リモート認証

認証サービス

Cisco UCS では、ユーザ ログインを認証するための次の 2 つの方法をサポートしています。

- ローカル ユーザ認証：ローカルの Cisco UCS Manager に存在するユーザ アカウントを使用します。
- リモート ユーザ認証：次のプロトコルのいずれかを使用します。
  - LDAP
  - RADIUS
  - TACACS+

リモート認証プロバイダに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダを作成して、Cisco UCS Manager がそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Manager にローカルに設定したり、リモート認証サーバに設定することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Manager GUIと Cisco UCS Manager CLIで表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Cisco UCS Manager で作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を Cisco UCS Manager で使用される名前と一致させることが必要です。ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

リモート認証プロバイダのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Cisco UCS Manager へのログインに使用する各リモート認証プロバイダに Cisco UCS 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

（注） この手順は、LDAP グループ マッピングを使用してロールとロケールを割り当てる LDAP 設定では必要ありません。

ユーザがログインすると、Cisco UCS Manager は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが有効である場合は、そのユーザに割り当てられているロールとロケールをチェックします。

次の表は、Cisco UCS でサポートしているリモート認証プロバイダのユーザ属性要件を比較したものです。

表 *1:* リモート認証プロバイダによるユーザ属性の比較

認証プロバイダ	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	グループ マッピング使用時は不要 グループ マッピング不使用時は任意	オプション。次のいずれかを実行するよう選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定する。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成する。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します サンプルの OID が次のセクションに示されています。
RADIUS	任意	オプション。次のいずれかを実行するよう選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用する。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成する。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザロールとロケールを指定する方法を示しています。 `shell:roles="admin,aaa"` `shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダ	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	必須です。スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。 `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。 cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコ デバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

Two-Factor Authentication

Cisco UCS Manager では、リモート ユーザのログインに二要素認証を使用して、アカウントのログインのセキュリティ レベルを高めています。二要素認証のログインでは、パスワード

フィールドでユーザ名、トークン、パスワードの組み合わせが必要です。PIN、証明書、またはトークンを指定できます。

二要素認証では、認証アプリケーションを使用します。このアプリケーションはトークン サーバを保持して、ログイン プロセス中にユーザ用のワンタイム トークンを生成し、パスワードを AAA サーバに保存します。ベンダー固有の属性を取得する要求がトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバが AAA サーバと統合されていることを想定するので、AAA サーバに要求を転送します。パスワードとトークンは、AAA サーバによって同時に検証されます。ユーザは、AAA サーバで設定されているのと同じ順序で、トークンとパスワードを入力する必要があります。

二要素認証は、RADIUS または TACACS+ プロバイダ グループを指定認証ドメインに関連付け、それらのドメインで二要素認証を有効にすることによってサポートされます。二要素認証では IPM をサポートしておらず、また認証レルムが LDAP、local、または none に設定されている場合はサポートされません。

Web セッションの更新および Web セッションのタイムアウト期限

[Web Session Refresh Period] は、Cisco UCS Manager GUI の Web セッションに対する更新要求間隔に許容される最大時間です。[Web Session Timeout] は、最後の更新要求後から Cisco UCS Manager GUI の Web セッションが非アクティブになるまでの最大経過時間です。

[Web Session Refresh Period] を 60 秒より長く、最大で 172800 秒まで長くすると、トークンとパスワードを繰り返し生成および再入力する必要があるセッション タイムアウトが頻繁に起きるのを避けることができます。デフォルト値は、二要素認証が有効の場合は 7200 秒、二要素認証が有効でない場合は 600 秒です。

[Web Session Timeout Period] には 300 から 172800 の間の値を指定できます。デフォルト値は、二要素認証が有効の場合は 8000 秒、二要素認証が有効でない場合は 7200 秒です。

LDAP プロバイダとグループ

ネストされた LDAP グループ

LDAP グループを別のグループのメンバーとして追加し、グループをネストすることで、グループ メンバーのアカウントを統合してレプリケーション トラフィックを削減できます。Cisco UCS Manager リリース 2.1(2) 以降では、LDAP グループ マップで定義されている別のグループに含まれるネストされた LDAP グループを検索できます。

（注） ネストされた LDAP の検索サポートは Microsoft Active Directory サーバに対してのみサポートされます。サポートされているバージョンは Microsoft Windows 2003 SP3、Microsoft Windows 2008 R2、および Microsoft Windows 2012 です。

デフォルトでは、LDAP グループを別のグループ内にネストするときにユーザ権限が継承されます。たとえば、Group_2 のメンバーとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバーと同じ権限が与えられます。その結果、Group_1 のメンバーであるユーザを検索するときは、LDAP グループ マップで Group_2 のみを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

