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 ユーザーの構成

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *usernumber*	ユーザー番号 *usernumber* に対するユーザー コマンド モードを開始します。
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	Cisco IMC でユーザー アカウントを有効または無効にします。
ステップ 3	Server /user # **set name** *username*	ユーザーのユーザー名を指定します。
ステップ 4	Server /user # **set role** {**readonly** |**user** |**admin**\\	ユーザーに割り当てるロールを指定します。ロールには、次のものがあります。 • readonly：このユーザーは情報を表示できますが、変更することはできません。 • user：このユーザーは、次の操作を実行できます。 • 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 ゾーンを設定する • IP アドレスを ping する • admin：このユーザーは、GUI、CLI、IPMI で可能なすべての処理を実行できます。
ステップ 5	Server /user # **set user-typeCIMC|SNMP|IPMI**	ユーザーに割り当てるユーザー タイプを指定します。1 人のユーザーに対して 1 つまたは複数のユーザー タイプを選択できます。

	コマンドまたはアクション	目的
ステップ 6	Server /user # **set password**	パスワードを 2 回入力するように求められます。 （注） 強力なパスワードを有効にすると、ガイドラインに従ってパスワードを設定する必要があります。 • 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ることはできません。 • 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（!、@、#、$、%、^、&、*、 強力なパスワードを無効にすると、1 ～ 20 文字の範囲で任意の文字（英数字、特殊文字または整数）を使用してパスワードを設定できます。
ステップ 7	Server /user # **set ipmi-password** *password*	IPMI ユーザー タイプのパスワードを設定します。
ステップ 8	Server /user # **set v3priv-proto***None*|*CFB128_AES128*	この値は、SNMP ユーザー タイプに設定します。

	コマンドまたはアクション	目的
ステップ 9	Server /user # **set v3proto***HMAC128_SHA224*| *HMAC192_SHA256*| *HMAC256_SHA384* |*HMAC384_SHA512* |*HMAC_SHA96* |*None*	この値は、SNMP ユーザー タイプに設定します。
ステップ 10	Server /user # **set v3priv-auth-key***Priv_Auth_key*	必要に応じてキーを設定します。
ステップ 11	Server /user # **set v3auth-key***Auth_key*	必要に応じてキーを設定します。
ステップ 12	Server /user # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、ユーザー 5 を 1 つの admin と 3 つすべてのユーザー タイプとして構成する例を示します。

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name UserName
Server /user *# set role readonly
Server /user *# set user-type CIMC,SNMP,IPMI
Server /user *# set password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 14 characters.
        The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
Please enter password:
Please confirm password:
Server /user *# set ipmi-password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 20 characters for IPMI
users and
maximum 127 characters for Non IPMI users.
        The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter ipmi-password:
Server /user *# set v3proto None
Server /user *# set v3priv-proto None
Server /user *# commit
```

ユーザーアカウントでの SSH キーの管理

SSH キーの設定

リリース 4.1.2 では、Cisco IMC はパスワード認証に加えて SSH RSA キーベースの認証を提供します。SSH キーは、認証に使用できる公開キーおよび秘密キーの RSA キー ペアのセットです。公開キーベースの認証は、パスワードベースの認証よりも強化されたセキュリティを提供します。

すべてのユーザーの SSH キーを構成するには、管理者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。管理者以外のユーザーの場合は、自分のアカウントにのみ認証してログインできる SSH キーを構成することができます。アカウントには、公開と秘密の SSH RSA キーペアを 1 つだけ構成できます。SSH キーは .pem または .pub フォーマットにする必要があります。

公開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。一部の C シリーズ サーバで使用可能な**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。

SSH キーの追加

始める前に

- すべてのユーザーの SSH キーを追加するには、管理者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。
- 管理者以外のユーザーの場合は、自分のアカウントの公開キーのみを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。ユーザーに構成されている SSH キーの数を確認するには、`[SSH キー数（SSH Key Count）]` フィールドを参照します。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。
ステップ 4	Server /user/ssh-keys # **add-key 1 remote**	このオプションを使用して、リモート サーバーから SSH キーを追加します。

	コマンドまたはアクション	目的
		次の詳細を入力します。 **1.** リモート サーバーに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP FTP SFTP SCP 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。 **2.** リモート サーバーのアドレスを指定します。 **3.** リモート ファイルのパスを指定します。 **4.** ユーザー名とパスワードを指定します。
ステップ 5	（任意） Server /user/ssh-keys # **add-key 2 paste**	このオプションを使用して、貼り付け方式で SSH キーを追加します。 SSH 公開キーを入力するためのダイアログを起動します。プロンプトが表示されたら、SSH キーのテキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押します。
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	アカウントに追加した公開 SSH キーを表示します。

例

1. この例では、リモート サーバーから SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 1 remote
```

```
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key added successfully
Server /user/ssh-keys #
```

