ユーザー アカウントの管理

この章は、次の内容で構成されています。

- Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの追加 （1 ページ）
- Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの変更 （5 ページ）
- ユーザ アカウントでの SSH キーの管理 （10 ページ）
- 非 IPMI ユーザー モード （14 ページ）
- 非管理者ユーザーとしてパスワードの変更 （16 ページ）
- パスワードの有効期限切れ （19 ページ）
- パスワードの有効期間の設定 （20 ページ）
- パスワード有効期限の有効化 （21 ページ）
- アカウントロックアウトの詳細の構成 （22 ページ）
- ユーザー認証の優先順位の構成 （22 ページ）
- ユーザー クレデンシャルを工場出荷時の値にリセットする （23 ページ）
- LDAP サーバー （24 ページ）
- TACACS+ 認証 （39 ページ）
- ユーザ セッションの表示 （41 ページ）

Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの追加

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、サーバー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）]**タブに表示される **[強力なパスワードの無効化（Disable Strong Password）]** ボタンを使用すると、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自由にパスワードを設定できます。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

ローカルユーザーアカウントを追加するには、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）] ペインの [管理（Admin）] メニューをクリックします。

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

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

ステップ 4

ステップ 5 ローカル ユーザー アカウントを追加するには、**[ユーザーを追加 （Add User）]**をクリックします。

ローカル ユーザー アカウントを変更するには、**[ローカル ユーザー管理（Local User Management）]**ペインで行をクリックし、**[ユーザの変更（Modify User**）をクリックします。

ステップ 6 **[ユーザーの詳細の変更（Modify User Details）]** または、**[ローカル ユーザー詳細（Local 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	ユーザーの固有識別情報。識別子はユーザーが構成できません。識別子が自動的に割り当てられます。
[ユーザー名（Username）] フィールド	ユーザーのユーザー名。 ユーザー名は、**CIMC** および **SNMP** ユーザー タイプ（任意の組み合わせ）の場合は最大 32 文字、**IPMI** ユーザー タイプ（任意の組み合わせ）の場合は最大 16 文字です。**ユーザー タイプ**の詳細については、**ユーザー タイプ** チェック ボックスの説明を参照してください。

名前	説明
[Role Played] 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。 • [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。 • [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 • vKVM 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 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。 • **snmponly** - SNMP ロールのみを持つユーザー。 （注） 管理ロールを持つユーザーには、**[設定 (Settings)]** ドロップダウン メニューの右上隅にある **[パスワードの変更 (Change Password)]** オプションがありません。 非管理ユーザーとしてパスワードを変更するには、**[読み取り専用 (read-only)]** または **[ユーザー (User)]** ロールを選択します。**[管理者 (admin)]** ロールは選択しません。
ユーザー タイプ チェックボックス	次のタイプのユーザーを作成できます。 • CIMC • SNMP • IPMI 単独のユーザーに複数のタイプを割り当てることができます。
[有効（Enabled）] チェックボックス	オンにすると、ユーザーはCisco IMC で有効にされています。

表 *1 : CIMC* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[**提案（**Suggest**）**]** ボタンの横にある **?** アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

表 *2 : SNMP* ユーザー タイプ

名前	説明
[Security Level] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザーには、許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドを有効にします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は Auth フィールドおよび Privacy フィールドを有効にします。
[Auth Type] ドロップダウン	許可タイプ。次のいずれかになります。 • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**

名前	説明
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

表 *3 : IPMI* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]** ボタンの横にある **?** アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

ステップ 7 [保存（Save）] をクリックします。

Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの変更

Cisco IMC に強力なパスワード ポリシーが導入されました。このポリシーでは、初めてサーバにログオンするときに、ガイドラインに従って強力なパスワードを設定する必要があります。

[ローカル ユーザ（Local User）]タブに表示される **[強力なパスワードの無効化（Disable Strong Password）]** ボタンを使用すると、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自由にパスワードを設定できます。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

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

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

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

ステップ 3 [ユーザー管理（User Management）] ペインの [ローカルユーザー管理（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変更するには、**[ローカル ユーザ管理（Local User Management）]** ペインで行をクリックし、**[ユーザの変更（Modify User）]** をクリックします。

