[ユーザ管理（Manage Users）]

このセクションでは、次の点について説明します。

[ユーザ管理（Manage Users）]

Cisco Prime Collaboration Assurance は、さまざまなタスクを実行できるようにする事前定義済みのアクセス コントロールを持つ、組み込みの静的ロールをサポートしています。

Cisco Prime Collaboration Assurance では、ユーザを作成し、ユーザにロールを割り当てることができます。

Cisco Prime Collaboration Assurance では、こうした組み込みの静的ロールによって、ロールベース アクセス コントロール（RBAC）が有効化されます。したがって、ユーザが実行できるタスク、またはユーザが表示または管理できるデバイスまたはデバイス グループは、ネットワーク管理者が割り当てたロールによって制御されます。

デバイスまたはデバイス グループをドメイン（Cisco Prime Collaboration Assurance を Enterprise モードで導入している場合）に関連付けることにより、選択したデバイスまたはデバイス グループ、およびそれらに関連するタスクのアクセス制御を強化できます。通常、オペレータ ロールを持つユーザは、特定の ドメインにのみアクセスが許可されます。

Cisco Prime Collaboration Assurance - 高度なユーザ ロール

ユーザ ロールは、ユーザがアクセスできるタスクの許可を定義するために使用されます。

次のロールのいずれかを割り当てることができます。

- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  レポート ビューア：レポートを表示およびエクスポートすることのみ可能です。レポート ビューアのホームページは、CDR および CMR レポートです。レポート ビューアのユーザ ロールでは、**検索**、**デバイス ス テータスの概要**、**アラーム**、**Advanced を取得**などのグローバル ユーザ インターフェイス コンポーネントを使用することはできません。次のものを除き、すべてのレポートを表示できます。

- CUCM レポートの起動
- 管理レポート
- スケジュール済みレポート

- ヘルプデスク：ネットワーク ステータス情報の表示とアクセスのみが可能です。また、デバイスでアクションを何も実行できず、ネットワークに到達するジョブをスケジュールすることもできません。
- オペレータ：すべてのヘルプデスク タスク、およびネットワーク データの収集に関連するタスクを実行します。デバイスの追加、検出、またはインポートなどのインベントリ管理操作は実行できません。また、アラームとイベントのしきい値を設定することもできません。
- ネットワーク管理者：すべてのオペレータ タスクと、クレデンシャルの管理やしきい値の設定など、ネットワーク設定の変更を引き起こすタスクを実行します。
- システム管理者：バックアップと復元、ログ ファイルの保守、ユーザの設定など、Assurance のユーザ インターフェイス関連の管理タスクを実行します。
- スーパー管理者：システム管理者とネットワーク管理者の両方が実行できるタスクを実行します。

ヘルプデスクは、Cisco Prime Collaboration Assurance のすべてのユーザに対して事前に割り当てられるロールです。

Cisco Prime Collaboration リリース 11.5 以降の場合

レポート ビューアは、Cisco Prime Collaboration Assurance のすべてのユーザに対して事前に割り当てられるロールです。

ユーザに対して選択されたロールによって、他のユーザのデータに対するアクセス権が決まります。たとえば、スーパー管理者のロールを持つユーザは、他のすべてのユーザを表示できますが、ネットワーク管理者のロールを持つユーザは、スーパー管理者やシステム管理者などの上位のロールを持つユーザを表示することはできず、オペレータやヘルプデスクのロールを持つ他のユーザのデータは参照できます。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、同じロールを持つ別のユーザに属する顧客を（その顧客に関連付けられているユーザであれば）参照することができます。

Cisco Prime Collaboration Assurance を ENT モードで展開した場合は、同じロールを持つ別のユーザに属するドメインを（そのドメインに関連付けられているユーザであれば）参照することができます。

