ユーザ アクセスの管理

ユーザ アクセスの概要

Cisco Unified Communications Manager に対するユーザ アクセスは、次の項目をエンド ユーザに割り当てることで管理できます。

- ロール
- アクセスコントロールグループ
- ユーザ ランク

ロール、アクセス コントロール グループ、ユーザ ランク コントロールでは、Cisco Unified Communications Manager に対する複数レベルのセキュリティを提供します。各ロールでは、Cisco Unified Communications Manager 内の特定のリソースに対する一連の権限を定義します。アクセス コントロール グループにロールを割り当て、そのアクセス コントロール グループにエンド ユーザを割り当てると、それらのエンド ユーザにそのロールで定義されているすべてのアクセス権限を付与することになります。

ユーザ ランク フレームワークはロールとアクセス コントロール グループ フレームワークをオーバーレイして、エンドユーザが使用可能なグループを決定します。エンドユーザとアプリケーション ユーザは、それぞれのユーザ ランクで許可されるアクセス コントロール グループにのみ割り当てることができます。

ロールの概要

エンドユーザをプロビジョニングする場合、ユーザにどのようなロールを割り当てるか決定する必要があります。ロールはエンドユーザ、アプリケーション ユーザ、またはアクセス コントロール グループに割り当てることができます。単独のユーザに複数のロールを割り当てることができます。

各ロールには、特定のリソースまたはアプリケーションに接続される一連の権限が含まれます。たとえば、標準 CCM エンドユーザのロールは、そのロールが割り当てられているユーザに、Cisco Unified Communications セルフ ケア ポータルへのアクセス権を提供します。

また、Cisco Unified Communications Manager の管理、Cisco CDR Analysis and Reporting、Dialed Number Analyzer、CTI インターフェイスなどのリソースへのアクセスを提供するロールを割り当てることもできます。

特定の設定ウィンドウのようなグラフィカル ユーザ インターフェイスを使用する大部分のリソースでは、ロールに接続された権限によって、そのウィンドウのデータ、または関連するウィンドウのグループ内のデータを閲覧したり更新できます。

ロールの設定と割り当て

標準ロールをユーザに割り当てるか、またはカスタム ロールを作成するかを決定する必要があります。

- 標準ロール：標準ロールとは、Cisco Unified Communications Manager に最初からインストールされている、デフォルトの事前定義のロールです。ロールの権限を編集または変更することはできません。
- カスタム ロール：カスタム ロールは自分で作成するロールです。ユーザに割り当てる権限を含む標準ロールがないときに、カスタム ロールを作成できます。たとえば、標準ロールを割り当てようとしたが、権限の 1 つを変更したい場合、標準ロールの権限をカスタム ロールにコピーし、そのカスタム ロールで権限を編集できます。

権限のタイプ

各ロールには、特定のリソースに接続される一連の権限が含まれます。リソースに割り当てられる権限には 2 種類あります。

- [読み取り（Read）]：読み取り権限では、ユーザはそのリソースの設定を閲覧できますが、設定を更新することはできません。たとえば、この権限ではユーザが特定の設定ウィンドウの設定を閲覧できますが、そのアプリケーションの設定ウィンドウには更新ボタンやアイコンは表示されません。
- [更新（Update）]：更新権限では、ユーザはそのリソースの設定を変更できます。たとえば、この権限ではユーザが特定の設定ウィンドウで更新を実行できます。

エンドユーザ ロールと管理者ロール

標準 CCM エンドユーザ（Standard CCM End Users）ロールは、Cisco Unified Communications セルフ ケア ポータルへのアクセス権をエンドユーザに提供します。CTI アクセスなどの追加権限については、標準 CTI 対応（Standard CTI Enabled）ロールなどの追加ロールを割り当てる必要があります。