ステップ 5 [ユーザーの詳細の変更（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	ユーザーの固有識別情報。 これは、ユーザーが構成することはできません。
[ユーザー名（Username）] フィールド	ユーザーのユーザー名。 1 ～ 16 文字の範囲で入力します。

名前	説明
[割り当てられるロール（Role Played）] 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。 • [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。 • [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 • vKVM 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 の点灯・消灯（リモート作業者に場所を示す） • タイムゾーンの設定 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
ユーザータイプ	ユーザー タイプを次のように更新できます： • CIMC • SNMP • IPMI 単独のユーザーに複数のタイプを割り当てることができます。
[Enabled] チェックボックス	オンにすると、ユーザはCisco IMC でイネーブルになります。
[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。パスワードを変更するには、このチェックボックスをオンにする必要があります。 **[パスワードの変更（Change Password）]** チェック ボックスも、チェックされているすべての **[ユーザー タイプ（User Type）]** オプションを開きます。

表 *4 : CIMC* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]**ボタンの横にある**?**アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

表 *5 : SNMP* ユーザー タイプ

名前	説明
[Security Level] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザーには、許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドを有効にします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は Auth フィールドおよび Privacy フィールドを有効にします。
[Auth Type] ドロップダウン	許可タイプ。次のいずれかになります。 • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**

名前	説明
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

表 *6 : IPMI* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]** ボタンの横にある **?** アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

ステップ 6 パスワード情報を入力します。

ユーザ アカウントでの SSH キーの管理

SSH キーの設定

すべてのユーザの SSH キーを表示するには、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。管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを表示できます。

パブリック SSH キーを使用して認証された Cisco IMC セッションは、パスワードの有効期限が切れてもアクティブのままです。また、パスワードの有効期限が切れた後に、公開 SSH キーを使用して新しいセッションを開始することもできます。

アカウント ロックアウト オプションは、公開キー認証を使用するアカウントには適用されません。

始める前に

- すべてのユーザの SSH キーを設定するには、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。
- SSH RSA キーのペア (パブリックおよびプライベート) が作成されていることを確認します。
- SSH キーが .pem または .pub 形式であることを確認します。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[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）]** タブをクリックします。

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 アカウントに設定されている SSH キーの数を確認するには、**[SSH キー数 (SSH Key Count)]** フィールドの詳細を参照します。

ステップ 5 アカウントの SSH キーの詳細を表示するには、**[ローカル ユーザ管理 (Local User Management)]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 6 **[SSH キー (SSH Keys)]** ウィンドウで、次のプロパティを表示します。

名前	説明
[ID] フィールド	SSH キーの固有識別子です。

名前	説明
備考	ユーザ名とリモート サーバのホスト名。*username@hostname* の形式を使用します。
Key	特定のユーザに対して設定されている公開 SSH キーの詳細。

次のタスク

SSH キーを追加または変更します。

SSH キーの追加

始める前に

- すべてのユーザに SSH キーを追加するには、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。
- 管理者以外のユーザの場合は、自分のアカウントに対してのみ SSH キーを追加できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[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）]** タブをクリックします。

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 アカウントの SSH キーを追加するには、**[ローカル ユーザ管理 (Local User Management)]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 **[ID]** 列の近くにあるオプション ボタンのいずれかをクリックします。

ステップ 6 **[キーの追加 (Add Keys)]** アイコン (**SSH キー (SSH Keys)]** ウィンドウ) をクリックして、SSH キーを追加します。

ステップ 7 SSH キーを追加するには、次のオプション ボタンのいずれかを選択します。

a) **[SSH キーをペースト (Paste SSH key)]** を選択します。

ホストから公開 SSH キーをコピーし、テキスト フィールドにキーを貼り付けます。

b) **[ローカルからアップロード (Upload from local)]** を選択します。

[参照 (Browse)] をクリックし、追加する公開キー ファイルの場所に移動します。

c) **[リモートの場所からアップロード (Upload from remote location)]** を選択します。

次の詳細情報を入力して、リモート ロケーションから公開キーファイルをアップロードします。

名前	説明
[SSH キー ファイルのアップロード元 (Upload SSH key from)] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	SSH キーファイルが使用可能なサーバの IP アドレスまたはホスト名
[パスおよびファイル名（Path and Filename）] フィールド	公開 SSH キー ファイルの、リモート サーバ上でのパスとファイル名。