注記：[ユーザ管理（User Management）] サブメニューは、次のロールでは使用できません。

Cisco Prime Collaboration リリース 11.5 以降の場合

1. Report Viewer
2. Helpdesk

3. 演算子

Cisco Prime Collaboration リリース 11.6 以降の場合

デフォルトのユーザ ロールの選択は、Cisco Prime Collaboration Assurance から削除されています。

（注） レポート ビューアのロールが選択されたユーザが他のロールを選択することや、他のロールのユーザがレポート ビューアを選択することはできません。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

複数レベルでの承認を可能にするために、次のロールがサポートされています。

1. **ネットワーク管理者**：すべてのオペレータ タスクと、クレデンシャルの管理などのネットワーク設定の変更を引き起こすタスクを実行します。
2. **システム管理者**：ユーザ インターフェイス関連の管理タスクを実行します。
3. **スーパー管理者**：システム管理者とネットワーク管理者の両方が実行できるタスクを実行します。

関連トピック

顧客の管理
ドメインの管理

Cisco Prime Collaboration Assurance のシングル サインオン

Cisco Prime Collaboration Assurance はセキュリティ アサーション マークアップ言語（SAML）を使用して Cisco Prime Collaboration Assurance でのシングル サインオン（SSO）を可能にする管理者権限をユーザに提供します。

Cisco Prime Collaboration Assurance は、マルチサーバの SAN 証明書およびエンドユーザの SAML SSO をサポートしていません。

SSO を有効にする前に、次の前提条件が満たされていることを確認してください。

- Cisco Prime Collaboration Assurance で LDAP 管理ユーザを手動で作成することにより、システムには少なくとも 1 人の LDAP 管理ユーザが存在します。
- Identity Provider（IdP）サーバは、単一ホストのアプリケーションおよびサービス プロバイダーが提供するその他多くのアプリケーションへのアクセスに SSO を使用できるようにします。サービス プロバイダーとはアプリケーションをホストする Web サイトです。

  次に、サポートされているサードパーティ IdP サーバを示します。

  - Open Access Manager（OpenAM）
  - Ping ID
  - Active Directory Federation Services（ADFS）
  - Oracle Identity Manager

IdP サーバをセットアップする手順については、『SAML SSO Deployment Guide for Cisco Unified Communication Applications, Release 10.0(1)』を参照してください。

- IdP サーバからのアイデンティティ プロバイダーのメタデータ ファイルをダウンロードし、ローカル システムに保存します。

シングル サインオンを有効にするには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[シングル サインオン（Single Sign-On）]**。

ステップ 2 [SSO を有効にする（Enable SSO）] をクリックします。

「Enabling SSO redirects you to the IdP server for authentication from the next login」という警告メッセージが表示されます。アプリケーションにアクセスするには、正常に認証される必要があります。

（注） 前述の前提条件が満たされていない場合は、[SSOを有効にする（Enable SSO）] は無効になっています。

ステップ 3 [続行（Continue）] をクリックします。

ステップ 4 シングル サインオンを有効にするには、SSO ウィザードに示される手順に従います。

a) ローカル システムから IdP メタデータ ファイルを見つけ、[IdP メタデータのインポート（Import IdP Metadata）] をクリックします。

b) [Trust Metadata ファイルのダウンロード（Download Trust Metadata file）] をクリックします。

c) IdP サーバを起動し、ダウンロードした信頼メタデータ ファイルをインポートします。

（注） これは、SSO を有効にするための手動の手順です。SSO のテストを進める前に、IdP サーバで信頼範囲（CoT）を作成し、ログアウトする必要があります。

d) SSO のテスト セットアップを実行するには、[有効な管理ユーザ名（Administrative Usernames）] ドロップダウンからユーザ名を選択します。Active Directory の管理者であり、SSO ユーザの下で Cisco Unified CDM によって同期される任意のユーザを入力することができます

（注） ほかのユーザ名を使用して IdP サーバにログインすると、管理者アカウントがロックされる可能性があります。

e) [SSOテストの実行（Run SSO Test）] をクリックし、IdP サーバ、Cisco Prime Collaboration Assurance のアプリケーション、シングル サインオン間の接続をテストします。

