ユーザ アカウントの管理

この章は、次の項で構成されています。

- Configuring Local Users （1 ページ）
- パスワードの有効期限切れ （3 ページ）
- パスワードの有効期間の設定 （4 ページ）
- パスワード有効期限の有効化 （5 ページ）
- LDAP サーバ （6 ページ）
- ユーザ セッションの表示 （21 ページ）

Configuring Local Users

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。[ローカルユーザ（Local User）] タブには [強力なパスワードの無効化（Disable Strong Password）] ボタンが表示され、そのボタンを使用することで、強力なパスワードポリシーを無効にし、ガイドラインを無視して希望するパスワードを設定することができます。強力なパスワードを無効にすると、[強力なパスワードの有効化（Enable Strong Password）] ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

始める前に

ローカルユーザアカウントを設定または変更するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [ローカル ユーザ管理（Local User Management）] タブをクリックします。

ステップ 4 ローカル ユーザ アカウントを設定または変更するには、[Local User Management] ペインの行をクリックして、[Modify User] をクリックします。

ステップ 5 [ユーザの詳細の変更（Modify User Details）] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザの固有識別情報。
[有効化（Enable）] チェックボックス	オンにすると、ユーザは Cisco IMC で有効になります。
[ユーザ名（Username）] フィールド	ユーザのユーザ名。 1 ～ 16 文字の範囲で入力します。

[ロール（Role）] フィールド	ユーザに割り当てられているロール。次のいずれかになります。
	• [読み取り専用（read-only）]：このロールのユーザは情報を表示できますが、変更することはできません。
	• [ユーザ（user）]：このロールのユーザは、次のタスクを実行できます。
	  • すべての情報を表示する
	  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
	  • KVM コンソールと仮想メディアを起動する
	  • すべてのログをクリアする
	  • ロケータ LED を切り替える
	  • タイム ゾーンを設定する
	  • ping
	• [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[パスワードの変更（Change Password）] チェックボックス	オンにすると、変更を保存した場合、このユーザのパスワードが変更されます。新しいユーザ名の場合は、このチェックボックスをオンにする必要があります。

名前	説明

[新しいパスワード（New Password）] フィールド	このユーザ名のパスワード。フィールドの横の [ヘルプ（Help）] アイコンの上にカーソルを重ねると、パスワードを設定する際の以下のガイドラインが表示されます。
	• パスワードは 8 ～ 14 文字とすること。
	• パスワードにユーザ名を含めないこと。
	• パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。
	  • 大文字の英字（A ～ Z）。
	  • 小文字の英字（a ～ z）。
	  • 10 進数の数字（0 ～ 9）。
	  • アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、')。
	
	これらのルールは、セキュリティ上の理由からユーザ用の強力なパスワードを定義するためのものです。ただし、これらのガイドラインを無視して希望するパスワードを設定する場合は、[ローカル ユーザ（Local Users）] タブで [強力なパスワードの無効化（Disable Strong Password）] ボタンをクリックします。強力なパスワード オプションが無効にされている場合は、1 ～ 20 文字のパスワードを設定できます。

[新しいパスワードの確認（Confirm New Password）] フィールド	確認のためのパスワードの再入力。

ステップ 6 パスワード情報を入力します。

ステップ 7 [変更の保存（Save Changes）] をクリックします。

パスワードの有効期限切れ

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。パスワードの期限が切れると、ユーザはログイン時に通知され、パスワードをリセットしない限りログインできなくなります。

（注） 古いデータベースにダウングレードした場合、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザは消去され、データベースは空になります。つまり、データベースのユーザ名はデフォルトの「admin」、パスワードは「password」となります。サーバにはデフォルトのユーザデータベースが残っているため、デフォルトのクレデンシャルの変更機能が有効になっています。これは、ダウングレード後に「admin」ユーザがデータベースに初めてログインする際に、そのユーザはデフォルトのクレデンシャルを強制的に変更する必要があることを意味します。

パスワード設定時刻

「パスワード設定時刻」は、すべての既存ユーザに対し、移行またはアップグレードが発生した時刻に設定されています。新規ユーザ（アップグレード後に作成されたユーザ）の場合、パスワード設定時刻は、ユーザが作成され、パスワードが設定された時刻に設定されます。一般ユーザ（新規および既存）の場合、パスワード設定時刻は、パスワードが変更されるたびに更新されます。