標準 CCM 管理ユーザ（Standard CCM Admin Users）ロールは、すべての処理タスクのベースロールであり、認証ロールとして機能します。このロールは、Cisco Unified Communications Manager Administration のユーザ インターフェイスへの管理者アクセスを提供します。Cisco Unified CM の管理では、このロールを Cisco Unified Communications Manager Administration にログインするために必要なロールとして定義しています。

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）] ページでは、システムへのアクセスを許可する際に、以下に示すようなタスクへのアクセスを制限できます。

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

次の表では、この設定で適用できる制御について詳しく説明します。

表 *1*: 高度なリソース アクセス情報

高度なリソース	アクセス制御
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次のように制御します。 • [ビュー（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。

高度なリソース	アクセス制御
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。 • [ビュー（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。
新しいユーザの追加	新しいユーザを追加する機能を次のように制御します。 • [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）] ボタンは使用できません。
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（Yes）] : ユーザは [アプリケーション ユーザ情報（Application User Information）] セクションでユーザのパスワードを変更できます。 • [いいえ（No）] : [アプリケーション ユーザ情報（Application User Information）] セクションで、[パスワード（Password）] と [パスワードの確認（Confirm Password）] は使用できません。

関連トピック

標準権限とアクセス コントロール グループ （20 ページ）

アクセス コントロール グループの概要

ロールとともにアクセス コントロール グループを使用して、同様のアクセス要件のユーザ グループにネットワークへのアクセス権限をすばやく指定できます。

アクセス コントロール グループは、エンドユーザとアプリケーション ユーザのリストです。類似したアクセスの必要性を共有するエンド ユーザとアプリケーション ユーザに、必要な権限と役割を含むアクセス コントロール グループを指定できます。アクセス コントロール グループに割り当てられるエンドユーザやアプリケーションのユーザは、そのアクセス コントロール グループの最小ランク要件を満たす必要があります。たとえば、4 のユーザ ランクを持つユーザは、最小ランク要件が 4 ～ 10 のアクセス コントロール グループにしか割り当てることができません。

システムには、一連の事前定義された標準アクセス コントロール グループが含まれています。それぞれの標準アクセス コントロール グループには、デフォルトで割り当てられている一連のロールがあります。ユーザをそのアクセス コントロール グループに割り当てると、それらの役割もそのエンドユーザに割り当てられます。

標準アクセス コントロール グループに割り当てられたロールは編集できません。ただし、カスタマイズされたアクセス コントロール グループを作成し、選択したロールをそのカスタマイズされたアクセス コントロール グループに割り当てることができます。

関連トピック

標準権限とアクセス コントロール グループ （20 ページ）

ユーザ ランクの概要

ユーザ ランクのアクセス コントロールでは、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。[ユーザ ランク（User Rank）] パラメータは 1 ～ 10 の整数で指定し、一番高いランクは 1 です。ユーザ ランクはユーザとアクセス コントロール グループの両方に割り当てられるため、特定のアクセス コントロール グループに割り当て可能なユーザを決定するランク階層が作成されます。

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 コントロール 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。管理者は、同じランクや下のランクのアクセス コントロール 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 コントロール グループに割り当てることができます。そのユーザを、ユーザ ランクが 1 である必要があるアクセス コントロール 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 ランクの設定（User Rank Configuration）] ウィンドウ内でユーザ ランクの階層をカスタマイズして、それらのランクをエンド ユーザ、アプリケーション ユーザ、アクセス コントロール グループに割り当てることができます。

ユーザ アクセスの前提条件

新しい役割またはアクセス コントロール グループを作成する前に、システムにあらかじめインストールされている標準権限およびアクセス コントロール グループを確認して、既存のアクセス コントロール グループにユーザに必要な権限とアクセス許可が含まれているかどうかを確認します。