「Unable to do Single Sign-On or Federation」というエラー メッセージが表示された場合は、次の手順を実行します。

- エンド ユーザ クレデンシャルを使用して手動で IdP サーバにログインし、認証が成功したかどうかを確認します。
- Trust Metadata ファイルが IdP サーバで正常にアップロードされているかどうかを確認します。
- Cisco Prime Collaboration Assurance サーバと IdP サーバが同じ信頼の輪にあるかどうかを確認します。

f) [終了（Finish）] をクリックします。

SSO のトラブルシューティングおよびログ

- SSO を有効化している間に Cisco Prime Collaboration Assurance サーバからログアウトした場合は、ブラウザを閉じて、Cisco Prime Collaboration Assurance アプリケーションを再起動することを推奨します。これは、Cisco Prime Collaboration Assurance サーバでの会議が期限切れになっても、IdP サーバ 会議はまだアクティブである可能性があるためです。
- SSO を有効化中、Cisco Prime Collaboration Assurance のホスト名が設定され、DNS の一部であることを確認します。

IdP サーバがダウンしている場合は、次のことが可能です。

- リカバリ URL（https://<PCserver IP アドレス または DNS に含まれているホスト名>:8443/ssosp/local/login）を使用します。
- CMD ユーティリティからシングル サインオンを無効にします。

Cisco Prime Collaboration Assurance アプリケーションで CMD ユーティリティから SSO を無効化するには、以下を実施します。

- ポート 26 の SSH を使用して Cisco Prime Collaboration Assurance サーバにログインします。
- Cisco Prime Collaboration Assurance の **/opt/emms/emsam/bin** ディレクトリに移動します。次の表に基づいて、**cpcmconfigsso.sh** ファイルの <Operation> と <Value> のエントリを追加します。

操作は次のとおりです。	値は次のとおりです。
1：シングル サインオン ステータスを取得	N/A
2：リカバリ URL ステータスを取得	N/A
3：シングル サインオン ステータスを設定	False （注） CLI から SSO を有効にすることはできません。SSO を有効にするにはユーザ インターフェイスの手順を使用します。
4：リカバリ URL ステータスを設定	True または False

- SSO を無効にするには、次のコマンドを実行します。

cpcmconfigsso.sh 3 false

（注） リカバリ URL は有効になっています。セキュリティ上の理由でこれを無効にする場合は、デフォルトで False に設定します。

デフォルト ユーザ アカウント

というデフォルトの Web クライアント管理者ユーザで事前設定されます。globaladmin は、の両方にアクセスできるスーパーユーザです。

仮想アプライアンスを設定するときに、globaladmin のパスワードを指定します。このクレデンシャルは、Cisco Prime Collaboration Assurance の Web クライアントを初めて起動する際に必要です。

注意 パスワードを忘れたり紛失した場合のために、root パスワードを書き留めておくことをお勧めします。root パスワードをリセットするには TAC サポート ケースを開く必要があります。

Cisco Prime Collaboration Assurance の Web クライアントに初めてログインする場合は、*globaladmin* としてログインします。

（注） これらのユーザのパスワード検証ルールについては、『Cisco Prime Collaboration Assurance および Analytics のインストールおよびアップグレード ガイド』を参照してください。

注意 名前を使用してユーザを作成しないでください（globaladmin、pmadmin、および admin）。

選択 。[ログをダウンロード（Download Log）] ボタンをクリックします。tar ファイルをダウンロードし、untar します。/opt/emms/emsam/log/importedprovisioninguser.log ファイルを確認し、重複するユーザ名（すでにCisco Prime Collaboration Assurance で使用されているユーザ名）、ユーザ名にパスワードがないなどの理由で Cisco Prime Collaboration Assurance データベースにインポートされなかったユーザを検索します。

