CHAPTER 3

ユーザ ロールおよび共通ロールの設定

Cisco MDS 9000 ファミリのすべてのスイッチで、Command Line Interface（CLI; コマンドライン インターフェイス）および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）に共通のロールを使用します。SNMP を使用して作成したロールは CLI を使用して変更でき、その逆も可能です。

ユーザ、パスワード、ロールは CLI ユーザおよび SNMP ユーザ全員が同じものを使用します。CLI を利用して設定したユーザは SNMP を利用して（たとえば Fabric Manager や Device Manager）、スイッチにアクセスできますし、その逆も可能です。

この章の内容は、次のとおりです。

ロール ベースの許可

Cisco MDS 9000 ファミリ スイッチはロールに基づいた認証を行います。ロールベースの許可は、ユーザにロールを割り当てることによってスイッチへのアクセスを制限します。この種類の認証では、ユーザに割り当てられたロールに基づいて管理操作が制限されます。

コマンドを実行したり、コマンドを完了させたり、コンテキスト ヘルプを取得したりする場合に、コマンドへのアクセス権限があれば、操作を継続できます。

ここで説明する内容は、次のとおりです。

ロールについて

ロールごとに複数のユーザを含めることができ、各ユーザは複数のロールに所属できます。たとえば、role1 ユーザにはコンフィギュレーション用コマンドへのアクセスだけが、role2 ユーザには debug コマンドへのアクセスだけが許可されているとします。この場合、role1 と role2 の両方に所属しているユーザは、コンフィギュレーション用コマンドと debug コマンドの両方にアクセスできます。

（注） ユーザが複数のロールに所属している場合、各ロールで許可されているすべてのコマンドを実行できます。コマンドへのアクセス権は、そのコマンドへのアクセス拒否よりも優先されます。たとえば、TechDocs グループに属しているユーザが、コンフィギュレーション コマンドへのアクセスを拒否されているとします。ただし、このユーザはエンジニアリング グループにも属していて、コンフィギュレーション コマンドへのアクセス権を持っています。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

ヒント ロールを作成した時点で、必要なコマンドへのアクセスが即時に許可されるわけではありません。管理者が各ロールに適切なルールを設定し、必要なコマンドへのアクセスを許可する必要があります。

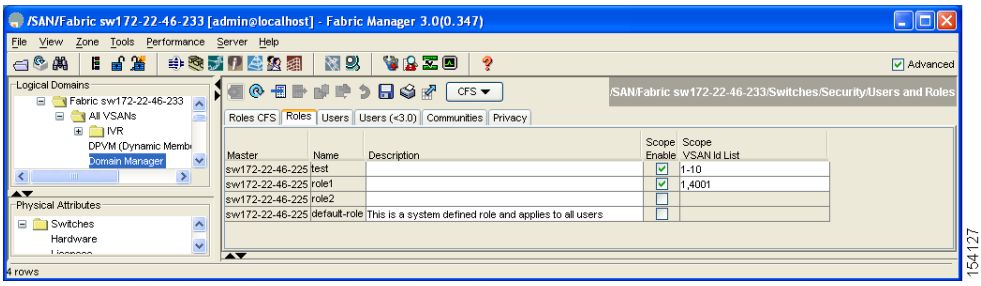
ロールとプロファイルの設定

Fabric Manager を使用して追加のロールを作成する、または既存ロールのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