2. この例では、貼り付け方式で SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key added successfully
Server /user/ssh-keys #
```

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ーの場合は、自分のアカウントの公開キーのみを変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。ユーザーに構成されている SSH キーの数を確認するには、[SSH キー数（SSH Key Count）] フィールドを参照します。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /user/ssh-keys # **modify-key 1 remote**	このオプションを使用して、リモート サーバーから変更されたキーを追加します。次の詳細を入力します。 **1.** リモート サーバーに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP FTP SFTP SCP 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。 **2.** リモート サーバーのアドレスを指定します。 **3.** リモート ファイルのパスを指定します。 **4.** ユーザー名とパスワードを指定します。
ステップ 5	（任意） Server /user/ssh-keys # **modify-key 2 paste**	このオプションを使用して、貼り付け方式で変更した SSH キーを追加します。 更新された公開 SSH キーを入力するためのダイアログを起動します。プロンプトが表示されたら、SSH キーのテキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押します。
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	アカウントで変更した更新済みの公開 SSH キーを表示します。

例

1. この例では、リモート サーバーから変更された SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 1 remote
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key modified successfully
Server /user/ssh-keys #
```

2. この例では、貼り付け方法によって変更された SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key modified successfully
Server /user/ssh-keys #
```

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ーの場合は、自分のアカウントの公開キーのみを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。`SSH Key Count` フィールドには、ユーザーに対して構成されている SSH キーの数が表示されます。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /user/ssh-keys # **delete-key 1**	続行しますか？というメッセージがプロンプト表示されます。[y/N] が表示されます。
ステップ 5	y を押して削除を確定します。	
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	更新されたユーザーの詳細と SSH キーの数を表示します。

例

この例では、SSH キーを削除します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # delete-key 1
This operation will delete the SSH key -
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
Do you wish to continue? [y/N]y
SSH Public key deleted successfully
Server /user/ssh-keys #
```

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 から非 IPMI へのユーザー モードの切り替え

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **scope user-mode**	ユーザー モード コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode non-ipmi**	IPMI 以外のユーザー モードに切り替えるには、確認プロンプトでyを入力します。
ステップ 4	Server /user-policy/user-mode * # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode non-ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable NON-IPMI based user mode.
         Converting to Non-IPMI User Mode disables IPMI Services and removes IPMI user
support.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
```

```
    User mode for IPMI accessibility: non-ipmi
Server /user-policy/user-mode #
```

非 IPMI から IPMI へのユーザー モードの切り替え

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **scope user-mode**	ユーザー モード コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode ipmi**	IPMI ユーザー モードに切り替えるには、確認プロンプトでyを入力します。 （注） IPMIユーザーモードに切り替えると、すべての UCS ユーザーが削除され、デフォルトのユーザー名とパスワードに戻ります。
ステップ 4	Server /user-policy/user-mode * # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable IPMI based user mode.
         Converting to IPMI User Mode deletes all UCS users and reverts to default
userid/password.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
```

```
    User mode for IPMI accessibility: ipmi
Server /user-policy/user-mode #
```

強力なパスワードの無効化

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。Cisco IMC の CLI では、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、[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