ステップ 8 **[SSH キーのアップロード (Upload SSH Key)]** をクリックします。

次のタスク

SSH キーを変更または削除します。

SSH キーの変更

始める前に

- すべてのユーザの SSH キーを変更するには、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。
- 管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを変更できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[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）]** タブをクリックします。

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 SSH キーを表示および変更するには、**[ローカル ユーザ管理（Local User Management）]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 SSH キーを変更するには、SSH キーのリストを確認し、**[SSH キー (SSH keys)]** ウィンドウで目的の行を選択します。

ステップ 6 **[キーの変更（Modifye Key）]** アイコンをクリックします。

ステップ 7 SSH キーを変更するには、次のオプション ボタンのいずれかを選択します。

a) **[SSH キーをペースト (Paste SSH key)]** を選択します。

アップデートされた公開 SSH キーをホストからコピーし、テキスト フィールドにキーをペーストします。

b) **[ローカルからアップロード (Upload from local)]** を選択します。

[参照 (Browse)] をクリックし、アップロードする、アップデートされた公開キー ファイルの場所に移動します。

c) **[リモートの場所からアップロード (Upload from remote location)]** を選択します。

次の詳細情報を入力して、アップデートされた公開キー ファイルをリモートの場所からアップロードします。

名前	説明
[SSH キー ファイルのアップロード元 (Upload SSH key from)] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	更新された SSH キーファイルが使用可能なサーバの IP アドレスまたはホスト名
[パスおよびファイル名（Path and Filename）] フィールド	アップデートされた公開 SSH キー ファイルの、リモート サーバ上でのパスとファイル名。

ステップ 8 **[SSH キーのアップロード (Upload SSH Key)]** をクリックします。

次のタスク

SSH キーを削除します。

SSH キーの削除

始める前に

- すべてのユーザの SSH キーを削除するには、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。
- 管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを削除できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[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）]** タブをクリックします。

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 ユーザアカウントの SSH キーを表示および削除するには、**[ローカル ユーザ管理（Local User Management）]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 SSH キーを削除するには、SSH キーのリストを確認し、**[SSH キー (SSH keys)]** ウィンドウで目的の行を選択します。

ステップ 6 **[キーの削除（Delete Key）]** アイコンをクリックします。

ポップアップ ウィンドウに *[*選択した *SSH* キーを削除しますか*? (Do you want to delete the selected SSH key?)]* というメッセージが表示されます。?

ステップ 7 **[はい (Yes)]** をクリックして削除を確認します。

非 IPMI ユーザー モード

リリース4.1 では、IPMI と非 IPMI の両方のユーザー モードを切り替えることができる**ユーザー モード**と呼ばれる新しいユーザー設定オプションが導入されています。非 IPMI ユーザー モードの導入では、ユーザー向けに強化されたパスワードセキュリティと、IPMI 2.0 標準による制約により以前のリリースで制限された BMC データベースに対してセキュリティ強化を提供し

ます。非 IPMI ユーザー モードでは、127 文字を使用してユーザー パスワードを設定できますが、IPMI モードのユーザーはパスワードの長さが 20 文字に制限されます。非 IPMI ユーザー モードでは、このモードで設定されたユーザーに対してより強力なパスワードを設定できます。

次の場合に、ユーザー モードの切り替え中に発生する次の設定変更を考慮する必要があります。

- 非 IPMI モードに切り替えると、IPMI 経由の IPMI はサポートされません。
- 非 IPMI から IPMI モードに切り替えて、すべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

  IPMI から非 IPMI モードに切り替えた場合、ユーザー データは影響を受けません。
- ファームウェアを 4.1 よりも低いバージョンにダウングレードします。ユーザー モードが非 IPMI の場合、はすべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

（注） 工場出荷時の初期状態にリセットすると、ユーザー モードは IPMI モードに戻ります。

IPMI と非 IPMI のユーザー モードの切り替え

注意 この手順を実行すると、SSH、KVM、Web サーバ、XML API、および REST API サービスが再起動されます。また、非 IPMI ユーザー モードに切り替えると、IPMI ユーザー サポートも削除されます。

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[管理 (Admin)]** タブの **[ユーザー管理 (User Management)]** をクリックします。