詳細については、標準権限とアクセス コントロール グループ （20 ページ）を参照してください。

ユーザ アクセス設定のタスク フロー

次のタスクを実行して、ユーザ アクセスを設定します。

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 ユーザ ランクの作成 （7 ページ）	カスタム ユーザ ランクを作成して、ユーザ ランク階層を設定します。
ステップ 2	次のいずれかの方法で新しいロールを作成します。 • カスタム ロールの作成 （8 ページ） • 権限のコピー （9 ページ）	新しいロールを最初から作成して設定するには、[作成（Create）] 手順を使用します。 新しいロールが標準ロールと同様の設定を持つ場合は、[コピー（Copy）] コマンドを使用します。既存の標準ロールから新しいロールに権限設定をコピーできます。続けて、新しいロールの設定を編集できます。
ステップ 3	次のいずれかの方法でアクセス コントロール グループを作成します。 • アクセス コントロール グループの作成 （10 ページ） • アクセス コントロール グループのコピー （10 ページ）	新しいアクセス コントロール グループを作成して設定するには、[作成（Create）] 手順を使用します。 新しいアクセス コントロール グループがデフォルト グループのいずれかとよく似ている場合は、[コピー（Copy）] コマンドを使用できます。既存のグループから新しいグループにロールの割り当てをコピーして、編集できます。
ステップ 4	アクセス コントロール グループへの権限の割り当て （11 ページ）	ロールを追加または削除して、アクセス コントロール グループに割り当てられたロールを更新します。
ステップ 5	アクセス コントロール グループへのユーザの割り当て （12 ページ）	ユーザを追加したり削除して、アクセス コントロール グループのユーザ リストを更新します。グループに割り当てられているすべてのユーザは、グループに割り当てられているロールに設定されている権限を継承します。
ステップ 6	ユーザ権限レポートの表示 （13 ページ）	これはオプションです。ユーザに割り当てられているアクセス権限を確認する必要がある場合は、そのユーザの権限レポートを表示します。
ステップ 7	アクセス コントロール グループの重複する特権ポリシーの設定 （14 ページ）	これはオプションです。Cisco Unified Communications Manager がアクセス コントロール 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

	コマンドまたはアクション	目的
		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 コントロール 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。
ステップ 8	カスタム ヘルプ デスク ロールの作成タスク フロー （14 ページ）	これはオプションです。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。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。
ステップ 9	アクセス コントロール グループの削除（17 ページ）	これはオプションです。システムからアクセス コントロール グループを削除する必要がある場合に、この手順を使用します。

カスタム ユーザ ランクの作成

ランク階層を目的として、カスタム ユーザ ランクを作成するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[ユーザの管理（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（Save）]** をクリックします。

カスタム ロールの作成

カスタム権限を作成し、その権限の特権を設定するには、次の手順を実行します。システムで定義された標準権限に、ユーザに割り当てようとする特権と一致する権限がない場合、カスタム権限を作成できます。

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）] > [権限（Role）]** をクリックします。

ステップ 2 [アプリケーション（Application）] ドロップダウン リストボックスから、この権限を関連付けるアプリケーションを選択します。
[権限の設定（Role Configuration）] ウィンドウが表示されます。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [名前（Name）] テキストボックスに、権限の名前を入力します。

名前は、128 文字まで入力できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。

ステップ 5 [説明（Description）] テキストボックスに、権限の説明を入力します。

説明は 128 文字以内にする必要があります。

ステップ 6 新しい権限が各リソースに対して持つ特権を次のように編集します。

- 権限がそのリソースを表示できるようにするには、[読み取り（Read）] チェックボックスをクリックします。
- 権限がそのリソースを編集できるようにするには、[更新（Update）] チェックボックスをクリックします。
- 権限がそのリソースを表示および編集できるようにするには、[読み取り（Read）] と [更新（Update）] の両方のチェックボックスをオンにします。
- 権限に、リソースへのどのようなアクセスも許可しない場合は、両方のチェックボックスをオフのままにします。

ステップ 7 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 8 [保存（Save）] をクリックします。

