り当てにより発生する可能性がある、ユーザ権限の重複を処理する方法を設定します。これにより、エンドユーザが複数のアクセス制御グループに割り当てられ、ロールや権限の設定に不整合が生まれる状況に対処できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 [ユーザ管理パラメータ（User Management Parameters）] で、[重複したユーザ グループとロールの実質的なアクセス権（Effective Access Privileges For Overlapping User Groups and Roles）] に次のいずれかの値を設定します。

- [最大（Maximum）]—実質的な権限は、重複したすべてのアクセス制御グループの最大限の権限になります。これがデフォルトのオプションです。
- [最小（Minimum）]—実質的な権限は、重複したすべてのアクセス制御グループの最小限の権限になります。

ステップ 3 **[保存（Save）]** をクリックします。

ユーザ権限レポートの表示

既存のエンドユーザや既存のアプリケーションユーザのユーザ権限レポートを表示するには、次の手順を実行します。ユーザ権限レポートは、エンド ユーザまたはアプリケーション ユーザに割り当てられたアクセス コントロール グループ、ロール、およびアクセス権限が表示されます。

手順

ステップ 1 Cisco Unified CM の管理で、次の手順のいずれかを実行します。

- エンド ユーザの場合は、**[ユーザの管理（User Management）] > [エンド ユーザ（End User）]**を選択します。
- アプリケーション ユーザの場合は、**[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]**を選択します。

ステップ 2 [検索（Find）] をクリックして、アクセス権限を表示するユーザを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リストから [ユーザ権限レポート（User Privilege Report）] を選択し、[移動（Go）] をクリックします。
[ユーザ権限（User Privilege）] ウィンドウが表示されます。

カスタム ヘルプ デスク ロールの作成タスク フロー

企業によっては、ヘルプデスク担当者に特定の管理タスクを実行できる権限を与える必要があると考えている場合があります。このタスク フロー内の手順に従って、電話機の追加やエンドユーザの追加などのタスクをヘルプ デスク チームのメンバーが実行できるようにする、ヘルプ デスク チームのメンバー用のロールとアクセス コントロール グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	カスタム ヘルプ デスク ロールの作成（13 ページ）	ヘルプ デスク チームのメンバーのカスタム ロールを作成し、新しい電話機の

	コマンドまたはアクション	目的
		追加や新しいユーザの追加などの項目のロール権限を割り当てます。
ステップ 2	カスタム ヘルプ デスク アクセス コントロール グループの作成 （14 ページ）	ヘルプ デスク ロール用の新しいアクセス コントロール グループを作成します。
ステップ 3	アクセス制御グループへのヘルプ デスク ロールの割り当て （14 ページ）	ヘルプ デスク アクセス コントロール グループにヘルプ デスク ロールを割り当てます。このアクセス コントロール グループに割り当てられたユーザには、ヘルプ デスク ロールの権限が割り当てられます。
ステップ 4	アクセス制御グループへのヘルプ デスク メンバーの割り当て （15 ページ）	カスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

カスタム ヘルプ デスク ロールの作成

この手順を実行して、組織内のヘルプ デスク メンバーに割り当てることができるカスタム ヘルプ デスク権限を作成します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[権限（Role）]** をクリックします。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [アプリケーション（Application）] ドロップダウン リストから、この権限に割り当てるアプリケーションを選択します。たとえば、[Cisco CallManager Administration] を選択します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 新しいロールの [名前（Name）] を入力します。たとえば、**`Help Desk`** です。

ステップ 6 [読み込みおよび更新権限（Read and Update Privileges）] の下で、ヘルプ デスク ユーザに割り当てる権限を選択します。たとえば、ヘルプ デスク メンバーがユーザおよび電話を追加できるようにする場合は、[ユーザ（User）] Web ページと [電話（Phone）] Web ページの [読み込み（Read）] および [更新（Update）] チェック ボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

カスタム ヘルプ デスク アクセス コントロール グループの作成 （14 ページ）

カスタム ヘルプ デスク アクセス コントロール グループの作成

始める前に

カスタム ヘルプ デスク ロールの作成 （13 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]**>**[ユーザ設定（User Settings）]**>**[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 アクセス制御グループの名前を入力します。たとえば、「**Help_Desk**」と入力します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのヘルプ デスク ロールの割り当て （14 ページ）