ステップ 3 **[IPMI ユーザー モードの無効化 (DISABLE Ipmi User mode)]** または **[IPMI ユーザー モードの有効化 (Enable IPMI User Mode)]** ボタンをクリックし、**[OK]** をクリックして確定します。

非管理者ユーザーとしてパスワードの変更

（注） このタスクを実行するには、まず管理者としてログインし、読み取り専用権限またはユーザー権限を持つユーザーを追加する必要があります。その場合にのみ、非管理者ユーザーとしてログインしてパスワードを変更できます。

手順

ステップ 1 管理者ユーザーとしてログインします。

ステップ 2 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 3 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 4 [ユーザー管理（User Management）] ペインの [ローカル ユーザー管理（Local User Management）] タブをクリックします。

ステップ 5 ローカル ユーザ アカウントを設定または追加するには、[ローカルユーザ管理（Local User Management）] ペインの行をクリックして、[ユーザの追加（Add User）] をクリックします。

ステップ 6 **[Add User]** ダイアログボックスで、読み取り専用またはユーザ権限をもつユーザを追加することで、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。
[ユーザ名（Username）] フィールド	ユーザーのユーザー名。 1 ～ 16 文字の範囲で入力します。

名前	説明
[割り当てられるロール（Role Played）] 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。 • [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。 • [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 の点灯・消灯（リモート作業者に場所を示す） • タイムゾーンの設定 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。 （注） パスワードを変更するには、[読み取り専用（）] または[ユーザー（User）] ロールを選択します。[管理者（admin）] ロールは選択しません。
[Enabled] チェックボックス	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[Change Password] チェックボックス	オンにすると、ユーザがパスワードを変更できるようになります。

名前	説明
[新しいパスワード（New Password）]	このユーザー名のパスワードを入力します。 **[Suggest]** ボタンをクリックして、使用するシステム生成パスワードを取得します。 このフィールドの横にあるヘルプ アイコン上にマウスを移動すると、パスワード設定に関する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。 IPMI 以外のユーザーの場合、パスワードの最大文字数は 127 文字です。 • パスワードにユーザー名を含めないこと。 • 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。 • 英大文字（A から Z まで）。 • 英小文字（a から z まで）。 • 10 進数の数字（0 ～ 9）。 • アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、'）。 これらのガイドラインは、セキュリティ上の理由でユーザーのための強力なパスワードを定義することを意図したものです。しかし、これらのガイドラインを無視して自分で選択したパスワードを設定するには、**[ローカル ユーザ管理（Local User Management）]** タブにある **[強力なパスワードを無効にする（Disable Strong Password）]** ボタンをクリックします。強力なパスワードのオプションが無効になっている場合にパスワードを設定する場合、1 文字以上、20 文字以下のものを使用できます。
[パスワードの確認（Confirm Password）] フィールド	確認のために繰り返して入力するパスワード。

ステップ 7 [Save Changes] をクリックします。

（注） パスワードを変更する場合、Cisco IMC からログアウトされます。

ステップ 8 読み取り専用またはユーザー権限をもつ新しいユーザを作成した後、管理者としてログアウトします。

ステップ 9 ここでは、読み取り専用で新しく作成したログインまたはユーザ ロール。**[Change Password (パスワードの作成)]**オプションは、**[Settings (設定)]**ドロップダウン メニューで右上隅で選択できます。

[Settings] アイコンをクリックすると、ドロップダウンには **[Change Password]** オプションがリストされます。このオプションは、非管理者ユーザとしてログインする場合にのみ表示されます。

ドロップダウン リストに [パスワードの変更（Change Password）] オプションが表示されない場合は、読み取り専用権限またはユーザ権限をもつ非管理者ユーザとしてログインします。

[Change Password] オプションを使用してパスワードを変更できます。パスワードを変更するとすぐに、非管理者ユーザーは自動的にログアウトし、新しいパスワードを使用してログインするように求められます。

パスワードの有効期限切れ

パスワードが期限切れになる有効期限を設定できます。管理者はこの期間を日単位で設定できます。この設定はすべてのユーザに対して共通です。パスワードが期限切れになると、ユーザに対してログイン時にこのことが通知され、パスワードをリセットするまでは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すると、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が消去され、データベースは空になります。つまり、データベースにはデフォルトのユーザ名「admin」とパスワード「password」が設定されます。サーバにはデフォルトのユーザ データベースが残るため、デフォルト クレデンシャル変更機能が有効になります。つまり、「admin」ユーザはダウングレード後にデータベースに初めてログインするときに、デフォルトのクレデンシャルを変更する必要があります。