Cisco Prime Collaboration Assurance アプリケーションは、互いにインベントリ データベースを共有しません。のタスクを実行するには、デバイスを別々に管理する必要があります。Cisco Prime Collaboration Assurance アプリケーションを使用してデバイスの管理タスクを実行するには、「デバイス クレデンシャルの管理」を参照してください。

関連トピック

デバイス クレデンシャルの管理
デバイス グループの管理

ユーザ ロールおよびタスク

Cisco Prime Collaboration Assurance バージョン 11.x の [ユーザ ロールおよびタスク（User Roles and Tasks）と、Cisco Prime Collaboration Assurance バージョン 12.x の [ユーザ ロールおよびタスク（User Roles and Tasks）]には、自身に対応付けられた Cisco Prime Collaboration Assurance のロールおよびタスクが一覧で表示されます。

（注） スーパー管理者は、すべてのユーザ インターフェイス メニューにアクセスし、すべてのタスクを実行できます。したがって、スーパー管理者は一覧に表示されません。

関連トピック

Cisco Prime Collaboration Assurance のユーザ ロールとタスク

ユーザの追加

ユーザを追加して、事前定義済みの静的ロールを割り当てることができます。ユーザは、Cisco Prime Collaboration Assurance の Web クライアントにのみアクセスでき、Cisco Prime Collaboration Assurance サーバに CLI からログインすることはできません。

ユーザを追加するには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[ユーザ管理（User Management）]**。

ステップ 2 **[ユーザ管理（User Management）]** ページで、**[追加（Add）]** をクリックします。

ステップ 3 **[ユーザの追加（Add User）]** ページで、必要なユーザの詳細情報を入力します。

LDAP サーバは認証を実行するため、Cisco Prime Collaboration Assurance と同じユーザ ID を持っている必要があることに注意してください。詳細については、「LDAP サーバの設定」を参照してください。

[LDAP User] オプションを選択した場合、[Password] フィールドおよび [Confirm Password] フィールドは表示されません。

ステップ 4 適切な Cisco Prime Collaboration Assurance ロールを選択します。

ステップ 5 **[Save]** をクリックします。

ユーザの詳細を編集するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** を選択して、必要な変更を行います。

Cisco Prime Collaboration リリース 11.6 以降の場合

レポート ビューアーのユーザ ロールを割り当て済みのロールから除外するには、[レポートビューアー（Report Viewer）] オプションを手動で選択解除して [保存（Save）] をクリックします。

通常のシステム管理タスクの一部として、Cisco Prime Collaboration Assurance データベースからユーザを削除する必要がある場合があります。ただし、Cisco Prime Collaboration Assurance の Web クライアントのデフォルトの管理者である *globaladmin* は削除できません。

ユーザを削除するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** **[削除（Delete）]**をクリックします。削除したユーザ名でスケジュールされたジョブは、キャンセルされるまで引き続き実行されます。

ユーザ ロールの変更

ユーザの連絡先情報、ロール、またはアカウント ステータスが変更された場合、管理者はシステムの対応する情報を編集する必要があります。

ユーザの詳細を編集するには、**[システム管理（System Administration）]**>**[ユーザ管理（User Management）]** を選択して、必要な変更を行います。

Cisco Prime Collaboration リリース 11.6 以降の場合

レポート ビューアーのユーザ ロールを割り当て済みのロールから除外するには、[レポート ビューアー（Report Viewer）] オプションを手動で選択解除して [保存（Save）] をクリックします。

通常のシステム管理タスクの一部として、Cisco Prime Collaboration Assurance データベースからユーザを削除する必要がある場合があります。ただし、Cisco Prime Collaboration Assurance の Web クライアントのデフォルト管理者「globaladmin」は削除できません。

ユーザを削除するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** でユーザを選択し、**[削除（Delete）]**をクリックします。削除したユーザ名でスケジュールされたジョブは、ジョブがキャンセルされるまで引き続き実行されます。