アクセス制御グループへのヘルプ デスク ロールの割り当て

次の手順を実行して、ヘルプ デスク ロールからの権限を持つヘルプ デスク アクセス コントロール グループを設定します。

始める前に

カスタム ヘルプ デスク アクセス コントロール グループの作成 （14 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]**>**[ユーザ設定（User Settings）]**>**[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、ヘルプ デスク用に作成したアクセス コントロール グループを選択します。
[アクセス コントロール グループの設定（Access Control Group Configuration）] ウィンドウが開きます。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[アクセス コントロール グループに権限を割り当て（Assign Role to Access Control Group）] オプションを選択し、[移動（Go）] をクリックします。
[ロールの検索/一覧表示（Find and List Roles）] ポップアップが表示されます。

ステップ 4 [グループに権限を割り当て（Assign Role to Group）] ボタンをクリックします。

ステップ 5 [検索（Find）] をクリックし、ヘルプ デスク ロールを選択します。

ステップ 6 [選択項目の追加（Add Selected）] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのヘルプ デスク メンバーの割り当て （15 ページ）

アクセス制御グループへのヘルプ デスク メンバーの割り当て

始める前に

アクセス制御グループへのヘルプ デスク ロールの割り当て （14 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]**>**[ユーザ設定（User Settings）]**>**[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、作成したカスタム ヘルプ デスク アクセス コントロール グループを選択します。

ステップ 3 次のいずれかの手順を実行します。

- ヘルプ デスク チームのメンバーがエンド ユーザとして設定されている場合は、[グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。
- ヘルプ デスク チームのメンバーがアプリケーション ユーザとして設定されている場合は、[グループにアプリケーション ユーザを追加（Add App Users to Group）] をクリックします。

ステップ 4 [検索（Find）] をクリックし、ヘルプ デスク ユーザを選択します。

ステップ 5 [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。
Cisco Unified Communications Manager が、作成したカスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

アクセス制御グループの削除

アクセス コントロール グループ全体を削除するには、次の手順を使用します。

始める前に

アクセス コントロール グループを削除すると、Cisco Unified Communications Manager がデータベースからすべてのアクセス コントロール グループ データを削除します。アクセス コントロール グループを使用しているロールが判明していることを確認します。

手順

ステップ 1 **[ユーザ管理(User Management)]** > **[ユーザ設定(User Settings)]** > **[アクセスコントロールグループ(Access Control Group)]** を選択します。

[アクセス制御グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウが表示されます。

ステップ 2 削除するアクセス コントロール グループを検索します。

ステップ 3 削除するアクセス ポイント グループの名前をクリックします。

選択したアクセス コントロール グループが表示されます。このアクセス コントロール グループ内のユーザがアルファベット順に一覧表示されます。

ステップ 4 アクセス コントロール グループ全体を削除するには、[削除（Delete）] をクリックします。

アクセス コントロール グループを削除すると元に戻せないことを警告するダイアログボックスが表示されます。

ステップ 5 アクセス コントロール グループを削除するには、[OK] をクリックします。アクションをキャンセルするには、[キャンセル（Cancel）] をクリックします。[OK] をクリックすると、Cisco Unified Communications Manager がデータベースからアクセス コントロール グループを削除します。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセス トークンを取得したり、企業アカウントへログインできないようにすることができます。API は、AXL クレデンシャルで保護されている REST ベースの API です。任意のコマンドライン ツールを使用して API を呼び出すことができます。次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

引数の説明

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。

• end_user は、更新トークンを取り消すユーザのユーザ ID です。

非アクティブなユーザ アカウントの無効化

Cisco Database Layer Monitor サービスを使用して非アクティブなユーザ アカウントを無効にするには、次の手順を実行します。

Cisco Database Layer Monitor は、指定日数内に Cisco Unified Communications Manager にログインしていない場合、スケジュールされたメンテナンス タスク時にユーザ アカウント ステータスを非アクティブに変更します。無効にされたユーザは、その後の監査ログで自動的に監査対象になります。