パスワード設定時刻

既存のすべてのユーザの「パスワード設定時刻」は、移行またはアップグレードの実行時刻に設定されます。新しいユーザ（アップグレード後に作成されるユーザ）の場合、パスワード設定時刻はそのユーザが作成され、パスワードが設定された時刻に設定されます。ユーザ全般（新規および既存）について、パスワードが変更されるたびにパスワード設定時刻が更新されます。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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 [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
[パスワード有効期日を有効にする（Enable Password Expiry）] チェックボックス	このボックスをオンにすると、[パスワード有効期間（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。 （注） 管理者により一度設定されたパスワード有効期限は、その後に作成されるすべてのユーザに適用されます。
[Password History] フィールド	パスワードが入力された回数。このフィールドを有効にすると、指定された回数を超えてパスワードを繰り返し使用することができなくなります。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 日から 15 日までの値を入力します。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。

名前	説明
[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 日から 5 日までの値を入力します。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（User Password Expiry Policy configuration error）]** が表示されます。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 オプションで、**[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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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るので、有効期間を日数単位で設定できます。

次のタスク

パスワードの有効期間を設定します。

アカウントロックアウトの詳細の構成

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

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

ステップ 4 **[ローカル ユーザー管理（Local User Management）]** ウィンドウで、**[アカウント ロックアウトの詳細（Account Lockout Details）]** をクリックします。

ステップ 5 **[アカウント ロックアウト詳細（Account Lockout Details）]** ダイアログボックスで、次の手順を行います：

名前	説明
許可された試行（0 ～ 20）フィールド	**[ロックアウト期間]** で定義された期間中にロックアウトされるまでの、ユーザーの失敗したログイン試行の数。
ロックアウト期間 (0 ～ 60 分）フィールド	許可された試行の後、ユーザー アカウントがロックアウトされる時間（分単位）。
ロックアウト状態のユーザーを無効化 チェックボックス	ロックアウト状態でユーザー識別子を無効化します。

ユーザー認証の優先順位の構成

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

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

ステップ 4 **[ローカル ユーザー管理（Local User Management）]** ウィンドウで、**[ユーザー認証の優先順位の構成（Configure User Authentication Precedence）]** をクリックします。

ステップ 5 **[ユーザー認証の優先順位の構成（Configure User Authentication Precedence）]** ダイアログ ボックスで、優先順位を更新するデータベースを選択します。

ステップ 6 上矢印または下矢印を使用して、データベースの優先順位を変更します。

ユーザー クレデンシャルを工場出荷時の値にリセットする

⚠

注意 この手順を実行すると、現在の IP アドレス設定、NIC ポート設定、NIC 冗長性が失われる可能性があります。この手順を実行する前に、現在のサーバ設定をメモしておくことを推奨します。

始める前に

管理イーサネット ケーブルを専用管理ポートに差し込みます。

手順

ステップ 1 管理者ユーザとしてログインします。

ステップ 2 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 3 [Chassis] メニューの [Summary] をクリックします。

ステップ 4 ツールバーで、**[KVM の起動 (Launch KVM)]**をクリックします。

ステップ 5 または、[Navigation] ペインの [Compute] メニューをクリックします。

1. [Compute] メニューでサーバを選択します。
2. 作業ウィンドウの [Remote Management] タブをクリックします。
3. [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
4. **[仮想 KVM (Virtual KVM)]** タブで、**[HTML ベース KVM コンソールの起動 (Launch HTML based KVM console)]** をクリックします。

ステップ 6 **[電源 (Power)]** メニューから **[システムのリセット (Reset System)]** を選択します。

ステップ 7 プロンプトが表示されたら、**F8** を押して、Cisco IMC 設定ユーティリティを起動します。このユーティリティは、KVM コンソール ウィンドウで開きます。