Cisco UCS Manager のグループ マップでサブグループを常に作成する必要がなくなります。

LDAP グループ ルール

LDAP グループ ルールによって、ユーザ ロールおよびロケールをリモート ユーザに割り当てるときに Cisco UCS が LDAP グループを使用するかどうかが決まります。

LDAP プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **set attribute** *attribute*	指定された属性を含むレコードにデータベース検索を限定します。
ステップ 4	UCS-A /security/ldap # **set basedn** *distinguished-name*	指定された識別名を含むレコードにデータベース検索を限定します。
ステップ 5	UCS-A /security/ldap # **set filter** *filter*	指定されたフィルタを含むレコードにデータベース検索を限定します。
ステップ 6	（任意） UCS-A /security/ldap # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、LDAP サーバからの応答を待つ時間間隔を設定します。
ステップ 7	UCS-A /security/ldap # **commit-buffer**	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

次の例は、LDAP 属性を CiscoAvPair に、ベース識別名を「DC=cisco-ucsm-aaa3,DC=qalab,DC=com」に、フィルタを sAMAccountName=$userid、タイムアウト間隔を 5 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAvPair
UCS-A /security/ldap* # set basedn "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap* # set filter sAMAccountName=$userid
UCS-A /security/ldap* # set timeout 5
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

（注） ユーザ ログインは、LDAP ユーザの userdn が 255 文字を超えると失敗します。

次のタスク

LDAP プロバイダを作成します。

LDAP プロバイダの作成

Cisco UCS Manager は最大 16 の LDAP プロバイダをサポートします。

始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

- LDAP サーバで、次のいずれかの設定を行います。
  - LDAP グループを設定します。LDAP グループには、ユーザのロールとロケール情報が含まれています。
  - Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性について LDAP スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、CiscoAVPair 属性などのカスタム属性を作成します。

    シスコの LDAP の実装では、Unicode タイプの属性が必要です。

    CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します
  - クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インター

コネクトで障害が発生し、システムが2つ目のファブリックインターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager で使用される仮想 IPv4 または IPv6 アドレスからではありません。

- セキュア通信を使用するには、Cisco UCS Manager で LDAP サーバのルート認証局（CA）の証明書を含むトラスト ポイントを作成します。
- LDAP プロバイダを変更したり、追加または削除したりする必要がある場合は、ドメイン認証レルムをローカルに変更し、プロバイダに変更を加えた後、ドメイン認証レルムを LDAP に戻す必要があります。
- Active Directory バインド識別名の属性を定義する際に次の表にある特殊文字を使用する場合、対応する文字の 16 進数値の後にバックスラッシュ（\）を使用して、特殊文字をエスケープ文字で置き換える必要があります。

特殊文字	説明	16 進数値
,	カンマ	0x2C
+	プラス記号	0x2B
"	二重引用符	0x22
\	バックスラッシュ	0x5C
<	左角ブラケット	0x3C
>	右角ブラケット	0x3E
;	セミコロン	0x3B
LF	改行	0×0A
CR	復帰	0x0D
=	等号	0x3D
/	スラッシュ	0x2F

https://msdn.microsoft.com/en-us/library/aa366101 に特殊文字をエスケープ文字と 16 進数値に置き換える方法についての説明があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create server** *server-name*	LDAP サーバインスタンスを作成し、セキュリティ LDAP サーバモードを開始します。SSL が有効の場合、*server-name* は、通常 IP アドレスまたは FQDN となり、LDAP サーバのセキュリティ証明書内の Common Name（CN）と正確に一致している必要があります。IP アドレスが指定されている場合を除き、DNS サーバは Cisco UCS Manager で設定する必要があります。
ステップ 4	（任意） UCS-A /security/ldap/server # **set attribute** *attr-name*	ユーザロールとロケールの値を保管する 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 スキーマを拡張しない場合、既存の未使用 LDAP 属性を Cisco UCS ロールとロケールに設定できます。あるいは、属性 ID「**`1.3.6.1.4.1.9.287247.1`**」を持つ、CiscoAVPair という名前の属性をリモート認証サービスに作成できます。 デフォルトの属性が LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 5	（任意） UCS-A /security/ldap/server # **set basedn** *basedn-name*	リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から CN= username の長さを差し引いた長さに設定することができます。ここで、username は、LDAP 認証を使用して Cisco UCS Manager へアクセスしようとしているリモートユーザの識別に使用されます。