LDAP サーバの設定

Lightweight Directory Access Protocol（LDAP）サーバに保存されているユーザ情報にアクセスするために、Cisco Prime Collaboration Assurance を設定して LDAP サーバに接続することができます。

[ユーザ管理（User Management）] ページで LDAP ユーザを作成して、このユーザが LDAP のクレデンシャルを使用してログインできるようにする必要があります。ユーザを追加するには、「ユーザの追加」を、ユーザを編集または削除するには、「ユーザ ロールの変更」を参照してください。

Cisco Prime Collaboration Assurance は、1 つのプライマリ LDAP サーバと 1 つのバックアップ LDAP サーバをサポートしています。

LDAP サーバを設定するには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[LDAP設定（LDAP Settings）]**。

ステップ 2 [LDAP Settings] ページで、すべてのフィールドに値を入力します。フィールドの説明については、[LDAP Configuration] のパラメータを参照してください。

（注）

1. Cisco Prime Collaboration Assurance で SSL 暗号化を使用する必要がある場合は、[SSL を使用する（Use SSL）] チェックボックスをオンにして、ポート 636 を指定します。

   Cisco Prime Collaboration リリース 12.1 の場合

   SSL を有効にした LDAP 設定はサポートされていません。

2. 無効なログインの場合は、「ユーザ名またはパスワードが無効です。Please try again or check LDAP server configuration if you are a LDAP user（ユーザ名またはパスワードが無効です。もう一度やり直すか、LDAP ユーザの場合は LDAP サーバの設定を確認してください）」 というメッセージが表示されます。このメッセージは、ローカルと LDAP の両方のユーザに表示されます。

ステップ 3 LDAP サーバへの接続を確認するには、[テスト接続（Test Connection）] をクリックします。

ステップ 4 接続が正常に行われたら、[設定の適用（Apply Settings）] をクリックし、Cisco Prime Collaboration Assurance サーバを再起動して、LDAP を使用してログインします。

Cisco Prime Collaboration Assurance サーバを再起動するには、admin ユーザとしてログインし、次のコマンドを実行します。

```
application stop cpcm application start cpcm
```

application stop cpcm コマンドは実行完了までに 10 分、**application start cpcm** コマンドは実行完了までに 10 ～ 15 分かかります。

[LDAP Configuration] のパラメータ

たとえば、Microsoft Active Directory について考えてみましょう。

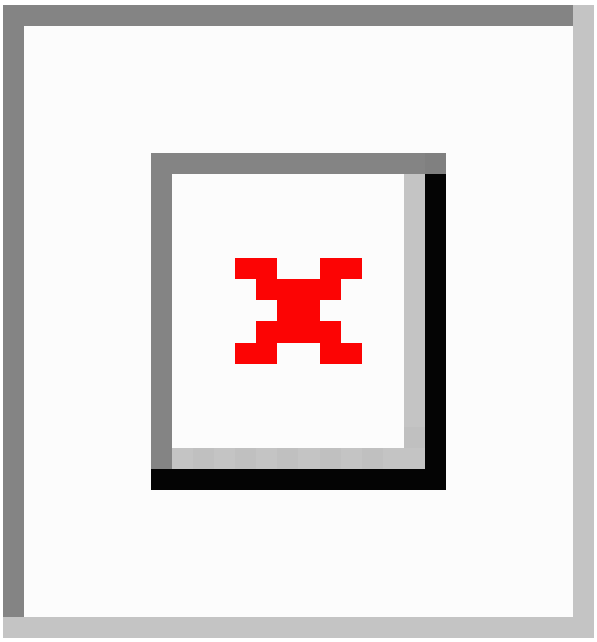

表 *1 : LDAP* サーバの設定

フィールド	説明
サーバの IP アドレス	LDAP サーバ名または IP アドレスを入力します。 オプションで、バックアップ LDAP サーバの IP アドレスを入力します。