ステップ 8 **[工場出荷時 (Factory Default)]** チェックボックスをオンにすると、サーバは出荷時の初期状態に戻ります。

ステップ 9 F5 を押して、行った設定に更新します。次の手順でサーバをリブートする前は、新しい設定が表示されメッセージ「**ネットワーク設定が構成されました**」が表示されるまでに約 45 秒かかる場合があります。

ステップ 10 F10 を押して設定を保存し、サーバを再起動します。

LDAP サーバー

Cisco IMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリ サービスがサポートされます。Cisco IMC は、ネットワークでディレクトリ情報を保管および保持する軽量ディレクトリ アクセス プロトコル（LDAP）をサポートします。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 ユーザー データベース内に見つからないユーザー アカウントに関するユーザー認証とロール許可は、LDAP サーバーによって実行されます。LDAP ユーザー認証の形式は username@domain.com です。

[LDAP 設定（LDAP Settings）] 領域の [暗号化の有効化（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。

LDAP サーバの設定

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 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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）] ペインで [LDAP] をクリックします。

ステップ 4 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 5 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	値
Common Name	**CiscoAVPair**
LDAP Display Name	**CiscoAVPair**
Unique X500 Object ID	**1.3.6.1.4.1.9.287247.1**
Description	**CiscoAVPair**
Syntax	**Case Sensitive String**

ステップ 6 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 [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) [Attributes] タブをクリックして、[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 7 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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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）] ペインで [LDAP] をクリックします。

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

名前	説明
[LDAP を有効にする（Enable LDAP）] 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、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 データベース内に見つからないユーザ アカウントの認証が行われます。
[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、ユーザーおよびグループのロード元を示します。 Active Directory サーバでは、**dc=domain,dc=com** の形式でなければなりません。
[ドメイン（Domain）]フィールド	すべてのユーザーが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバー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。
[Enable Secure LDAP] チェックボックス	オンにすると、サーバはセキュア LDAP を有効にし、LDAP CA 証明書をダウンロードするように求めます。LDAP CA 証明書のダウンロード方法については、LDAP CA 証明書のダウンロード （35 ページ） を参照してください。 既存のセキュア LDAP 証明書を削除するには、このオプションをオフにします。システム プロンプトに従って、削除を確認します。

名前	説明
[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ー（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。

（注） **[セキュア LDAP を有効化 (Enable Secure LDAP)]**チェックボックスをオンにする場合には、LDAP サーバのの完全修飾ドメイン名 (FQDN)を **[LDAP サーバ(LDAP Server)]** フィールドに入力します。LDAP サーバーの 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 サーバーの設定（Configure LDAP Servers）] 領域で、次のプロパティを更新します。

名前	説明
[事前設定の LDAP サーバ（Pre-Configure LDAP Servers）] オプション ボタン	これを選択すると、Active Directory は事前設定された LDAP サーバを使用します。
[LDAP サーバ（LDAP Servers）] フィールド	
[サーバー（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、サーバ 4、5、6 はグローバル カタログです。LDAP に Active Directory を使用していない場合は、最大で 6 つの LDAP サーバを設定できます。 （注） また、ホスト名の IP アドレスも指定できます。
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 ポートで行われます。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートで行われます。

名前	説明
[DNS を使用して LDAP サーバを設定する（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	
[Source] ドロップダウンリスト	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。次のいずれかを指定できます。 • **[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ことを指定します。 • **[設定済み（Configured）]**：設定された検索ドメインを使用することを指定します。 • **[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優先することを指定します。
[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。 **[抽出済み（Extracted）]** としてソースが指定されている場合、このフィールドは無効になります。
[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。 **[抽出済（Extracted）]** としてソースが指定されている場合、このフィールドは無効になります。

ステップ 6 [バインド パラメータ（Binding Parameters）] エリアで、次のプロパティを更新します。

名前	説明
[Method] ドロップダウンリスト	次のいずれかを指定できます。 • **[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で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）が照会されて、その DN が再バインディング プロセスで再利用されます。再バインド 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。 • **[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、ユーザー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ています。
[Binding DN]	ユーザーの識別名（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	ユーザーのパスワード。このフィールドは、バインディング方式として [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）] エリアで、次のプロパティを更新します。

名前	説明
[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している必要があります。 デフォルトでは、このフィールドに **sAMAccountName** と表示されます。
[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している必要があります。 デフォルトでは、このフィールドに **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 ユーザー 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）。
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。このパラメータでは、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）] エリアで、次のプロパティを更新します。