	コマンドまたはアクション	目的
		デフォルトのベース DN が LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 6	（任意） UCS-A /security/ldap/server # **set binddn** *binddn-name*	ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
ステップ 7	（任意） UCS-A /security/ldap/server # **set filter** *filter-value*	LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。 デフォルトのフィルタが LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 8	必須: UCS-A /security/ldap/server # **set password**	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。 パスワードを設定するには、 **set password** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 9	（任意） UCS-A /security/ldap/server # **set order** *order-num*	Cisco UCS でユーザーの認証にこのプロバイダを使用する順序。
ステップ 10	（任意） UCS-A /security/ldap/server # **set port** *port-num*	Cisco UCS が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。
ステップ 11	UCS-A /security/ldap/server # **set ssl** {**yes** **no**}	LDAP サーバと通信するときの暗号化の使用を有効または無効にします。オプションは次のとおりです。 • **yes** ：暗号化が必要です。暗号化をネゴシエートできない場合は、接続に失敗します。 有効にしている場合は、ポートを 636 に変更せず、389 のままにして

	コマンドまたはアクション	目的
		ください。Cisco UCS は、SSL 用のポート 636 で TLS セッションをネゴシエートしますが、初期接続は暗号化されない状態で 389 で開始されます。 • **no**：暗号化は無効です。認証情報はクリアテキストとして送信されます。 LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。
ステップ 12	UCS-A /security/ldap/server # **set timeout** *timeout-num*	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して LDAP の [General] で指定したタイムアウト値を使用します。デフォルトは 30 秒です。
ステップ 13	UCS-A /security/ldap/server # **set vendor** *{ms-ad | openldap}*	LDAP サーバのネストされた LDAP グループ検索機能の使用を有効または無効にします。オプションは次のとおりです。 • **ms-ad**：ネストされた LDAP グループ検索は、このオプションでサポートされます。ベンダーを *ms-ad*（Microsoft Active Directory）に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索できます。 • **openldap**：ネストされた LDAP グループ検索は、このオプションでサポートされません。ベンダーを *openldap* に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索しません。このオプションを選択すると、親グループがグループ マップにすでに設定されていても、Cisco

	コマンドまたはアクション	目的
		UCS Manager で LDAP グループマップとして各 LDAP サブグループを作成する必要があります。 （注） Cisco UCS Manager を旧バージョンからリリース 2.1(2) にアップグレードすると、LDAP プロバイダのベンダー属性は **openldap** にデフォルトで設定され、LDAP 認証が正常に機能し続けます。
ステップ 14	UCS-A /security/ldap/server # **commit-buffer**	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

次の例では、10.193.169.246 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 2
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 30
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次の例では、12:31:71:1231:45b1:0011:011:900 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 1
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
```

```
UCS-A /security/ldap/server* # set timeout 45
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次のタスク

単一のLDAPデータベースが関係する実装の場合、認証サービスとしてLDAPを選択します。

複数の LDAP データベースが関係する実装の場合は、LDAP プロバイダ グループを設定します。

LDAP プロバイダの LDAP グループ ルールの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **scope server** *ldap-provider*	セキュリティ LDAP プロバイダ モードを開始します。
ステップ 4	UCS-A /security/ldap/server # **scope ldap-group-rule**	LDAP グループ ルール モードを開始します。
ステップ 5	UCS-A /security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	ユーザ ロールとロケールをリモートユーザに割り当てるときに、Cisco UCS が LDAP グループを検索するかを指定します。 • **disable**：Cisco UCS はどの LDAP グループにもアクセスしません。 • **enable**：Cisco UCS はこの Cisco UCS ドメイン 内にマッピングされた LDAP プロバイダ グループを検索します。リモート ユーザが見つかると、Cisco UCS は関連する LDAP グループ マップでその LDAP グループに対して定義されているユーザ ロールとロケールを割り当てます。

	コマンドまたはアクション	目的
		（注） ロールとロケールの割り当ては累積されます。ユーザが複数のグループに含まれる、または LDAP 属性で指定されたロールやロケールがある場合、Cisco UCS はそのユーザに対し、それらのグループや属性のいずれかにマッピングされたすべてのロールとロケールを割り当てます。
ステップ 6	UCS-A /security/ldap/server/ldap-group-rule # **set member-of-attribute** *attr-name*	Cisco UCS が LDAP データベースのグループ メンバーシップを決定するのに使用する属性。 サポートされるストリングの長さは 63 文字です。デフォルトの文字列は「**`memberOf`**」です。
ステップ 7	UCS-A /security/ldap/server/ldap-group-rule # **set traversal** {**non-recursive** | **recursive**}	必要に応じて Cisco UCS がグループ メンバの親グループの設定を使用するかどうか指定します。ここに表示される値は次のとおりです。 • **non-recursive**：Cisco UCS はユーザが属するグループだけを検索します。 • **recursive**：Cisco UCS はユーザが属する継承元グループすべてを検索します。
ステップ 8	UCS-A /security/ldap/server/ldap-group-rule # **set use-primary-group** {**yes** | **no**}	プライマリ グループをメンバーシップの検証のために Cisco UCS ドメイン 内の LDAP グループ マップとして設定します。Cisco UCS Manager を有効にして、ユーザのプライマリ グループ メンバーシップをダウンロードして検証することができます。
ステップ 9	UCS-A /security/ldap/server/ldap-group-rule # **commit-buffer**	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