始める前に

Cisco Database Layer Monitor サービスで選択したサーバの **[メンテナンス時間（Maintenance Time）]**を入力します（**[システム]** > **[サービス パラメータ]**）。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム]** > **[サービス パラメータ]** の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスからサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリスト ボックスから [Cisco Database Layer Monitor] パラメータを選択します。

ステップ 4 [詳細設定（Advanced）] をクリックします。

ステップ 5 [この期間未使用のユーザ アカウントを無効化する（Disable User Accounts unused for（days））] フィールドに、日数を入力します。たとえば、90とします。システムはこの入力された値を、非アクティブとしてアカウントの状態を宣言するためのしきい値として使用します。自動無効化をオフにするには、値を 0 と入力します。

（注） 必須フィールドです。デフォルトおよび最小値は 0 で、単位は日数です。

ステップ 6 **[保存]** をクリックします。
非アクティブなまま設定された日数（たとえば 90 日間）が経過すると、ユーザは無効になります。監査ログにエントリが作成され、次のメッセージが表示されます。「<userID>ユーザは非アクティブとマークされています（<userID> user is marked inactive）」。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、**[サービス（Services）] > [リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）] フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）] フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

標準ロールとアクセス制御グループ

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている標準権限およびアクセス制御グループの概要です。標準権限が持つ特権はデフォルトで設定されています。また、標準権限に関連付けられたアクセス制御グループも、デフォルトで設定されています。

標準権限、および標準権限に関連付けられたアクセス制御グループの両方で、特権または権限の割り当てを編集できません。

表 *2:* 標準権限、特権 およびアクセス制御グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 AXL API アクセス	AXL データベース API へのアクセスを許可します。	標準 CCMスーパーユーザ
標準 AXL APIユーザ	AXL API を実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	
標準管理 Rep Tool 管理	Cisco Unified Communications Manager CDR Analysis and Reporting（CAR）の表示および設定が可能になります。	標準 CAR 管理ユーザ、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準監査ログ管理	監査ロギング機能の次のタスクを実行できます。 • Cisco Unified Serviceability の [監査ログ設定（Audit Log Configuration）] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability での Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新	標準監査ユーザ
標準 CCM 管理ユーザ	Cisco Unified Communications Manager Administration へのログイン権限を付与します。	標準 CCM 管理ユーザ、標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ モニタリング、標準 CCM スーパー ユーザ、標準 CCM サーバ メンテナンス、標準 パケット スニファ ユーザ
標準CCMエンドユーザ	Cisco Unified Communications セルフケアポータルにログインする権限をエンド ユーザに付与します。	標準CCMエンドユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 機能管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる次の項目の表示、削除、挿入：
	  • クライアント関連のコードと強制承認コード
	  • コール ピックアップ グループ
	• Cisco Unified Communications Manager Administration で、の次の項目を表示、設定できます。
	  • クライアント関連のコードと強制承認コード
	  • コール パーク
	  • コール ピックアップ
	  • ミートミーの番号またはパターン
	  • メッセージ受信
	  • Cisco Unified IP Phone サービス
	  • ボイスメールパイロット、ボイスメール ポート ウィザード、ボイスメールポート、ボイスメール プロファイル
		標準CCMサーバメンテナンス

