



ユーザ アクセスの管理

- [ユーザ アクセスの概要 \(1 ページ\)](#)
- [ユーザ アクセスの前提条件 \(6 ページ\)](#)
- [ユーザ アクセスの設定タスク フロー \(6 ページ\)](#)
- [非アクティブなユーザ アカウントの無効化 \(17 ページ\)](#)
- [リモート アカウントの設定 \(18 ページ\)](#)
- [標準ロールとアクセス制御グループ \(18 ページ\)](#)

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。

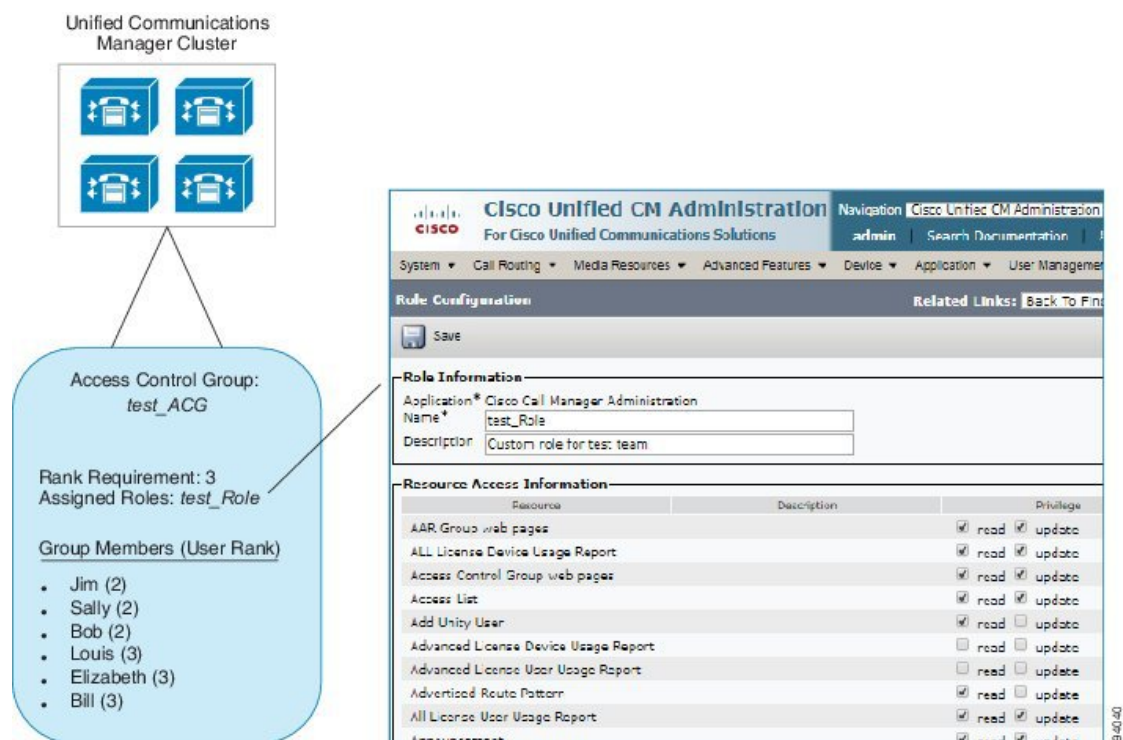
- カスタムアクセス制御グループ：必要条件を満たすロールの権限が標準のグループに含まれていない場合は、独自のアクセス制御グループを作成します。

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: 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
- パスワードの編集
- 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	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>(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。</p> <p>(注) [表示 (View)] を選択した場合、[ユーザは自分のユーザの権限情報を更新できます (User can update Permissions Information for own user)] フィールドが [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には、[権限情報 (Permission Information)] フィールドを [更新 (Update)] に設定する必要があります。</p>
ユーザは自分のユーザの権限情報を更新できる	<p>自分のアクセス権限を編集するユーザの機能を制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは自分の権限情報を更新できます。 • [いいえ (No)] : ユーザは自分の権限情報を更新できません。ただし、ユーザは、同じまたはより低いランクのユーザの権限情報を表示または変更できます。 <p>(注) [ユーザは自分のユーザの権限情報を更新できます (User can update Permissions Information for own user)] フィールドは [いいえ (No)] に設定され、[権限情報の更新 (Permission Information Update)] チェックボックスがオフの場合は無効になります。</p>