次のタスク

新しいアクセス コントロール グループを設定するには、次のいずれかの手順を実行します。

- アクセス コントロール グループの作成 （10 ページ）
- アクセス コントロール グループのコピー （10 ページ）

権限のコピー

新しい権限に標準権限の設定をコピーして、新しい権限を作成するには、次の手順を実行します。Cisco Unified Communications Manager では、標準権限の特権を編集できませんが、自分が作成した権限の特権は編集できます。

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）] > [権限（Role）]** をクリックします。

ステップ 2 [検索（Find）] をクリックし、コピーするリソースと特権がある権限を選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しい権限の名前を入力し、[OK] をクリックします。
[権限の設定（Role Configuration）] ウィンドウに新しい権限の設定が表示されます。新しい権限の特権は、コピーした権限の特権と同じです。

ステップ 5 新しい権限のリソースのいずれかで、次のように特権を編集します。

- [読み取り（Read）] チェックボックスをオンにして、ユーザにリソースの表示を許可します。
- [更新（Update）] チェックボックスをオンにして、ユーザにリソースの編集を許可します。
- リソースへのアクセスを制限するには、両方のチェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

ユーザに権限を割り当てるには、新しいアクセスコントロールグループを作成し、そのグループに権限を割り当てる必要があります。新しいアクセス コントロール グループを作成するには、次の手順のいずれかを実行します。

- アクセス コントロール グループの作成 （10 ページ）
- アクセス コントロール グループのコピー （10 ページ）

アクセス コントロール グループの作成

新しいアクセス コントロール グループを作成するには、この手順を実行します。

始める前に

アクセス コントロール グループを既存のグループと同様の設定にする場合は、Copy コマンドを使用して、既存のグループの設定を作成した新しいグループにコピーできます。

アクセス コントロール グループのコピー （10 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] 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 [名前（Name）] にアクセス コントロール 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（Save）]** をクリックします。

次のタスク

アクセス コントロール グループへの権限の割り当て （11 ページ）

アクセス コントロール グループのコピー

既存のアクセス コントロール グループから、編集できる新しいグループにロールの設定をコピーして、新しいアクセス コントロール グループを作成するには、次のタスクを実行します。

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）] をクリックして、設定をコピーする対象のアクセス コントロール グループを選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しいアクセス コントロール グループの名前を入力し、[OK] をクリックします。

ステップ 5 [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。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

アクセス コントロール グループに割り当てられたロールを確認し、編集する必要がある場合：

アクセス コントロール グループへの権限の割り当て （11 ページ）

アクセス コントロール グループへの権限の割り当て

アクセス コントロール グループに権限を割り当てるには、次の手順を使用します。既存のグループからアクセス コントロール グループの設定をコピーした場合、権限の削除が必要になることもあります。

管理者などのフル アクセスできるユーザは、アクセス コントロール グループへの権限の割り当てまたは削除ができます。権限を割り当てられたアクセス コントロール グループは、その権限に含まれるすべてのリソースにアクセスできます。

（注） アクセス コントロール グループに権限を割り当てるときには、そのアクセス コントロール グループに Standard Unified CM Admin Users 権限を割り当てる必要があります。この権限により、ユーザは Cisco Unified CM の管理にログインできます。

始める前に

新しいアクセス コントロール グループを作成するには、次のタスクのいずれかを実行します。

- アクセス コントロール グループのコピー （10 ページ）
- アクセス コントロール グループの作成 （10 ページ）

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）]** の順に選択します。

[アクセス コントロール 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 [検索（Find）] をクリックし、権限を割り当てるアクセス 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 リストで [アクセス コントロール グループへの権限の割り当て（Assign Role to Access Control Group）] を選択し、[移動（Go）] をクリックします。