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **set password-policy** {**enabled** | **disabled**}	確認プロンプトで、**y** を入力してアクションを完了するか、または **n** を入力してアクションをキャンセルします。強力なパスワードを有効または無効にします。
ステップ 3	Server /user-policy # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # set password-policy disabled
Warning: Strong password policy is being disabled.
Do you wish to continue? [y/N] y
Server /user-policy *# commit
Server /user-policy #
```

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。

ユーザー認証の優先順位の構成

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user-policy**	TACACS+ コマンド モードを開始します。
ステップ 2	Server/user-policy # **set authentication-precedence** *User Database name*	ユーザー データベースのコンマ区切りリストを入力します。
ステップ 3	Server/user-policy # **commit**	

例

```
Server # scope user-policy
Server /user-policy # set authentication-precedence DB1,DB2
Server /user-policy* # commit
```

ユーザ パスワードのリセット

[パスワードの変更（Change Password）] オプションを使用してパスワードを変更できます。

（注）
- このオプションは、admin としてログインしているときには使用できません。読み取り専用の権限をもつ設定済みのユーザのパスワードだけが変更できます。
- パスワードを変更すると、Cisco IMC からログアウトされます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user** *user ID*	選択したユーザ コマンド モードを開始します。
ステップ 2	Server /chassis/user # **set password**	パスワードの要件の指示を読み、現在のパスワード、新しいパスワード、パスワードの確認をそれぞれのプロンプトで入力します。
ステップ 3	Server /chassis/user * # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、設定されているユーザのパスワードを変更する方法を示します。

```
Server # scope user 2
Server /chassis/user # set password
Warning:
Strong Password Policy is enabled!
For CIMC protection your password must meet the following requirements:
      The password must have a minimum of 8 and a maximum of 20 characters.
       The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter current password:Testabcd1
Please enter password: Testabcd2
Please confirm password: Testabcd2
Server /chassis/user * # commit
Server /chassis/user #
```

ユーザに対するパスワード期限切れの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **scope password-expiration**	パスワードの有効期限コマンド モードを開始します。
ステップ 3	Server /user-policy/password-expiration # **set password-expiry-duration** *0 ～ 3650* の整数	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 0 ～ 3650 日です。0 を入力すると、このオプションが無効になります。
ステップ 4	Server /user-policy/password-expiration * # **set notification-period** *0 ～ 15* の整数	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、このオプションが無効になります。
ステップ 5	Server /user-policy/password-expiration * # **set grace-period** *0 ～ 5* の整数	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、このオプションが無効になります。
ステップ 6	Server /user-policy/password-expiration * # **set password-history** *0 ～ 5* の整数	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、このオプションが無効になります。
ステップ 7	Server /user-policy/password-expiration *# **commit**	トランザクションをコミットします。
ステップ 8	（任意） Server /user-policy/password-expiration # **show detail**	パスワードの有効期限の詳細を表示します。
ステップ 9	（任意） Server /user-policy/password-expiration # **restore**	確認のプロンプトで、**yes** と入力してパスワード有効期限の設定をデフォルト値に復元します。

例

この例では、パスワードの有効期限を設定し、設定をデフォルト値に戻します。