次の例は、権限を有効にするLDAPグループルールを設定し、属性のメンバをmemberOfに設定し、traversalをnon-recursiveに設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # scope server ldapprovider
UCS-A /security/ldap/server # scope ldap-group-rule
UCS-A /security/ldap/server/ldap-group-rule # set authorization enable
UCS-A /security/ldap/server/ldap-group-rule* # set member-of-attribute memberOf
UCS-A /security/ldap/server/ldap-group-rule* # set traversal non-recursive
UCS-A /security/ldap/server/ldap-group-rule* # set use-primary-group yes
UCS-A /security/ldap/server/ldap-group-rule* # commit-buffer
UCS-A /security/ldap/server/ldap-group-rule #
```

LDAP プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	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、ldap1という名前のLDAPサーバを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete server ldap1
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

LDAP グループ マッピング

LDAPグループマッピングを使用すると、LDAPユーザオブジェクトのロールまたはロケール情報を定義する必要がなくなります。LDAPデータベースへのアクセスを制限するLDAPグ

ループを使用している組織にログインする際、UCSM はグループ メンバーシップ情報を使用してロールとロケールを LDAP ユーザに割り当てます。

ユーザが Cisco UCS Manager にログインすると、LDAP グループ マップからそのユーザのロールとロケールに関する情報が取得されます。ロールとロケールの条件がポリシー内の情報と一致すれば、アクセス権が付与されます。リリース バージョンに応じて、Cisco UCS Manager では最大 28 個、128 個、または 160 個の LDAP グループ マップをサポートしています。

（注） Cisco UCS Manager リリース 3.1 (1) では最大 128 個の LDAP グループ マップ、リリース 3.1 (2) 以降では最大 160 個の LDAP グループ マップがサポートされます。

Cisco UCS Manager でローカルに構成したロールとロケールの定義が、LDAP ディレクトリの変更に応じて自動的に更新されることはありません。LDAP ディレクトリ内の LDAP グループを削除または名前変更するときには、その変更が反映されるよう Cisco UCS Manager も更新する必要があります。

LDAP グループ マップは、次のロールとロケールの組み合わせのいずれかを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケールの両方

たとえば、特定の場所のサーバ管理者グループを表す LDAP グループがあるとします。LDAP グループ マップには、サーバ プロファイルやサーバ機器などのユーザ ロールが含まれていることもあります。特定の場所のサーバ管理者へのアクセスを制限するために、ロケールに特定のサイト名を設定することができます。

（注） Cisco UCS Manager には、すぐに使用可能な多くのユーザ ロールが含まれていますが、ロケールは含まれていません。LDAP プロバイダ グループをロケールにマッピングするには、カスタム ロケールを作成する必要があります。

LDAP グループ マップの作成

始める前に

- LDAP サーバで LDAP グループを作成します。
- LDAP サーバで LDAP グループの識別名を設定します。
- Cisco UCS Manager でロケールを作成します（任意）。
- Cisco UCS Manager でカスタム ロールを作成します（任意）。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを作成します。 グループ DN の最大文字数は 240 です。 （注） このコマンドに特殊文字を入力する場合は、特殊文字の前にエスケープ文字 \\（バックスラッシュ 2 個）を付ける必要があります。
ステップ 4	UCS-A /security/ldap/ldap-group # **create locale** *locale-name*	指定されたロケールに LDAP グループをマッピングします。
ステップ 5	UCS-A /security/ldap/ldap-group # **create role** *role-name*	指定されたロールに LDAP グループをマッピングします。
ステップ 6	UCS-A /security/ldap/ldap-group # **commit-buffer**	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、DN に LDAP グループをマッピングし、ロケールを pacific に設定し、ロールを admin に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap/ldap-group* # create locale pacific
UCS-A /security/ldap/ldap-group* # create role admin
UCS-A /security/ldap/ldap-group* # commit-buffer
UCS-A /security/ldap/ldap-group #
```

次のタスク

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	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 マップを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダ

RADIUS プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS 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 3	（任意） UCS-A /security/radius # **set retries** *retry-num*	サーバをダウンとして通知する前にRADIUSサーバとの通信を再試行する回数を設定します。
ステップ 4	（任意） UCS-A /security/radius # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、RADIUSサーバからの応答を待つ時間間隔を設定します。
ステップ 5	UCS-A /security/radius # **commit-buffer**	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