高度なリソース	アクセス制御
ユーザ ランク	<p>ユーザ ランクを変更する機能を制御します。</p> <ul style="list-style-type: none"> • [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。 <p>(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。</p> <p>(注) [表示 (View)] を選択した場合、[ユーザは自分のユーザ ランクを更新できます (User can update User Rank for own user)] フィールドが [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には、[ユーザ ランク (User Rate)] フィールドを [更新 (Update)] に設定する必要があります。</p>
ユーザは自分のユーザのユーザランクを更新できる	<p>自分のユーザ ランクを編集するユーザの機能を制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは自分のユーザ ランクを更新できます。 • [いいえ (No)] : ユーザは自分のユーザ ランクを更新できません。ただし、同じまたはより低いランクのユーザのランクを表示または変更できます。 <p>(注) [ユーザは自分のユーザのユーザ ランクを更新できます (User can update User Rank for own user)] フィールドは [いいえ (No)] に設定されており、[ユーザー ランク (User Rank)] [更新 (Update)] チェックボックスが選択されていない場合は無効になっています。</p>
新しいユーザの追加	<p>新しいユーザを追加する機能を次のように制御します。</p> <ul style="list-style-type: none"> • [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 (Password)]	<p>パスワードを変更する機能を制御します。</p> <ul style="list-style-type: none"> • [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。

ユーザーランクの概要

ユーザー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ー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ーランクを割り当てる必要があります。**Control** 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、ユーザのユーザー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 ユーザのユーザーランクが3の場合、3～10のユーザー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のユーザーランク要件を持つアクセス制御グループに割り当ててはできません。

管理者は、**[ユーザー順位の設定]** ウィンドウ内に独自のユーザー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。ユーザー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 **control** グループにアクセスするときにユーザー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ーランク 1 (可能な限り高いランク) が割り当てられます。

ユーザーアクセスの前提条件

ユーザに必要なアクセスレベルがわかるように、ユーザのニーズを必ず確認してください。ユーザが必要とするアクセス権限を持つロールを割り当てる必要がありますが、アクセスできないシステムへのアクセスは提供しません。

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。

ユーザーアクセスの設定タスク フロー

以下のタスクを実行して、ユーザーアクセスを設定します。

始める前に

デフォルトの役割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ロールとアクセス制御グループを作成するためのタスクをスキップできます。ユーザ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ことができます。

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。このタスクを省略すると、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)が割り当てられることに注意してください。
ステップ2	カスタムロールの作成 (8 ページ)	デフォルトのロールに必要なアクセス権限がない場合は、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)	オプション。カスタムロールの高度な権限を使用すると、管理者によるキーユーザ設定の編集機能を制御できます。
ステップ4	アクセス制御グループの作成 (10 ページ)	デフォルトグループに必要なロール割り当てがない場合は、カスタム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 (11 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 (12 ページ)	オプション。この設定は、ユーザが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割り当てられている場合に使用されます。

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 (Save)] 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

高度なロール設定を使用すると、カスタムロールの権限をより詳細なレベルで編集できます。[エンドユーザの設定 (End User configuration)] ウィンドウと [アプリケーションユーザの設定 (Application User configuration)] ウィンドウで、次のキー設定を編集する管理者の機能を制御できます。

- 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およびその設定についてのヘルプは、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る場合は、**[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 (Copy)]** 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** **[名前 (Name)]** に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 (Save)]** 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 \(11 ページ\)](#)