名前	説明
[LDAP Group Authorization] 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、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行われます。 このチェックボックスをオンにすると、Cisco IMC は **[Configure Group]** ボタンをイネーブルにします。
[Group Name] カラム	サーバへのアクセスが許可された LDAP サーバ データベース内のグループの名前。
[Group Domain] カラム	グループを所属させる LDAP サーバ ドメイン。

名前	説明
[Role] カラム	すべてのユーザーに割り当てられているこの LDAP サーバー グループのロール。次のいずれかになります。 • [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。 • [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 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
[Configure] ボタン	上にリストされている**グループ名**、**グループドメイン**、および**ロール**オプションが同じ Active directory グループの [**LDAP グループの設定 (Configure LDAP Group**)] ウィンドウを開きます。 設定が完了したら、**[変更の保存 (Save Changes)]** をクリックします。
[Delete] ボタン	既存の LDAP グループを削除します。

ステップ 9 [Save Changes] をクリックします。

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。リモートユーザー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、誰でもユーザー認証用のディレクトリ サーバー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。

LDAP クライアントには、暗号化 TLS/SSL 通信中にディレクトリ サーバ証明書を検証できる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)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

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

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

ステップ 4 [Certificate Status] 領域で、次のフィールドを確認します。

名前	説明
[Download Status]	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。
[Eport 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 [Navigation] ペインの [Admin] タブをクリックします。

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

ステップ 3 [ユーザー管理（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
[Export to Remote Location]	

名前	説明
	このオプションを選択すると、リモートロケーションの証明書を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 サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵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?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [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。 • [サーバー 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ーの 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 が使用するパスとファイル名。

名前	説明
	• **[ユーザ名（Username）]** フィールド—リモート サーバにログインするためにシステムが使用するユーザ名。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 サーバーのユーザー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。
[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

（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。デフォルトでは、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

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] メニューで、[User Management] をクリックします。
3. [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。
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。

   [Download LDAP CA Certificate] ダイアログボックスが表示されます。
5. **[LDAP CA 証明書のダウンロード (Download LDAP CA Certificate)]** ダイアログ ボックスで必要な情報を入力します。

名前	説明
[リモートの場所からのダウンロード/アップロード (DownloadUpload from remote location)] オプション ボタン	

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ダウンロード/アップロードできます。次の詳細を入力します。 • • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵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?*）*]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [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。 • [サーバー 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ーの IP アドレスまたはホスト名。[証明書のダウンロード元/アップロード元 (Download/Upload Certificate from)] ドロップダウン リストの設定によっては、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 — Cisco IMC がファイルをリモート サーバにダウンロード/アップロードするときに使用するパスおよびファイル名です。 • [Username] フィールド：システムがリモート サーバーにログインする際に使用するユーザー名。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 サーバーのユーザー名に対応するパスワード。このフィールドは、

名前	説明
	プロトコルが TFTP または HTTP の場合は適用されません。
[ブラウザクライアントを使用してダウンロード/アップロード (Download/Upload 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、インポートするファイルに移動するために使用できる [参照（Browse）] ボタンが表示されます。
[証明書の内容を貼り付け（Paste Certificate content）] オプション ボタン	このオプションを選択すると、署名付き証明書の内容全体をコピーして、[証明書の内容の貼り付け（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/アップロード (Download/Upload Certificate)] ボタン	証明書をサーバにダウンロード/アップロードできるようにします。

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） **[暗号化の有効化（Enable Encryption）]** チェックボックスと **[CA 証明書のバインドの有効化（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 サーバーの 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)]** ペインの **[管理者 (Admin)]** メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。
ステップ 3 [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。
ステップ 4 **[LDAP バインドのテスト（Test LDAP Binding）]** リンクをクリックします。

[LDAP CA 証明書バインドのテスト（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
[ユーザー名（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。

TACACS+ 認証

4.1（3b） リリース以降、Cisco IMC は Terminal Access Controller Access-Control System Plus（TACACS+）ユーザー認証をサポートします。Cisco IMC は、最大 6 つの TACACS+ リモート サーバーをサポートします。ユーザーが正常に認証されると、ユーザー名に **[（TACACS+）]** が追加されます。これは Cisco IMC インターフェースにも表示されます。