パスワードの有効期間の設定

始める前に

- パスワードの有効期限を有効にする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [Local User Management] ペイン（デフォルトで開きます）で、[Password Expiration Details] をクリックします。

ステップ 4 [パスワードの有効期限の詳細（Password Expiration Details）] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[パスワードの有効期限の有効化（Enable Password Expiry）] チェックボックス	このチェックボックスをオンにすると、[パスワードの有効期間（Password Expiry Duration）] を設定できます。無効にするには、このチェックボックスをオフにします。
[パスワードの有効期間（Password Expiry Duration）] フィールド	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します）。範囲は 1 ～ 3650 日です。

名前	説明
[パスワード履歴（Password History）] フィールド	パスワードが入力された回数。これを有効にすると、パスワードを繰り返すことができません。0 ～ 5 の間の値を入力します。0 を入力すると、このフィールドが無効になります。
[通知期間（Notification Period）] フィールド	パスワードの期限が切れる時間を通知します。0 ～ 15 日の間の値を入力します。0 を入力すると、このフィールドが無効になります。 （注） 通知期間の時間は、パスワードの有効期間内でなければなりません。
[猶予期間（Grace Period）] フィールド	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0 ～ 5 日の間の値を入力します。0 を入力すると、このフィールドが無効になります。 （注） 猶予期間の時間は、パスワードの有効期間内でなければなりません。

（注） 有効な [パスワードの有効期間（Password Expiry Duration））] は、[通知期間（Notification Period）] および [猶予期間（Grace Period）] より長い必要があります。そうでない場合、**ユーザ パスワードの有効期限ポリシーの設定エラー**が表示されます。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

ステップ 6 必要に応じて、[値のリセット（Reset Values）] をクリックして、テキスト フィールドをクリアし、入力した値をリセットします。デフォルト設定に戻すには、[デフォルトに戻す（Restore Defaults）] をクリックします。

パスワード有効期限の有効化

始める前に

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [Local User Management] ペイン（デフォルトで開きます）で、[Password Expiration Details] をクリックします。

ステップ 4 [パスワードの有効期限の詳細（Password Expiration Details）] ダイアログ ボックスで、[パスワードの有効期限の有効化（Enable Password Expiry）] チェック ボックスをオンにします。

[パスワードの有効期間（Password Expiry Duration）] テキスト フィールドが編集可能になり、日数の数値を入力することで期間を設定できます。

次のタスク

パスワードの有効期間を設定します。

LDAP サーバ

Cisco IMC は、ディレクトリ内の情報を整理し、この情報へのアクセスを管理するディレクトリ サービスをサポートしています。Cisco IMC は、Lightweight Directory Access Protocol（LDAP）をサポートしています。これは、ネットワークでのディレクトリ情報を保存し維持するものです。さらに、Cisco IMC は Microsoft Active Directory（AD）もサポートします。Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、ローカル ユーザ データベース内に見つからないユーザ アカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は username@domain.com です。

[LDAP 設定（LDAP Settings）] 領域の [暗号化を有効にする（Enable Encryption）] チェック ボックスをオンにすると、LDAP サーバへの送信データを暗号化するようサーバに要求できます。

Configuring the LDAP Server

ユーザ認証および権限付与のために LDAP を使用するよう、Cisco IMC を設定できます。LDAP を使用するには、Cisco IMC に関するユーザ ロール情報とロケール情報を保持する属性を使ってユーザを設定します。Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

（注） この例では CiscoAVPair という名前のカスタム属性を作成しますが、Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用することもできます。

Cisco IMC の LDAP 設定でグループ認証を使用している場合、手順 1 ~ 4 をスキップし、*Cisco IMC で LDAP 設定とグループ認証の構成*のセクションに記載されている手順を実行します。

LDAP サーバに対して次の手順を実行する必要があります。

手順

ステップ 1 LDAP スキーマ スナップインがインストールされていることを確認します。

ステップ 2 スキーマ スナップインを使用して、次のプロパティを持つ新しい属性を追加します。

プロパティ（**Properties**）	値
Common Name	**`CiscoAVPair`**
LDAP Display Name	**`CiscoAVPair`**
Unique X500 Object ID	**`1.3.6.1.4.1.9.287247.1`**
Description	**`CiscoAVPair`**
Syntax	**大文字小文字を区別した文字列**