図 3-1 のとおりの情報が表示されます。

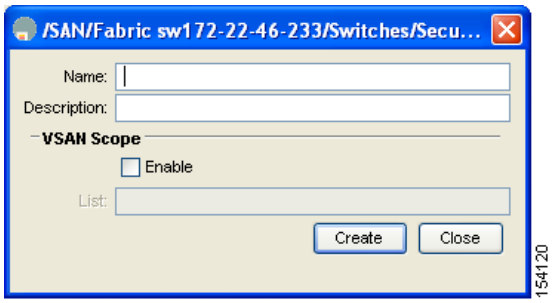
図 3-1　[Users and Roles] 画面の [Roles] タブ



ステップ 2　Fabric Manager でロールを作成するために [Create Row] アイコンをクリックします。

図 3-2 の [Create Roles] ダイアログボックスが表示されます。

図 3-2　[Create Roles] ダイアログボックス



ステップ 3　ロールの設定先のスイッチを選択します。

ステップ 4　[Name] フィールドに、ロールの名前を入力します。

ステップ 5　[Description] フィールドにロールの説明を入力します。

ステップ 6　（任意）[Enable] チェックボックスをオンにして Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）範囲をイネーブルにし、このロールを適用できる VSAN のリストを [Scope] フィールドに入力します。

ステップ 7　ロールを作成するには、[Create] ボタンをクリックします。共通ロールを作成せずに [Roles - Create] ダイアログボックスを閉じるには、[Close] ボタンをクリックします。

（注）　Device Manager では、スイッチのビューを表示するために、Device Manager に必要な 6 つのロールが自動的に作成されます。作成されるロールは、**system**、**snmp**、**module**、**interface**、**hardware**、および **environment** です。

共通ロールの削除

Fabric Manager を使用して共通ロールを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　削除するロールをクリックします。

ステップ 3　[Delete Row] アイコンをクリックして共通ロールを削除します。

ステップ 4　[Yes] をクリックして削除を確認するか、[No] でキャンセルします。

VSAN ポリシーの概要

VSAN ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください）。

選択した VSAN セットだけにタスクの実行が許可されるように、ロールを設定できます。デフォルトでは、どのロールの VSAN ポリシーも許可されるため、すべての VSAN に対してタスクが実行されます。選択した VSAN セットだけにタスクの実行が許可されるロールを設定できます。1 つのロールに対して選択的に VSAN を許可するには、VSAN ポリシーを拒否に設定し、そのあとでその設定を許可に設定、または適切な VSAN に設定します。

（注） VSAN ポリシーが拒否に設定されているロールに設定されているユーザは、E ポートの設定を変更できません。これらのユーザが変更できるのは、（ルールの内容に応じて）F ポートまたは FL ポートの設定だけです。これにより、これらのユーザが、ファブリックのコア テクノロジーに影響する可能性のある設定を変更できなくなります。

ヒント ロールを使用して、VSAN 管理者を作成できます。設定したルールに応じて、これらの VSAN 管理者は他の VSAN に影響を与えることなく、VSAN に MDS 機能（ゾーン、fcdomain、VSAN プロパティなど）を設定できます。また、ロールが複数の VSAN での処理を許可している場合、VSAN 管理者はこれらの VSAN 間で F ポートまたは FL ポートのメンバーシップを変更できます。

VSAN ポリシーが拒否に設定されているロールに属すユーザのことを、VSAN 制限付きユーザと呼びます。

VSAN ポリシーの変更

Fabric Manager で既存のロールの VSAN ポリシーを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　[Scope Enable] チェックボックスをオンにして、VSAN 範囲をイネーブルにし、ロールの VSAN 範囲を制限します。

ステップ 3　[Scope VSAN Id List] フィールドに、ロールを制限する VSAN のリストを入力します。

ステップ 4　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

各ロールに対するルールと機能の設定

各ロールに、最大 16 のルールを設定できます。これらのルールは、許可される CLI コマンドを反映します。ユーザ側で指定するルール番号によって、ルールが適用される順序が決まります。たとえば、rule 1 のあとに rule 2 が適用され、rule 3 以降が順に適用されます。network-admin ロールに属さないユーザは、ロールに関連したコマンドを実行できません。

たとえば、ユーザ A がすべての **show** CLI コマンドの実行を許可されている場合、ユーザ A が network-admin ロールに所属していないかぎり、ユーザ A は **show role** CLI コマンドの出力を表示できません。

ルールは、特定のロールにより実行できる操作を指定します。ルールを構成する要素は、ルール番号、ルール タイプ（許可または拒否）、CLI コマンド タイプ（たとえば **config**、**clear**、**show**、**exec**、**debug**）、および任意の機能名（たとえば FSPF、zone、VSAN、fcping、interface など）です。