フィールド	説明
サーバ ポート	サーバの LDAP 要求を受信するポート番号を入力します。 [Non-secure port]：389 [Secure SSL port]：636 オプションでバックアップLDAPサーバのポート番号を入力します。 （注） 標準以外のポートを使用するように LDAP サーバが設定されている場合は、そのポートもここで入力する必要があります。
Admin Distinguished Name	[Admin Distinguished Name] は使用する識別名です。 たとえば、前述のイメージでは、LDAP ディレクトリに John Doe という名前のユーザが 含まれていますが、[Admin Distinguished Name] は次のようになります。 • CN = John Doe • OU = Campus • OU = AdminBLR • OU = ABC • DC = eta • DC = com
管理者パスワード	LDAPサーバのパスワードを入力し、パスワードを再確認します。 （注） パスワードにシャープ記号（#）を使用しないでください。LDAP のユーザパスワードにシャープ記号が含まれていると、LDAP サーバへの接続が失敗します。

フィールド	説明
LDAP ユーザの検索ベース	ユーザの検索ベースを入力します。LDAPサーバはこのベースに基づいてユーザを検索します。 検索ベースは次のとおりです。 • DC = eta • DC = com （注） LDAP 認証は、検索ベースで特殊文字を入力すると失敗します。

（注）

1. Cisco Prime Collaboration Assurance は、必要に応じて、LDAP ユーザの CN、sAMAccountName、または uid 属性を使用した PCA へのログインをサポートします。
2. LDAP ユーザの uid 属性は一意である必要があります。
3. LDAPパラメータ値では、識別名（DN）でアンパサンド（&）を使用することはできません。

   LDAP に接続するには、次の LDAP パラメータ値を入力します。

   ```
   ?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?
   ```

サポートされている LDAP サーバの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

パスワードの最大数を設定

認証メカニズムは、そのクレデンシャルと同じだけの強度しかありません。

強力な認証メカニズムを使用することは、強力なパスワードを使用するために重要です。パスワードが複雑になっていない場合（特にパスワード長）、検索スペースが大幅に削減されます。

（注）

- デフォルトのパスワードの最大長は 127 文字です。
- デフォルトの管理者である globaladmin のみが、Cisco Prime Collaboration Assurance ユーザインターフェイスの [セキュリティ設定（security settings）] ページを変更する権限を持ちます。

ステップ 1 [システム管理（**System Administration**）] > [セキュリティ設定（**Security Settings**）] を選択します。

（注） ユーザは、80-127 文字（バイトではありません）の範囲で値を入力する必要があります。入力した値が範囲外の場合は、入力された値が許容範囲を超えていることを示すメッセージが表示されます。**[OK]** をクリックして続行します。

ステップ 2 値を入力するか、またはスピン ボックスをクリックして、パスワード長を設定します。

ステップ 3 [保存（Save）] をクリックして、設定の詳細を正常に更新します。アプリケーションは、ユーザがパスワードの最大長を変更していることをアラートします。「Ensure compliance with this new value while setting password in other pages」と表示されます。

[キャンセル（Cancel）] をクリックして終了します。

（注） ユーザは、他のページでパスワードが必要な場合に、ここで設定した値よりも長いパスワードを入力することはできません。コンプライアンスに従っていないことを示すエラー メッセージが、そのページに表示されます。

Cisco Prime Collaboration Assurance アカウントのロック解除

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance のユーザ インターフェイスへのログインの最大試行回数は 10 です。10 回試行しても、Cisco Prime Collaboration Assurance のユーザ インターフェイスにログインできない場合は、アカウントが無効になります。

管理者権限を持つ globaladmin ユーザであれば、アカウントのロックを解除することができます。

アカウントのロックを解除するには、次のようにします。

ステップ 1 Cisco Prime Collaboration Assurance に globaladmin としてログインします。

ステップ 2 選択 **[システム管理（System Administration）]** > **[ユーザ管理（User Management）]**。

ステップ 3 **[ユーザ管理（User Management）]** ページで、ユーザを選択し、**[ロック解除（Unlock）]** をクリックします。