TACACS+ 認証のイネーブル化 （40 ページ） を参照して TACACS+ 認証を有効化します。
Cisco IMC はまた、TACACS+ リモート サーバーにアクセスできない場合のユーザー認証の優先順位もサポートします。ユーザー認証の優先順位の構成 （22 ページ） を使用してユーザー認証の優先順位の構成が行えます。

TACACS+サーバ設定

ユーザーの特権レベルは、そのユーザーに設定された **[cisco-av-pair]** 値に基づいて計算されます。TACACS+ サーバにー **[cisco-av-pair]** を作成する必要があります。ユーザーは既存の TACACS+ 属性は使用できません。

cisco-av-pair 属性のサポートされる 3 つのシンタックスは、次のとおりです。

- **`admin`** 特権の場合：**[cisco-av-pair=shell:roles=”admin”]**
- **`user`** 権限の場合：**[cisco-av-pair=shell:roles=”user”]**
- **`read-only`** 権限の場合：**[cisco-av-pair=shell:roles=”read-only”]**

必要に応じて、**[comma]** を区切り文字として使用して、さらにロールを追加できます。

（注） **[cisco-av-pair]** が TACACS+ サーバーで構成されていない場合、そのサーバーのユーザーには **[read-only]** 権限があります。

TACACS+ 認証のイネーブル化

始める前に

Terminal Access Controller Access-Control System（TACACS+）ベースのユーザー認証を構成する前に、ユーザーの特権レベルが **[cisco-av-pair]** 値に基づいて TACACS+ サーバーで構成されていることを確認してください。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[TACACS+]** タブをクリックします。

ステップ 4 **[TACACS+ のプロパティ（TACACS+ Properties）]** エリアで、次の手順を実行します。

名前	説明
[Enabled] チェックボックス	TACACS+ベースのユーザー認証を有効にするには、このボックスをオンにします。
[接続がない場合のみフォールバック（Fallback only on no connectivity）] チェック ボックス	オンにすると、Cisco IMC が構成済みの TACACS+ サーバーに接続できない場合にのみ、認証は次の優先順位データベースにフォールバックします。 ユーザ認証の優先順位の構成を確認します。ユーザー認証の優先順位の構成 （22 ページ）を参照してください。
タイムアウト（サーバーごと）：（5 ～ 30）秒（Timeout (for each server): (5 - 30) seconds）] フィールド	Cisco IMC が各 TACACS+ サーバーからの応答を待機する時間（秒単位）

TACACS+ リモート サーバー設定の構成

最大 6 つの TACACS+ リモート サーバーを設定できます。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[TACACS+]** タブをクリックします。

ステップ 4 **[サーバー リスト（Server List）]** エリアで、構成するサーバー識別子のラジオ ボタンをクリックし、**[編集（Edit）]** ボタンをクリックします。

ステップ 5 次のフィールドを更新します。

名前	説明
ID	これはサーバーの一意の識別子であり、ユーザーは編集できません。
IPアドレスまたはホスト名	TACACS+ サーバーが稼働している IP アドレス。
[ポート（Port）]	TACACS+ サーバーが稼働しているポート。
[サーバー キー（Server key）]	TACACS+サーバーで構成されているのと同じキー。 **[サーバー キーの確認（Confirm Server Key）]** に対して同じキーを繰り返します。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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）] ペインで [セッション管理（Session Management）] をクリックします。

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

名前	説明
[Session ID] カラム	セッションの固有識別情報。
BMC セッション ID	BMC セッションの識別子。
[User name (ユーザー名)] カラム	ユーザーのユーザー名。
[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、[N/A] と表示されます。

名前	説明
[Session Type] カラム	ユーザーがサーバー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。 • [Web GUI（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。 • [serial]：ユーザーがシリアル ポートを使用してサーバーに接続されていることを示します。 • **[XML API]** — ユーザーが XML API を使用してサーバーに接続していることを示します。 • **[Redfish]** — ユーザーが Redfish API を使用してサーバーに接続していることを示します。
[Action] カラム	このカラムには、SoL が有効である場合は [該当なし（N/A）] が表示され、SoL が無効である場合は [終了（Terminate）] が表示されます。Web UI で [終了（Terminate）] をクリックすると、セッションを終了できます。

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。