ステップ 3 スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。

a) 左ペインで [クラス（Classes）] ノードを展開し、**`U`** を入力してユーザ クラスを選択します。

b) [属性（Attributes）] タブをクリックして、[追加（Add）] をクリックします。

c) **`C`** を入力して CiscoAVPair 属性を選択します。

d) [OK] をクリックします。

ステップ 4 Cisco IMC にアクセスできるようにするユーザに対し、次のユーザ ロール値を CiscoAVPair 属性に追加します。

ロール	**CiscoAVPair 属性値**
admin	**`shell:roles="admin"`**
user	**`shell:roles="user"`**
read-only	**`shell:roles="read-only"`**

（注） 属性に値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

次のタスク

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC での LDAP 設定およびグループ認証の設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ウィンドウの [LDAP] をクリックします。

ステップ 4 [LDAP 設定（LDAP Settings）] 領域で、次のプロパティを更新します。

名前	説明
[LDAP の有効化（Enable LDAP）] チェックボックス	これを選択した場合、まずLDAPサーバによってユーザ認証とロール許可が実行された後、ローカル ユーザ データベースに存在しないユーザ アカウントによって実行されます。
[ベース DN（Base DN）] フィールド	ベース識別名。このフィールドは、ユーザおよびグループのロード元を示します。 Active Directory サーバでは、これは **dc=domain,dc=com** という形式でなければなりません。
[ドメイン（Domain）] フィールド	すべてのユーザが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[暗号化を有効にする（Enable Encryption）] チェックボックス	これを選択した場合、サーバは LDAP サーバに送るすべての情報を暗号化します。
[CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックス	オンにすると、LDAP CA 証明書をバインドできます。

名前	説明
[タイムアウト（0 ～ 180）秒数（Timeout (0 - 180) seconds）]	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数。 検索操作がタイムアウトになった場合、Cisco IMC はこのタブで次にリストされているサーバ（存在する場合）に接続しようと試行します。 （注） このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。
[ユーザ検索の優先順位（User Search Precedence）]	ローカル ユーザ データベースと LDAP ユーザ データベースの間の検索の順序を指定できます。次のいずれかになります。 • [ローカル ユーザ データベース（Local User Database）]（デフォルト設定） • **[LDAP ユーザ データベース（LDAP User Database）]**

（注） [暗号化を有効にする（Enable Encryption）] チェックボックスと [CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

ステップ 5 [LDAP サーバの設定（Configure LDAP Servers）] 領域で、次のプロパティを更新します。

名前	説明
[LDAP サーバの事前設定（Pre-Configure LDAP Servers）] オプション ボタン	これを選択すると、Active Directory は事前構成された LDAP サーバを使用します。
[LDAP サーバ（LDAP Servers）] フィールド	
[サーバ（Server）]	6 つの LDAP サーバの IP アドレス。 LDAP に Active Directory を使用している場合、サーバ 1、2、3 はドメイン コントローラで、サーバ 4、5、6 はグローバル カタログです。LDAP 用に Active Directory を使用していない場合は、最大で 6 つの LDAP サーバを構成できます。 （注） また、ホスト名の IP アドレスも提供できます。

名前	説明
Port	サーバのポート番号。 LDAP に Active Directory を使用している場合、サーバ 1、2、3（ドメイン コントローラ）のデフォルト ポート番号は389です。サーバ4、5、6（グローバル カタログ）のデフォルト ポート番号は 3268 です。 LDAPS 通信は TCP 636 ポートで発生します。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートで発生します。
[DNS を使用した LDAP サーバの設定（Use DNS to Configure LDAP Servers）] オプション ボタン	これを選択した場合、DNS を使って LDAP サーバへのアクセスを設定できます。
[DNS パラメータ（DNS Parameters）] フィールド	
ソース（**Source**）	DNS SRV 要求に使われるドメイン名を取得する方法を指定します。この属性の種類は次のとおりです。 • [抽出済み（Extracted）] : ログイン ID からのドメイン名抽出ドメインを使用するよう指定します。 • [設定済み（Configured）] : 設定された検索ドメインの使用を指定します。 • [設定済み - 抽出済み（Configured-Extracted）] : 設定された検索ドメインよりも、ログイン ID から抽出されるドメイン名を使用することを指定します。
検索するドメイン（**Domain to Search**）	DNS クエリーのソースとして機能する設定済みドメイン名。 ソースが [抽出済み（Extracted）] と指定される場合、このフィールドは無効になります。
検索するフォレスト（**Forest to Search**）	DNS クエリーのソースとして機能する設定済みフォレスト名。 ソースが [抽出済み（Extracted）] と指定される場合、このフィールドは無効になります。