[権限の割り当て（Role Assignment）] ペインが表示されます。

ステップ 4 アクセス コントロール グループに新しい権限を追加するには、次の手順を実行します。

a) [グループに権限を割り当て（Assign Role to Group）] をクリックします。
b) [検索（Find）] をクリックし、権限の一覧を検索します。
c) アクセス コントロール グループに追加する権限を選択します。
d) [選択項目の追加（Add Selected）] をクリックします。
新しい権限が、[権限（Role）] リスト ボックスに表示されます。

ステップ 5 割り当てた権限を、アクセス コントロール グループから削除するには、次の手順を実行します。

a) [権限（Role）] リスト ボックスで、削除する権限を強調表示します。
b) [割り当てた権限の削除（Delete Role Assignment）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

権限の割り当ては、データベースのアクセス コントロール グループに追加されます。

次のタスク

アクセス コントロール グループへのユーザの割り当て （12 ページ）

アクセス コントロール グループへのユーザの割り当て

新規ユーザを割り当てるか既存ユーザを削除することによってアクセス コントロール グループのエンド ユーザまたはアプリケーション ユーザのリストを更新するには、このタスクを実行します。

（注） ユーザのランクがアクセス コントロール 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。

始める前に

アクセス コントロール グループへの権限の割り当て （11 ページ）

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）]** の順に選択します。

[アクセス コントロール 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 [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 コントロール グループを選択します。

ステップ 3 [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 4 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 コントロール 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 コントロール 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 コントロール 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 5 アクセス コントロール 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 6 [保存（Save）] をクリックします。

次のタスク

これはオプションです。特定のエンド ユーザまたはアプリケーション ユーザのユーザ特権レポートを表示する必要がある場合は、次を参照してください。

- ユーザ権限レポートの表示 （13 ページ）

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制御グループ、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。

アクセス コントロール 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 コントロール 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 コントロール 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 の管理（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 コントロール 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 コントロール 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。

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 デスク権限の作成 （15 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。

	コマンドまたはアクション	目的
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 （16 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 コントロール グループへのヘルプ デスク ロールの割り当て （16 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 コントロール グループへのヘルプ デスク メンバーの割り当て （17 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 デスク権限の作成

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 新しい権限の [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 （16 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 デスク権限の作成 （15 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）]** の順に選択します。

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 コントロール 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 コントロール グループへのヘルプ デスク ロールの割り当て （16 ページ）

アクセス コントロール 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 （16 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。
[権限の検索/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 コントロール グループへのヘルプ デスク メンバーの割り当て （17 ページ）

アクセス コントロール 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 コントロール グループへのヘルプ デスク ロールの割り当て （16 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 コントロール 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）]** の順に選択します。

[アクセス コントロール 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 [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） これは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（Save）]** 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（Save）]** 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。

標準権限とアクセス コントロール 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 コントロール 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 コントロール 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 コントロール 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 コントロール 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 コントロール 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 コントロール 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 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 の管理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 コントロール グループ

標準 CCM 機能管理	Cisco Unified Communications Manager の管理で、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 の管理での次の項目の表示および設定
	  • 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 の管理で、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 コントロール グループ

標準 CCM 電話管理	Cisco Unified Communications Manager の管理で、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 の管理での次の項目の表示および設定
	  • 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
	  • 電話機
	  • [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 コントロール グループ
標準 CCM ルート プラン計画管理	Cisco Unified Communications Manager の管理で、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 コントロール グループ

標準 CCM サービス管理	Cisco Unified Communications Manager の管理で、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 コントロール グループ

標準 CCM システム管理	Cisco Unified Communications Manager の管理で、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 のグループ
	  • 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 コントロール グループ
標準 CCM ユーザ権限管理	Cisco Unified Communications Manager の管理で、アプリケーション ユーザの表示および設定ができます。	
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 の管理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 の管理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 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 パークをモニタできます。	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 コントロール グループ
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 を使う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 コントロール グループ
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 コントロール グループ
標準 SERVICEABILITY	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 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 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 コントロール グループ
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 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 コントロール グループ
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 およびプレゼンスのレポーティング