次の例は、RADIUS リトライを 4 に設定し、タイムアウト間隔を 30 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # set retries 4
UCS-A /security/radius* # set timeout 30
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

次のタスク

RADIUS プロバイダを作成します。

RADIUS プロバイダの作成

Cisco UCS Manager は最大 16 の RADIUS プロバイダをサポートします。

始める前に

RADIUS サーバで、次の設定を行います。

- Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性について RADIUS スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の RADIUS 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、cisco-avpair 属性などのカスタム属性を作成します。

  シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。

  次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インターコネクトで障害が発生し、システムが 2 つ目のファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create server** *server-name*	RADIUS サーバインスタンスを作成し、セキュリティ RADIUS サーバ モードを開始します。
ステップ 4	（任意） UCS-A /security/radius/server # **set authport** *authport-num*	RADIUS サーバとの通信に使用するポートを指定します。
ステップ 5	UCS-A /security/radius/server # **set key**	RADIUS サーバ キーを設定します。キー値を設定するには、 **set key** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 6	（任意） UCS-A /security/radius/server # **set order** *order-num*	このサーバが試行される順序を指定します。
ステップ 7	（任意） UCS-A /security/radius/server # **set retries** *retry-num*	サーバをダウンとして通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
ステップ 8	（任意） UCS-A /security/radius/server # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。 ヒント RADIUS プロバイダに二要素認証を選択する場合は、より高い**タイムアウト値**を設定することを推奨します。
ステップ 9	UCS-A /security/radius/server # **commit-buffer**	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

次の例は、radiusserv7 という名前のサーバインスタンスを作成し、認証ポートを 5858 に設定し、キーを radiuskey321 に設定し、順序を 2 に設定し、再試行回数を 4 回に設定し、タイムアウトを 30 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create server radiusserv7
UCS-A /security/radius/server* # set authport 5858
UCS-A /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCS-A /security/radius/server* # set order 2
UCS-A /security/radius/server* # set retries 4
UCS-A /security/radius/server* # set timeout 30
UCS-A /security/radius/server* # commit-buffer
UCS-A /security/radius/server #
```

次のタスク

単一の RADIUS データベースが関係する実装の場合、RADIUS をプライマリ認証サービスとして選択します。

複数の RADIUS データベースが関係する実装の場合は、RADIUS プロバイダ グループを設定します。

RADIUS プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope RADIUS**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/radius # **commit-buffer**	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

次の例は、radius1 という RADIUS サーバを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete server radius1
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS+ プロバイダ

TACACS+ プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。
ステップ 3	（任意） UCS-A /security/tacacs # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	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

次の例は、TACACS+ タイムアウト間隔を 45 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

次のタスク

TACACS+ プロバイダを作成します。

TACACS+ プロバイダの作成

Cisco UCS Manager は最大 16 の TACACS+ プロバイダをサポートします。

始める前に

TACACS+ サーバで、次の設定を行います。

- cisco-av-pair 属性を作成します。既存の TACACS+ 属性は使用できません。

  cisco-av-pair 名は、TACACS+ プロバイダの属性 ID を提供する文字列です。

  次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インターコネクトで障害が発生し、システムが 2 つ目のファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create server** *server-name*	TACACS+ サーバ インスタンスを作成し、セキュリティ TACACS+ サーバモードを開始します
ステップ 4	（任意） UCS-A /security/tacacs/server # **set key**	TACACS+ サーバ キーを設定します。キー値を設定するには、 **set key** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 5	（任意） UCS-A /security/tacacs/server # **set order** *order-num*	このサーバが試行される順序を指定します。
ステップ 6	（任意） UCS-A /security/tacacs/server # **set timeout***seconds*	システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。

	コマンドまたはアクション	目的
		ヒント　TACACS+ プロバイダに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。
ステップ 7	UCS-A /security/tacacs/server # **set port** *port-num*	TACACS+ サーバとの通信に使用するポートを指定します。
ステップ 8	UCS-A /security/tacacs/server # **commit-buffer**	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

次の例は、tacacsserv680 という名前のサーバインスタンスを作成し、キーを tacacskey321 に設定してそのキーを確認し、順序を 4 に設定し、認証ポートを 5859 に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create server tacacsserv680
UCS-A /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set order 4
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
UCS-A /security/tacacs/server #
```

次のタスク

単一の TACACS+ データベースが関係する実装の場合、TACACS+ をプライマリ認証サービスとして選択します。

複数の TACACS+ データベースが関係する実装の場合は、TACACS+ プロバイダ グループを設定します。

TACACS+ プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS 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 3	UCS-A /security/tacacs # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	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