ステップ 6 [バインディング パラメータ（Binding Parameters）] 領域で、次のプロパティを更新します。

名前	説明
方法（Method）	この属性の種類は次のとおりです。 • [匿名（Anonymous）] : ユーザ名とパスワードを NULL にする必要があります。このオプションが選択され、LDAP サーバで匿名ログインが設定されている場合は、ユーザがアクセスすることができます。 • [設定済みクレデンシャル（Configured Credentials）] : 初期バインド プロセスに対して既知のクレデンシャル セットを指定する必要があります。初期バインド プロセスが成功した場合、ユーザ名の識別名（DN）が照会され、再バインディング プロセス用に再利用されます。再バインディング プロセスが失敗すると、ユーザはアクセスを拒否されます。 • [ログイン クレデンシャル（Login Credentials）] : ユーザ クレデンシャルが必要です。バインド プロセスが失敗すると、ユーザはアクセスを拒否されます。 デフォルトでは、[ログイン クレデンシャル（Login Credentials）] オプションが選択されます。
バインド DN（Binding DN）	ユーザの識別名（DN）。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。
Password	ユーザのパスワード。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。

ステップ 7 [検索パラメータ（Search Parameters）] 領域で、次のフィールドを更新します。

名前	説明
フィルタ属性（Filter Attribute）	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [sAMAccountName] と表示されます。

名前	説明
グループ属性（**Group Attribute**）	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [memberOf] と表示されます。
属性（**Attribute**）	ユーザのロールとロケール情報を保持する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP 属性では、Cisco IMC ユーザ ロールおよびロケールにマップされる既存の LDAP 属性を使用することも、スキーマを変更して新しいLDAP属性を作成することもできます。（たとえば **CiscoAvPair** など）。 （注） このプロパティを指定しない場合、ユーザはログインできません。オブジェクトは LDAP サーバ上に存在していますが、このフィールドで指定される属性と正確に一致する必要があります。
階層化するグループ検索の深さ（**1 ～ 128**）（**Nested Group Search Depth (1-128)**）	LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索するパラメータ。このパラメータは、ネストされたグループ検索の深さを定義します。

ステップ 8 （任意） [グループ認証（Group Authorization）] 領域で、次のプロパティを更新します。

名前	説明
[LDAP グループ認証（LDAP Group Authorization）] チェックボックス	これを選択した場合、ローカル ユーザ データベースにない LDAP ユーザに関しても、グループ レベルでユーザ認証が実行されます。 このチェックボックスをオンにすると、Cisco IMC は [**Configure Group**] ボタンを有効にします。
[グループ名（Group Name）] カラム	サーバへのアクセスが許可されているグループの名前を LDAP サーバ データベースに指定します。
[グループ ドメイン（Group Domain）] カラム	LDAP サーバのドメインがグループに存在する必要があります。

名前	説明

[Role] カラム	すべてのユーザに割り当てられているこの LDAP サーバ グループのロール。次のいずれかになります。
	• [読み取り専用（read-only）]：このロールのユーザは情報を表示できますが、変更することはできません。
	• [ユーザ（user）]：このロールのユーザは、次のタスクを実行できます。
	  • すべての情報を表示する
	  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
	  • KVM コンソールと仮想メディアを起動する
	  • すべてのログをクリアする
	  • ロケータ LED を切り替える
	  • タイム ゾーンを設定する
	  • ping
	• [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[設定（Configure）] ボタン	Active Directory グループを設定します。
[削除（Delete）] ボタン	既存の LDAP グループを削除します。

ステップ 9 [変更の保存（Save Changes）] をクリックします。

ユーザ検索の優先順位の設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ウィンドウの [LDAP] タブをクリックします。

ステップ 4 [LDAP Settings] 領域の [User Search Precedence] フィールドで、[Local User Database] または [LDAP User Database] を選択します。

このフィールドでは、上記のオプション間の検索順序を指定することができます。[ローカル ユーザ データベース（Local User Database）] がデフォルトのオプションです。

次のタスク

LDAP 証明書の概要

Cisco C シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモートユーザ認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザ認証用のディレクトリ サーバを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

暗号化された TLS/SSL 通信中にディレクトリ サーバ証明書を検証するには、LDAP クライアントに新しい設定オプションが必要です。

LDAP CA 証明書ステータスの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [証明書ステータス（Certificate Status）] 領域で、次のフィールドの値を確認します。