```
Server # scope user-policy
Server /user-policy # scope password-expiration
Server /user-policy/password-expiration # set password-expiry-duration 5
Server /user-policy/password-expiration * # set notification-period 2
Server /user-policy/password-expiration *# set grace-period 1
Server /user-policy/password-expiration *# set password-history 4
Server /user-policy/password-expiration *# commit
Server /user-policy/password-expiration # show detail
Password expiration parameters:
 Valid password duration: 5
 Number of stored old passwords: 4
 Notification period: 2
 Grace period: 1
Server /user-policy/password-expiration #
Restoring the password expiry parameters to default values:
Server /user-policy/password-expiration # restoreAre you sure you want to restore
User password expiration parameters to defaults?
Please enter 'yes' to confirm:yes
Server /user-policy/password-expiration #
```

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。

サーバの Active Directory 設定で暗号化を有効にすると、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

The Cisco IMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

Important For more information about altering the schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

Note This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales.

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

Procedure

ステップ 1 Ensure that the LDAP schema snap-in is installed.

ステップ 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	Value
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 3 Add the CiscoAVPair attribute to the user class using the snap-in:

a) Expand the **Classes** node in the left pane and type `U` to select the user class.
b) Click the **Attributes** tab and click **Add**.
c) Type `C` to select the CiscoAVPair attribute.
d) Click **OK**.

ステップ 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

Role	CiscoAVPair Attribute Value
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

Note For more information about adding values to attributes, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to do next

Use the Cisco IMC to configure the LDAP server.

Cisco IMC での LDAP の設定

ローカル ユーザの認証と許可に LDAP サーバを使用するには、Cisco IMC で LDAP を設定します。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **set enabled** {**yes** |**no**\\	LDAP セキュリティをイネーブルまたはディセーブルにします。LDAPセキュリティがイネーブルの場合、ローカル ユーザーデータベースにないユーザー アカウントに対し、ユーザー認証とロール許可が LDAP によって実行されます。
ステップ 3	Server /ldap # **set domain***LDAP* ドメイン名	LDAP ドメイン名を指定します。
ステップ 4	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数を指定します。0 ～ 1800 秒の間隔を指定する必要があります。
ステップ 5	Server /ldap # **set base-dn** *domain-name*	LDAP サーバーで検索するベース DN を指定します。
ステップ 6	Server /ldap # **set attribute** 名	ユーザーのロールとロケール情報を保持する LDAP 属性を指定します。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

	コマンドまたはアクション	目的
		レコードで、この属性名と一致する値を検索します。 Cisco IMC ユーザのロールおよびロケールにマップされた既存の LDAP 属性を使用するか、CiscoAVPair 属性など、次の属性 ID を持つカスタム属性を作成できます。 `1.3.6.1.4.1.9.287247.1` （注） このプロパティを指定しない場合、ユーザーアクセスが拒否されます。
ステップ 7	Server /ldap # **set filter-attribute**	アカウント名属性を指定します。Active Directory を使用している場合は、このフィールドに **sAMAccountName** を指定します。
ステップ 8	Server /ldap # **scope secure**	セキュリティ LDAP モードを開始します。
ステップ 9	セキュア LDAP を有効にして、証明書をリモートでダウンロードするか、証明書を貼り付けます。	次のいずれかの操作を行います。 **1.** Server /ldap # **secure-ldap** *disabled|enabled paste tftp | ftp | sftp | scp | http* 証明書の内容を貼り付け るよう求められます。 **2.** 証明書の内容を貼り付けて **CTRL+D** キーを押します。 確認のプロンプトが表示されます。 **3.** 確認プロンプトで、**y** と入力します。 これにより LDAP CA 証明書のダウンロードが開始されます。 または **1.** Server /ldap # **secure-ldap** *disabled|enabled remote tftp | ftp | sftp | scp | http IP Address LDAP CA Certificate file*

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] 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。 **2.** 確認プロンプトで、**y** と入力します。 これにより LDAP CA 証明書のダウンロードが開始されます。
ステップ 10	Server /ldap # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 11	Server /ldap # **show** [**detail**]	（任意）LDAP の設定を表示します。

例

この例では、リモート ダウンロード オプションを使用して LDAP を構成します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled remote ftp xx.xx.xx.xx filename
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1282  100  1282    0     0   1247      0  0:00:01  0:00:01 --:--:--  1635
100  1282  100  1282    0     0   1239      0  0:00:01  0:00:01 --:--:--  1239
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is downloaded successfully
Server /ldap/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
Server /ldap #
```

この例では、証明書の貼り付けオプションを使用してセキュア LDAP を構成します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled ftp paste

 Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQttjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLGQBGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgs0T0JKUkEySkhC
UTEbMBkGA1UEAxMSV0lOLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNloX
DTIxMDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LGQBGRYLNE9CSlJBMkpIQlExGzAZBgNVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8OIY97w8lC/2S4qK46T+fnX13rXe8vvVHAO5wgPDVQTGS4nlF46A6Ba
FK+krKcIgFrQB1gnF74qs/ln1YtKHNBjrvg5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTuJAviVIrjSwU5j
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2pl0U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pE9BcM0rL9xKoIu6X0kSNEssoGnepFyNaH3t8vnMC
AwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FBAUulHTAWBT1OBz8IgAEzXsfcCsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBCwUAA4IBAQAzUMZr+0r1dWkVfFNBd7lu8tQbAEJf/A7PIKnJGNoUq8moAGs4
pMndoxdpNGZhYCWDWX3GWdeF1HqZHhb38gGQ9ylu0pIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xW3N665y4ePgUcUI7e/6aBGcGkGeUYodBPtExe28tQyeuYwD4Zj
nLuZKkT+I4PAYygVCqxDGsvfRHDpGneb3R+GeonOf4ED/0tn5PLSL9khb9qkHu/V
```