標準 CCM ゲートウェイ管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • 一括管理ツールによるゲートウェイテンプレートの表示および設定 • ゲートキーパー、ゲートウェイ、およびトランクの表示および設定	標準 CCM ゲートウェイ管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 電話管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる電話の表示とエクスポート
	• 一括管理ツールによるユーザデバイス プロファイルの表示と挿入
	• Cisco Unified Communications Manager Administration で、次の項目を表示および設定できます。
	  • BLF 短縮ダイヤル
	  • CTI ルート ポイント
	  • デフォルトデバイスプロファイルまたはデフォルト プロファイル
	  • 電話番号、および回線の状態
	  • ファームウェア ロード情報
	  • 電話ボタンテンプレートまたはソフトキー テンプレート
	  • 電話
	  • [電話の設定（Phone Configuration）] ウィンドウの [ボタン項目を変更（Modify Button Items）] をクリックすることによる、特定の電話に対する電話ボタンの情報の並べ替え
		標準 CCM 電話管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ルート プラン計画管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • アプリケーション ダイヤル ルールの表示および設定 • コーリング サーチ スペースおよびパーティションの表示および設定 • ダイヤル ルール パターンを含むダイヤル ルールの表示および設定 • ハント リスト、ハント パイロット、回線グループの表示および設定 • ルート フィルタ、ルート グループ、ルート ハント リスト、ルートリスト、ルートパターン、ルート プラン レポートの表示および設定 • 時間帯およびスケジュールの表示および設定 • トランスレーション パターンの表示および設定	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM サービス管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 次の項目を表示および設定できます。
	  • アナンシエータ、会議ブリッジ、トランスコーダ
	  • オーディオ ソースおよび MOH サーバ
	  • メディア リソース グループおよびメディア リソース グループ リスト
	  • Media Termination Point; メディア ターミネーション ポイント
	  • Cisco Unified Communications Manager Assistant ウィザード
	• 一括管理ツールの [マネージャの削除（Delete Managers）]、[マネージャ/アシスタントの削除（Delete Managers/Assistants）] および [マネージャ/アシスタントの挿入（Insert Managers/Assistants）] ウィンドウでの表示および設定ができます。
		標準CCMサーバメンテナンス

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM システム管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 次の項目を表示および設定できます。
	  • 代替ルーティング（AAR）グループの自動化
	  • Cisco Unified Communications Manager（Cisco Unified CM）および Cisco Unified Communications Manager グループ
	  • 日時グループ
	  • デバイス デフォルト
	  • デバイス プール
	  • エンタープライズパラメータ
	  • エンタープライズ電話の設定
	  • ロケーション
	  • Network Time Protocol（NTP）サーバ
	  • プラグイン
	  • Skinny Call Control Protocol（SCCP）または Session Initiation Protocol（SIP）を実行する電話用のセキュリティプロファイル、SIP トランク用のセキュリティプロファイル
	  • Survivable Remote Site Telephony（SRST）の参照
	  • サーバ
	• 一括管理ツールの、[ジョブ スケジューラ（Job Scheduler）] ウィンドウでの表示と設定
		標準 CCMサーバメンテナンス

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ユーザ権限管理	Cisco Unified Communications Manager Administration で、アプリケーションユーザの表示および設定を実行できます。	
標準 CCMADMIN 管理	CCMAdmin システムのすべての面を利用できます。	
標準 CCMADMIN 管理	Cisco Unified Communications Manager Administration および一括管理ツールのすべての項目を表示および設定できます。	標準 CCM スーパーユーザ
標準 CCMADMIN 管理	Dialed Number Analyzer の情報を表示および設定できます。	
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	
標準CCMADMIN読み取り専用	Cisco Unified Communications Manager Administration および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ メンテナンス、標準 CCM サーバ モニタリング
標準 CCMADMIN 読み取り専用	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	標準CCMエンドユーザ
標準 CTI 通話モニタリング許可	CTI アプリケーションまたはデバイスでコールをモニタできます。	標準 CTI 通話モニタリング許可

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CTI コール パーク モニタリング許可	CTI アプリケーションまたはデバイスでコール パークを使用できます。 **重要** 開いている回線およびパーク回線の最大数は 65,000 を超えてはいけません。 合計が 65,000 を超える場合は、アプリケーション ユーザーから標準 CTI 許可コール パーク モニタリングのロールを削除するか、設定されているパーク回線の数を減らします。	標準 CTI コール パーク モニタリング許可
標準 CTI 通話録音許可	CTI アプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準 CTI 発信者番号の変更許可	CTI アプリケーションが発信者番号を通話中に変更できます。	標準 CTI 発信者番号の変更許可
標準 CTI によるすべてのデバイスの制御	CTI で制御可能なすべてのデバイスを制御できます。	標準 CTI によるすべてのデバイスの制御
標準 CTI 接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべての CTI デバイスを制御できます。	標準 CTI 接続された転送と会議をサポートする電話の制御許可
標準 CTI ロールオーバー モードをサポートする電話の制御許可	ロールオーバー モードをサポートするすべての CTI デバイスを制御できます。	標準 CTI ロールオーバー モードをサポートする電話の制御許可
標準 CTI SRTP 重要素材の受信許可	CTI アプリケーションが、SRTP を使用する重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
標準 CTI 対応	CTI アプリケーションの制御を可能にします。	標準 CTI 対応
標準 CTI セキュア接続	Cisco Unified Communications Manager へのセキュアな CTI 接続が可能になります。	標準 CTI セキュア接続