次の例は、tacacs1 という TACACS サーバを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete server TACACS1
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

マルチ認証システムの設定

マルチ認証サービス

次の機能の実装により、Cisco UCS が複数の認証サービスを使用するよう設定することができます。

- プロバイダ グループ
- 認証ドメイン

プロバイダ グループと認証ドメインを Cisco UCS Manager で構成した後、構文 **ucs:***auth-domain* \ *user-name* を使用すると、Cisco UCS Manager CLI を使ってシステムにログインできます。

リモート認証サービスで複数の認証ドメインとネイティブ認証が設定されている場合は、次のいずれかの構文例を使用して SSH、Telnet または Putty でログインします。

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

  ssh ucs-example\\jsmith@192.0.20.11

  ssh ucs-example\\jsmith@2001::1

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

  ssh -l ucs-example\\jsmith 192.0.20.11

```
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

Linux 端末からは以下の Telnet を使用します。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントから：

- **ucs-***auth-domain**username* でログインします。

```
Login as: ucs-example\jsmith
```

（注） デフォルトの認証がローカルに設定され、コンソール認証がLDAPに設定されている場合は、**ucs-local\admin**（admin はローカル アカウント名）を使用して Putty クライアントからファブリック インターコネクトにログインできます。

マルチ認証システムの設定

プロバイダ グループ

プロバイダ グループは、認証プロセス中に Cisco UCS がアクセスするプロバイダのセットです。プロバイダ グループ内のすべてのプロバイダが、ユーザの認証にCisco UCS プロバイダが使用する順にアクセスされます。設定されたすべてのサーバが使用できない場合、または到達不能な場合、Cisco UCS Manager は、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

Cisco UCS Manager では、最大 16 のプロバイダ グループを作成でき、グループごとに最大 8 つのプロバイダを含めることができます。

LDAP プロバイダ グループの作成

LDAP プロバイダ グループを作成すると、複数の LDAP データベースを使用して認証できます。

始める前に

1 つ以上の LDAP プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create auth-server-group** *auth-server-group-name*	LDAP プロバイダ グループを作成し、認証サーバ グループの LDAP セキュリティ モードを開始します。
ステップ 4	UCS-A /security/ldap/auth-server-group # **create server-ref** *ldap-provider-name*	指定された LDAP プロバイダを LDAP プロバイダ グループに追加し、サーバ参照認証サーバ グループの LDAP セキュリティ モードを開始します。
ステップ 5	UCS-A /security/ldap/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/ldap/auth-server-group/server-ref # **commit-buffer**	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

次の例は、ldapgroup という名前の LDAP プロバイダ グループを作成し、プロバイダ グループに ldap1 および ldap2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create auth-server-group ldapgroup
UCS-A /security/ldap/auth-server-group* # create server-ref ldap1
```

```
UCS-A /security/ldap/auth-server-group/server-ref* # set order 1
UCS-A /security/ldap/auth-server-group/server-ref* # up
UCS-A /security/ldap/auth-server-group* # create server-ref ldap2
UCS-A /security/ldap/auth-server-group/server-ref* # set order 2
UCS-A /security/ldap/auth-server-group/server-ref* # commit-buffer
UCS-A /security/ldap/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

LDAP プロバイダ グループの削除

始める前に

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete auth-server-group** *auth-server-group-name*	LDAP プロバイダ グループを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	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、ldapgroup という名前の LDAP プロバイダ グループを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete auth-server-group ldapgroup
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダ グループの作成

RADIUS プロバイダ グループを作成すると、複数の RADIUS データベースを使用して認証できます。

始める前に

1 つ以上の RADIUS プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create auth-server-group** *auth-server-group-name*	RADIUS プロバイダ グループを作成し、認証サーバ グループの RADIUS セキュリティ モードを開始します。
ステップ 4	UCS-A /security/RADIUS/auth-server-group # **create server-ref** *radius-provider-name*	指定された RADIUS プロバイダを RADIUS プロバイダ グループに追加し、サーバ参照認証サーバ グループの RADIUS セキュリティ モードを開始します。
ステップ 5	UCS-A /security/radius/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/radius/auth-server-group/server-ref # **commit-buffer**	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

次の例は、radiusgroup という名前の RADIUS プロバイダ グループを作成し、プロバイダ グループに radius1 と radius2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create auth-server-group radiusgroup
UCS-A /security/radius/auth-server-group* # create server-ref radius1
UCS-A /security/radius/auth-server-group/server-ref* # set order 1
UCS-A /security/radius/auth-server-group/server-ref* # up
UCS-A /security/radius/auth-server-group* # create server-ref radius2
UCS-A /security/radius/auth-server-group/server-ref* # set order 2
UCS-A /security/radius/auth-server-group/server-ref* # commit-buffer
UCS-A /security/radius/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

RADIUS プロバイダ グループの削除

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete auth-server-group** *auth-server-group-name*	RADIUS プロバイダ グループを削除します。