```
dO3/HmKVzUhloTDBuAMq/wES2WZAWhGr3hBc4nWQNjZWEMOKDpYZVK/GhBmNF+xi
eRcFqgh64oEmH9qAp0caGS1e7UyYaN+LtPRe
-----END CERTIFICATE-----
CTRL+D
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]
y

Server /ldap/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
Server /ldap #
```

次のタスク

グループ許可用にLDAPグループを使用する場合は、「*Cisco IMC* での *LDAP* グループの設定」を参照してください。

Cisco IMC での LDAP グループの設定

（注） Active Directory（AD）グループ許可をイネーブルにして設定すると、ローカル ユーザ データベースにないユーザや、Active Directory で Cisco IMC の使用を許可されていないユーザに対するグループ レベルでのユーザ認証も行われます。

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。
- Active Directory（または LDAP）をイネーブルにして、設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** |**no**}	LDAP グループ許可をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **scope role-group** *index*	設定に使用可能なグループ プロファイルのいずれかを選択します。ここで、*index* は 1 から 28 までの数字です。
ステップ 5	Server /ldap/role-group # **set name** *group-name*	サーバーへのアクセスが許可されているグループの名前を AD データベースに指定します。
ステップ 6	Server /ldap/role-group # **set domain** *domain-name*	グループが存在する必要がある AD ドメインを指定します。
ステップ 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループのすべてのユーザーに割り当てられる権限レベル（ロール）を指定します。次のいずれかになります。 • **admin**：ユーザーは使用可能なすべてのアクションを実行できます。 • **user**：ユーザーは、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） • **readonly**：ユーザーは情報を表示できますが、変更することはできません。
ステップ 8	Server /ldap/role-group # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、LDAP グループの許可を設定する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
1      (n/a)            (n/a)            admin
2      (n/a)            (n/a)            user
3      (n/a)            (n/a)            readonly
4      (n/a)            (n/a)            (n/a)
5      Training         example.com      readonly

Server /ldap/role-group #
```

LDAP グループでのネストされたグループの検索深度の設定

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ことができます。

- 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。
- Active Directory（または LDAP）をイネーブルにして、設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-search-depth** *value*	ネストされた LDAP グループの検索を有効にします。
ステップ 4	Server /ldap/role-group-rule # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、別の定義済みのグループ内にネストされた LDAP グループの検索を実行するために検索する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-search-depth 10
Server /ldap/role-group-rule* # commit
Server /ldap/role-group-rule # show detail
Group rules for LDAP:
    Group search attribute: memberOf
    Enable Group Authorization: yes
    Nested group search depth: 10
Server/ldap/ldap-group-rule #
```

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 （27 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 （14 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 **[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+ サーバーで設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope tacacs+**	TACACS+ コマンド モードを開始します。
ステップ 2	Server/tacacs+ # **set enabled** *yes*|*no*	
ステップ 3	Server/tacacs+ # **set fallback-only-on-no-connectivity** *yes*|*no*	**fallback-only-on-no-connectivity** を有効にする場合は、**Y** を入力して確認します。
ステップ 4	Server/tacacs+ # **set timeout** タイムアウト時間（秒）	5 ～ 30の値を入力してください
ステップ 5	Server/tacacs+ # **restore**	タイム アウトした場合に TACACS+ 構成をデフォルトに復元したい場合、**yes** と入力して確定してください。
ステップ 6	Server/tacacs+ # **commit**	システムで変更を保存します。

例