名前	説明
ダウンロード ステータス	このフィールドには、LDAP CA 証明書のダウンロード ステータスが表示されます。
エクスポート ステータス（Export Status）	このフィールドには、LDAP CA 証明書のエクスポート ステータスが表示されます。

LDAP CA 証明書のエクスポート

始める前に

このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。

署名付き LDAP CA 証明書をエクスポートするには、あらかじめ証明書がダウンロードされている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）] リンクをクリックします。

[LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）] ダイアログボックスが表示されます。

名前	説明
[リモート ロケーションにエクスポート（**Export to Remote Location**）**[**	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • **• TFTP サーバ（TFTP Server）** **• FTP サーバ（FTP Server）** **• SFTP サーバ（SFTP Server）** **• SCP サーバ（SCP Server）** **• HTTP サーバ（HTTP Server）** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キーフィンガープリントは *<server_finger_print _ID>* です。続行しますか?（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバフィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（No）] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。

名前	説明
	• [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[ローカル デスクトップにエクスポート（Export to Local Desktop）]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ステップ 5 [証明書のエクスポート（Export Certificate）] をクリックします。

LDAP CA 証明書のダウンロード

始める前に

- このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- このアクションは、バインディング CA 証明書が有効にされていないと実行できません。

（注） Cisco IMC では CA 証明書またはチェーン CA 証明書のみを使用する必要があります。デフォルトの CA 証明書の形式は .cer です。チェーン CA 証明書を使用する場合は、Cisco IMC にダウンロードする前に .cer 形式に変換する必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書のダウンロード（Download LDAP CA Certificate）] リンクをクリックします。

[LDAP CA 証明書のダウンロード（Download LDAP CA Certificate）] ダイアログボックスが表示されます。

名前	説明
[リモート ロケーションからダウンロード（Download from remote location）] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • **• TFTP サーバ（TFTP Server）** **• FTP サーバ（FTP Server）** **• SFTP サーバ（SFTP Server）** **• SCP サーバ（SCP Server）** **• HTTP サーバ（HTTP Server）** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー フィンガープリントは *<server_finger_print _ID>* です。続行しますか?（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（No）] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC で使用するパスおよびファイル名。 • [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[ブラウザクライアント経由でダウンロード（Download through browser client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[証明書コンテンツの貼り付け（Paste Certificate content）] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [証明書コンテンツの貼り付け（Paste certificate content）] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[証明書のダウンロード（Download Certificate）] ボタン	証明書をサーバにダウンロードできます。

LDAP バインディングのテスト

始める前に

このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。

（注） [暗号化を有効にする（Enable Encryption）] チェックボックスと [CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP バインディングのテスト（Test LDAP Binding）] リンクをクリックします。

[LDAP CA 証明書のバインディングのテスト（Test LDAP CA Certificate Binding）] ダイアログボックスが表示されます。

名前	説明
[ユーザ名（Username）] フィールド	ユーザ名を入力します。
[パスワード（Password）] フィールド	対応するパスワードを入力します。

ステップ 5 [テスト（Test）] をクリックします。

LDAP CA 証明書の削除

始める前に

このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書の削除（Delete LDAP CA Certificate）] リンクをクリックし、[OK] をクリックして確定します。

ユーザ セッションの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ウィンドウの [セッション管理（Session Management）] をクリックします。

ステップ 4 [セッション（Sessions）] ペインで、現在のユーザセッションに関する次の情報を表示します。

名前	説明
[セッションの終了（Terminate Session）] ボタン	ユーザ アカウントに [管理者（admin）] ユーザ ロールが割り当てられている場合、このオプションを使用して、関連付けられているユーザ セッションを強制的に終了できます。 （注） このタブから現在のセッションを終了することはできません。
[セッション ID（Session ID）] カラム	セッションの固有識別情報。
[ユーザ名（User name）] カラム	ユーザのユーザ名。
[IP アドレス（IP Address）] カラム	ユーザがサーバにアクセスした IP アドレス。シリアル接続の場合は、[なし（N/A）] と表示されます。
[タイプ（Type）] カラム	ユーザがサーバにアクセスするために選択したセッション タイプ。次のいずれかになります。 • [webgui]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [シリアル（serial）]：ユーザがシリアル ポートを使用してサーバに接続されていることを示します。