ステップ 4	UCS-A /security/radius # **commit-buffer**	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

次の例は、radiusgroup という RADIUS プロバイダ グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete auth-server-group radiusgroup
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS プロバイダ グループの作成

TACACS+ プロバイダ グループを作成すると、複数の TACACS+ データベースを使用して認証できます。

始める前に

TACACS プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create auth-server-group** *auth-server-group-name*	TACACS プロバイダ グループを作成し、認証サーバグループのセキュリティ TACACS モードを開始します。
ステップ 4	UCS-A /security/tacacs/auth-server-group # **create server-ref** *tacacs-provider-name*	指定した TACACS プロバイダを TACACS プロバイダ グループに追加し、サーバ参照認証サーバ グループ セキュリティ TACACS モードを開始します。
ステップ 5	UCS-A /security/tacacs/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/tacacs/auth-server-group/server-ref # **commit-buffer**	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

次の例は、tacacsgroup という名前の TACACS プロバイダ グループを作成し、プロバイダ グループに tacacs1 と tacacs2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create auth-server-group tacacsgroup
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs1
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 1
UCS-A /security/tacacs/auth-server-group/server-ref* # up
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs2
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 2
UCS-A /security/tacacs/auth-server-group/server-ref* # commit-buffer
UCS-A /security/tacacs/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

TACACS プロバイダ グループの削除

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **delete auth-server-group** *auth-server-group-name*	TACACS プロバイダ グループを削除します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	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

次の例は、tacacsgroup という TACACS プロバイダ グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete auth-server-group tacacsgroup
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

認証ドメイン

Cisco UCS Manager では、複数の認証システムを活用するために認証ドメインを使用しています。各認証ドメインはログイン時に指定および設定できます。これを行わない場合、Cisco UCS Manager はデフォルトの認証サービス設定を使用します。

最大 8 個の認証ドメインを作成できます。各認証ドメインは、Cisco UCS Manager 内のプロバイダ グループと領域に関連付けられています。プロバイダ グループを指定しないと、Cisco UCS Manager では領域内のすべてのサーバを使用します。

認証ドメインの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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 2	UCS-A /security # **create auth-domain** *domain-name*	認証ドメインを作成し、認証ドメインモードを開始します。 （注） リモート認証プロトコルを使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、ローカルに作成されたユーザ名に対して32文字の制限が適用されます。Cisco UCS ではフォーマット用に 5 文字が挿入されるため、ドメイン名とユーザ名の合計が27文字を超える場合には認証が失敗します。
ステップ 3	（任意） UCS-A /security/auth-domain # **set refresh-period** *seconds*	Web クライアントが Cisco UCS Manager に接続する際は、Web セッションをアクティブ状態に維持するために、クライアントは Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションを強制終了することはしません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は600秒、二要素認証が有効の場合は 7200 秒です。 （注） [Web Session Refresh Period] に設定する秒数は、[Web Session Timeout] に設定する秒数未満である必要があります。[Web Session Refresh Period] に [Web Session Timeout] と同じ値を設定しないでください。
ステップ 4	（任意） UCS-A /security/auth-domain # **set session-timeout** *seconds*	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。こ

	コマンドまたはアクション	目的
		の時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、**セッションの更新**時間および**セッションのタイムアウト**時間を増やすことを検討してください。
ステップ 5	（任意） UCS-A /security/auth-domain # **create default-auth**	認証ドメインのデフォルト認証を作成します。
ステップ 6	（任意） UCS-A /security/auth-domain/default-auth # **set auth-server-group** *auth-serv-group-name*	認証ドメインのプロバイダ グループを設定します。
ステップ 7	UCS-A /security/auth-domain/default-auth # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	認証ドメインのレルムを設定します。
ステップ 8	（任意） UCS-A /security/auth-domain/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 9	UCS-A /security/auth-domain/default-auth # **commit-buffer**	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

次の例では、Web の更新時間が 3600 秒（1 時間）およびセッションのタイムアウト時間が 14400 秒（4 時間）の domain1 と呼ばれる認証ドメインを作成します。次に、radius1 でプロバイダを使用するように domain1 を設定し、レルム タイプを radius に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create auth-domain domain1
```

```
UCS-A /security/auth-domain* # set refresh-period 3600
UCS-A /security/auth-domain* # set session-timeout 14400
UCS-A /security/auth-domain* # create default-auth
UCS-A /security/auth-domain/auth-domain* # set auth-server-group radius1
UCS-A /security/auth-domain/auth-domain* # set realm radius
UCS-A /security/auth-domain/auth-domain* # set user-2-factor yes
UCS-A /security/auth-domain/auth-domain* # commit-buffer
UCS-A /security/auth-domain/auth-domain #
```