```
Server # scope tacacs+
Server /tacacs+ # set enabled yes
Server /tacacs+ # set fallback-only-on-no-connectivity yes

Warning: If TACACS+ and fallback option is enabled, then the fallback to the next
         precedence database happens only when CIMC is not able to connect to any
         of the configured TACACS+ servers.
Do you wish to continue? [y/N] y
Server /tacacs+ # set timeout 5
Server /tacacs+ # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+ # commit
```

TACACS+ リモート サーバー設定の構成

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope tacacs+**	TACACS+ コマンド モードを開始します。
ステップ 2	Server# **scope tacacs-server***Server Number*	TACACS サーバー コマンド モードを開始します。
ステップ 3	Server/tacacs+/tacacs-server # **set tacacs-port** *Port Number*	1 ～ 65535 の値を入力します。
ステップ 4	Server/tacacs+/tacacs-server # **set tacacs-key** *Server Key*	リモート TACACS+ サーバーで構成されているのと同じキーを入力します。
ステップ 5	Server/tacacs+/tacacs-server # **set tacacs-server** *Server IP Address*	リモート TACACS+ サーバーの IP アドレスを入力します。
ステップ 6	Server/tacacs+/tacacs-server # **restore**	タイム アウトした場合に TACACS+ 構成をデフォルトに復元したい場合、**[yes]** と入力して確定してください。

例

```
Server # scope tacacs+
Server # scope tacacs-server 1
Server /tacacs+/tacacs-server # set tacacs-port 6
Server /tacacs+/tacacs-server # set tacacs-key xxx
Server /tacacs+/tacacs-server # set tacacs-server xx.xx.xx.xx
Server /tacacs+/tacacs-server # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+/tacacs-server # commit
```

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 証明書のエクスポート

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **export-ca-certificate** *remote-protocol IP アドレス LDAP CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] 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。 証明書のエクスポートを開始します。

例

この例では、LDAP 証明書をエクスポートします。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate #  export-ca-certificate tftp 172.22.141.66 test.csv
 Initiating Export
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1262    0     0  100  1262      0   1244  0:00:01  0:00:01 --:--:--  1653
100  1262    0     0  100  1262      0   1237  0:00:01  0:00:01 --:--:--  1237
LDAP CA Certificate is exported successfully
Server /ldap/binding-certificate #
```

LDAP バインディングのテスト

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。

（注） [Enable Encryption] チェックボックスと [Enable Binding CA Certificate] チェックボックスをオンにする場合は、[LDAP Server] フィールドに LDAP サーバー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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **test-ldap-binding** ユーザ名	パスワードのプロンプトが表示されます。
ステップ 4	対応するパスワードを入力します。	ユーザを認証します。

例

次に、LDAP ユーザ バインドをテストする例を示します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # test-ldap-binding user
Password:
diagldapbinding: Authenticated by LDAP
User user authenticated successfully.
Server /ldap/binding-certificate #
```

LDAP CA 証明書の削除

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **delete-ca-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで LDAP CA 証明書が削除されます。

例

この例は、LDAP 証明書を削除します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # delete-ca-certificate
You are going to delete the LDAP CA Certificate.
 Are you sure you want to proceed and delete the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is deleted successfully
Server /ldap/binding-certificate #
```

ユーザ セッションの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザー セッションの情報を表示します。

コマンドの出力には、現在のユーザー セッションに関する次の情報が表示されます。

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。

例

次に、現在のユーザー セッションに関する情報を表示する例を示します。

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
15     admin            10.20.30.138      CLI          yes

Server /user #
```

ユーザー セッションの終了

始める前に

ユーザーセッションを終了するには、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

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザー セッションの情報を表示します。終了するユーザー セッションは、終了可能（killable）であり、独自のセッションではないことが必要です。
ステップ 2	Server /user-session # **scope user-session** セッション番号	終了する番号付きのユーザー セッションに対してユーザー セッション コマンド モードを開始します。
ステップ 3	Server /user-session # **terminate**	ユーザー セッションを終了します。

例

次に、ユーザー セッション 10 の admin がユーザー セッション 15 を終了する例を示します。

```
Server# show user-session
ID     Name              IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```

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。