（注）　この場合、**exec** CLI コマンドでは、**show**、**debug** および **clear** の各 CLI コマンドのカテゴリに入らない、EXEC モード内のすべてのコマンドが対象になります。

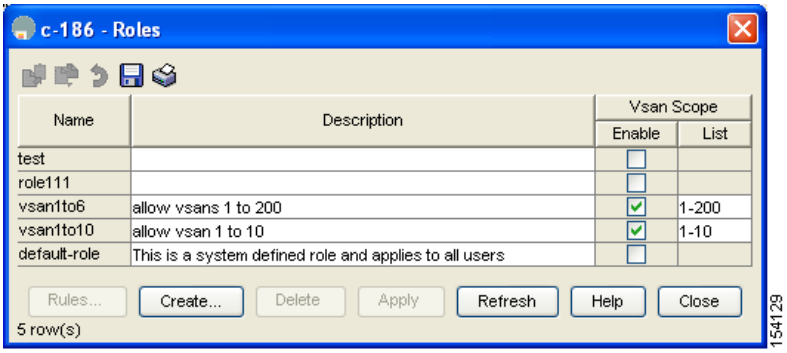
ルールの修正

Device Manager で既存のロールのルールを修正する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] をクリックします。

ステップ 2　[Common Roles] ダイアログボックスが表示されます（図 3-3 を参照）。

図 3-3　Device Manager の [Common Roles] ダイアログボックス

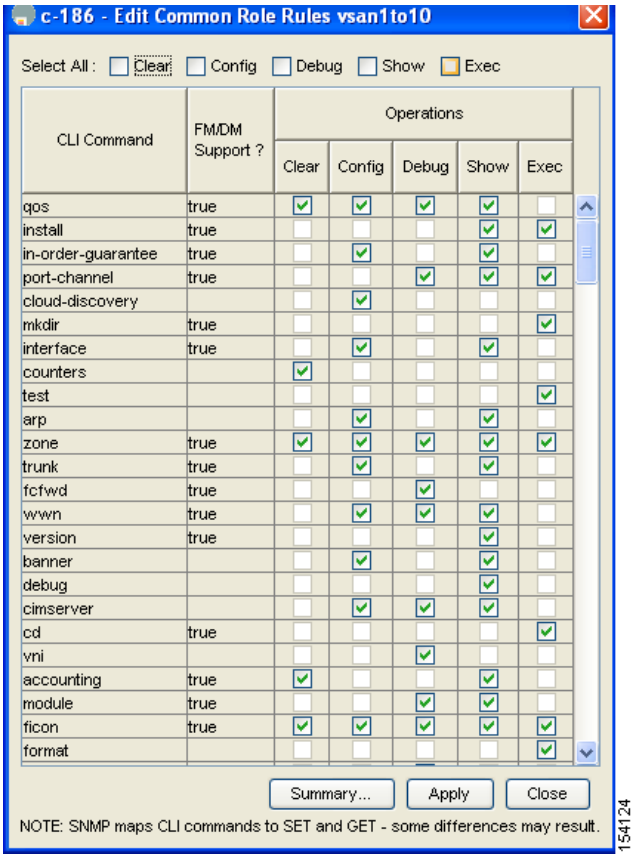


ステップ 3　ルールを編集するロールをクリックします。

ステップ 4　[Rules] ボタンをクリックして、そのロールのルールを表示します。

[Rules] ダイアログボックスが表示されます（図 3-4 を参照）。表示されるまでに数分かかる場合があります。

図 3-4　[Edit Common Role Rules] ダイアログボックス



ステップ 5　共通ロールについて、イネーブルまたはディセーブルにするルールを編集します。

ステップ 6　新しいルールを適用するには、[Apply] ボタンをクリックして [Rules] ダイアログボックスを閉じます。ルールを適用せずに [Rules] ダイアログボックスを閉じるには、[Close] ボタンをクリックします。

rule 1 が最初に適用され、たとえば sangroup ユーザがすべての **config** CLI コマンドにアクセスすることが許可されます。次に rule 2 が適用され、sangroup ユーザには FSPF 設定が拒否されます。結果として、sangroup ユーザは **fspf** CLI 設定コマンドを除く、他のすべての **config** CLI コマンドを実行できます。