プライマリ認証サービス

コンソール認証サービスの選択

始める前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダを作成します。Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダを作成する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope console-auth**	コンソール認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/console-auth # **set realm** *auth-type*	コンソール認証を指定します。*auth-type* 引数は次のいずれかのキーワードです。 • **ldap** ：LDAP 認証を指定します。 • **local** ：ローカル認証を指定します。 • **none** ：ローカル ユーザはパスワードを指定せずにログインできます。 • **radius** ：RADIUS 認証を指定します。 • **tacacs** ：TACACS+ 認証を指定します。
ステップ 4	（任意） UCS-A /security/console-auth # **set auth-server-group** *auth-serv-group-name*	関連付けられたプロバイダ グループ（存在する場合）。

	コマンドまたはアクション	目的
ステップ 5	（任意） UCS-A /security/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 6	UCS-A /security/console-auth # **commit-buffer**	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

次の例では、認証レルムを TACACS+ に設定し、コンソール認証プロバイダ グループを provider1 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope console-auth
UCS-A /security/console-auth # set realm tacacs
UCS-A /security/console-auth # set auth-server-group provider1
UCS-A /security/console-auth* # set use-2-factor yes
UCS-A /security/console-auth* # commit-buffer
UCS-A /security/console-auth #
```

デフォルト認証サービスの選択

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope default-auth**	デフォルト認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/default-auth # **set realm** *auth-type*	デフォルト認証を指定します。*auth-type* は次のキーワードのいずれかです。 • **ldap**：LDAP 認証を指定します。 • **local**：ローカル認証を指定します。 • **none**：ローカル ユーザはパスワードを指定せずにログインできます。 • **radius**：RADIUS 認証を指定します。

	コマンドまたはアクション	目的
		• **tacacs**：TACACS+ 認証を指定します。
ステップ 4	（任意） UCS-A /security/default-auth # **set auth-server-group** *auth-serv-group-name*	関連付けられたプロバイダグループ（存在する場合）。
ステップ 5	（任意） UCS-A /security/default-auth # **set refresh-period** *seconds*	Web クライアントが Cisco UCS Manager に接続する際は、Web セッションをアクティブ状態に維持するために、クライアントは Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションを強制終了することはしません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 600 秒、二要素認証が有効の場合は 7200 秒です。
ステップ 6	（任意） UCS-A /security/default-auth # **set session-timeout** *seconds*	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、**セッションの更新**時間および**セッションのタイムアウト**時間を増やすことを検討してください。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /security/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 8	UCS-A /security/default-auth # **commit-buffer**	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

次の例では、デフォルトの認証を RADIUS に設定し、デフォルトの認証プロバイダ グループを provider1 に設定し、二要素認証を有効にし、更新間隔を 7200 秒（2 時間）に設定し、セッションのタイムアウト間隔を 28800 秒（8 時間）に設定し、二要素認証を有効にします。そして、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope default-auth
UCS-A /security/default-auth # set realm radius
UCS-A /security/default-auth* # set auth-server-group provider1
UCS-A /security/default-auth* # set use-2-factor yes
UCS-A /security/default-auth* # set refresh-period 7200
UCS-A /security/default-auth* # set session-timeout 28800
UCS-A /security/default-auth* # commit-buffer
UCS-A /security/default-auth #
```

リモート ユーザのロール ポリシー

デフォルトでは、Cisco UCS Manager でユーザ ロールが設定されていない場合は、LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Cisco UCS Manager にログインしているすべてのユーザに読み取り専用アクセス権が付与されます。セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致するユーザへのアクセスを制限するのが望ましい場合があります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限しません。その他のユーザ ロールが Cisco UCS Manager で定義されていない限り、読み取り専用アクセス権がすべてのユーザに付与されます。

これはデフォルトの動作です。

no-login

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限します。リモート認証システムにユーザ ロールが割り当てられていない場合、アクセスは拒否されます。

リモート ユーザのロール ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **set remote-user default-role** {**assign-default-role** | **no-login**}	ユーザ ロールに基づいて Cisco UCS Manager へのアクセスが制限されるかどうかを指定します。
ステップ 3	UCS-A /security # **commit-buffer**	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

次の例では、リモートユーザのロールポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # set remote-user default-role assign-default-role
UCS-A /security* # commit-buffer
UCS-A /security #
```