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し、ランク階層とアクセスコントロールグループが適切な権限で作成されている場合、LDAP同期の一部としてグループを同期されたユーザに割り当てることができます。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)] > [アクセス制御グループ (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** [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。
- [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。
 - 追加するユーザを選択します。
 - [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。
- 削除するユーザを選択します。
 - [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、ル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制御グループ、ルール、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 権限の作成 (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 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 (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 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 (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 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 \(14 ページ\)](#)

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 権限の作成 \(13 ページ\)](#)

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)] 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 \(14 ページ\)](#)

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 \(14 ページ\)](#)

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。
[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 \(15 ページ\)](#)

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 \(14 ページ\)](#)

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://<UCAddress: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。
- UCAddress 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 (System)] > [サービスパラメータ (Service Parameters)])。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] [システム (System)] > [サービスパラメータ (Service Parameters)] 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に、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、暗号化パスワードを生成します。

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ワードを提供します。

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 スーパーユーザー (Standard CCM Super Users)]

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ユーザー	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 管理ユーザー、標準 CCM スーパー ユーザー
標準監査ログ管理	<p>監査ロギング機能の次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 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 	標準監査ユーザー
標準 CCM 管理ユーザー	Cisco Unified Communications Manager Administration へのログイン権限を付与します。	標準 CCM 管理ユーザー、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 サーバー モニタリング、標準 CCM スーパー ユーザー、標準 CCM サーバーメンテナンス、標準 パケット スニファ ユーザー
[標準CCMエンドユーザー (Standard CCM End Users)]	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ーに付与します。	[標準CCMエンドユーザー (Standard CCM End Users)]

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	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 一括管理ツールによる次の項目の表示、削除、挿入： <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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ィール 	[標準CCMサーバーメンテナンス (Standard CCM Server Maintenance)]
標準 CCM ゲートウェイ管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 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	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 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ー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。 <ul style="list-style-type: none"> • 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制御グループ
標準 CCM ルートプラン管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 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	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 次の項目を表示および設定できます。 <ul style="list-style-type: none"> • アナウンサー、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 サーバー • 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サーバーメンテナンス (Standard CCM Server Maintenance)]

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	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 次の項目を表示および設定できます。 <ul style="list-style-type: none"> • 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) サーバー • 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 • サーバー • 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 (Standard CCM Server Maintenance)

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 ユーザー権限管理	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 (Standard CCMADMIN Administration)	CCMAdmin システムのすべての面を利用できます。	
標準CCMADMIN管理 (Standard CCMADMIN Administration)	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スーパーユーザー (Standard CCM Super Users)]
標準CCMADMIN管理 (Standard CCMADMIN Administration)	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 (Standard CCMADMIN Read Only)	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 (Standard CCMADMIN Read Only)	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 サーバー メンテナンス、標準 CCM サーバー モニタリング
標準CCMADMIN読み取り専用 (Standard CCMADMIN Read Only)	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 (Standard CCM End Users)
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ーできます。	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 開通している回線およびパーク回線の最大数は 65,000 を超えてはなりません。 合計が 65,000 を超える場合は、アプリケーションユーザから Standard CTI Allow Call Park Monitoring 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CUREporting (Standard 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 (Standard 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 管理ユーザー、標準 CCM スーパーユーザー
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 スーパーユーザー、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アユーザー
標準 RealtimeAndTraceCollection (Standard 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。 <ul style="list-style-type: none"> • 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 (Standard 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
<p>標準 SERVICEABILITY</p>	<p>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。</p> <ul style="list-style-type: none"> • [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) <p>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。</p> <p>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。</p> <p>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。</p>	<p>標準 CCM サーバー モニタリング、標準 CCM スーパー ユーザー</p>

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 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 (Standard SERVICEABILITY Administration)	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 (Standard SERVICEABILITY Administration)	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 (Standard SERVICEABILITY Read Only)	Dialed Number Analyzer のコンポーネントで使用され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 (Standard SERVICEABILITY Read Only)	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 ユーザー	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 (Standard CCMADMIN Read Only)	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 (Standard CUReporting)	アプリケーションユーザーが、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のレポートニング

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。