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CUReporting	アプリケーションユーザが、さまざまなソースからレポートを作成できます。	
標準CUReporting	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準 CCM 管理ユーザ、標準 CCM スーパー ユーザ
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility（EM）の認証権限を管理します。この権限は、（Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの）Cisco Extension Mobility と対話するすべてのアプリケーションユーザに必要です。	標準 CCM スーパー ユーザ、標準 EM 認証プロキシ権限
標準パケット スニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケット スニッフィング（キャプチャ）ができます。	標準パケット スニファ ユーザ
標準RealtimeAndTraceCollection	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 • Simple Object Access Protocol（SOAP）Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル（Analysis Manager）データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定	標準RealtimeAndTraceCollection

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 SERVICEABILITY		標準 CCM サーバ モニタリング、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
	Cisco Unified Serviceability または Real-Time Monitoring Tool で、次のウィンドウを表示および設定できます。 • [アラーム設定およびアラーム定義（Alarm Configuration and Alarm Definitions）]（Cisco Unified Serviceability） • [監査トレース（Audit Trace）]（読み取りおよび表示のみ可能なマークが付けられています） • SNMP 関連のウィンドウ（Cisco Unified Serviceability） • [トレースの設定（Trace Configuration）] および [トレース設定のトラブルシューティング（Troubleshooting of Trace Configuration）]（Cisco Unified Serviceability） ） • ログパーティションのモニタリング • [アラートの設定（Alert Configuration）]（RTMT）、[プロファイルの設定（Profile Configuration）]（RTMT）、および [トレース収集（Trace Collection）]（RTMT） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベースサービスを表示および使用できます。 SOAP コールレコード API については、RTMT Analysis Manager Call Record の権限が、このリソースを介して制御されます。 SOAP 診断ポータルデータベース サービスについては、RTMT Analysis	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
	Manager Hosting Database アクセスが、このリソースを介して制御されます。	
標準SERVICEABILITY管理	有用性の管理者は、Cisco Unified Communications Manager の管理に表示されるプラグイン ウィンドウにアクセスでき、このウィンドウからプラグインをダウンロードできます。	
標準SERVICEABILITY管理	Dialed Number Analyzer の有用性をすべての面で管理できます。	
標準SERVICEABILITY管理	Cisco Unified Serviceability および Real-Time Monitoring Tool のすべてのウィンドウを表示および設定できます（[監査トレース（Audit Trace）] では表示のみ可能です）。 すべての SOAP Serviceability AXL API を表示および使用できます。	
標準SERVICEABILITY読み取り専用	Dialed Number Analyzer のコンポーネントで使用する有用性に関するすべてのデータを表示できます。	標準 CCM 読み取り専用
標準SERVICEABILITY読み取り専用	Cisco Unified Serviceability および Real-Time Monitoring Tool で、設定を表示できます。（標準監査ログ管理の権限により表示される監査設定ウィンドウは除きます） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスをすべて表示できます。	
標準システム サービス管理	Cisco Unified Serviceability で、サービスを表示、アクティベート、開始、および停止できます。	
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセス レベル ユーザ	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CCMADMIN管理	CCMAdmin システムをすべての面で管理できます。	標準Cisco Unified CM IM およびプレゼンスの管理
標準CCMADMIN読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	標準Cisco Unified CM IM およびプレゼンスの管理
標準CUReporting	アプリケーションユーザが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM & Presenceのレポーティング