（注）　ルールは適用する順序が重要です。これらの 2 つのルールを入れ替え、**deny config feature fspf** ルールを最初に置き、次に **permit config** ルールを置いた場合は、2 番めのルールがグローバルに効果を持って最初のルールに優先するため、sangroup ユーザの全員にすべての設定コマンドの実行を許可することになります。

ロールベース情報の表示

ルールはルール番号別、およびそれぞれのロールに基づいて表示されます。ロール名を指定しない場合は、すべてのロールが表示されます。

Device Manager を使用して特定のロールのルールを表示する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] をクリックします。

[Roles] ダイアログボックスが表示されます。

ステップ 2　ロール名を選択して [Rules] ボタンをクリックします。

[Rules] ダイアログボックスが表示されます。

ステップ 3　このロールに設定されたルールをまとめて表示するには [Summary] ボタンをクリックします。

ロールの配布

ロールベース設定は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的なデータベース管理を可能にし、ファブリック全体に対するシングル ポイントでの設定を提供します（第 7 章「CFS インフラストラクチャの使用」を参照）。

次の設定内容が配布されます。

- ロール名と説明
- ロールに対するルールのリスト
- VSAN ポリシーと許可されている VSAN のリスト

ここで説明する内容は、次のとおりです。

ロール データベースについて

ロールベース設定は 2 つのデータベースを利用して設定内容の受け取りと実装を行います。

- コンフィギュレーション データベース：ファブリックで現在実行されているランニング データベースです。

- ペンディング データベース：直後の設定変更はペンディング データベースに保存されます。設定を修正した場合は、ペンディング データベースの変更内容をコミットまたは廃棄する必要があります。この処理の実行中は、ファブリックはロックされた状態になります。ペンディング データベースへの変更は、その変更をコミットするまでコンフィギュレーション データベースに反映されません。

ファブリックのロック

データベースを修正する最初のアクションがペンディング データベースを作成し、ファブリック全体の機能をロックします。ファブリックがロックされると、次のような状況になります。

- 他のユーザは、この機能の設定を変更できなくなります。
- 最初の変更にともなって、コンフィギュレーション データベースの複製がペンディング データベースになります。

変更のコミット

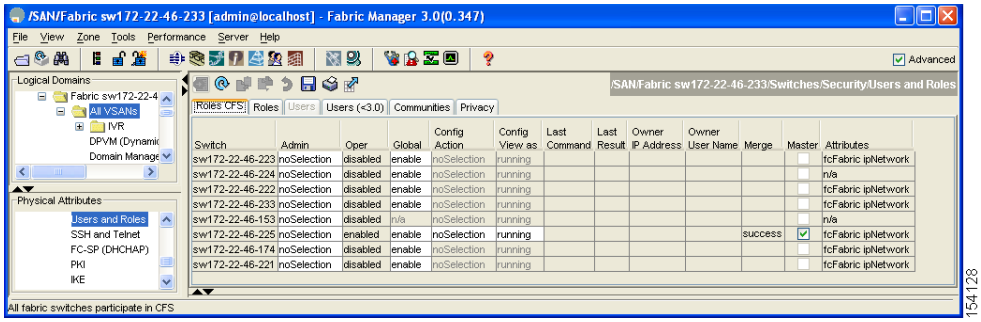
ペンディング データベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、ペンディング データベースは消去されます。

Fabric Manager を使用してロールベース設定変更をコミットする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

図 3-5 のような画面が表示されます。

図 3-5　[Roles CFS] タブ



ステップ 2　[Global] ドロップダウン メニューを [enable] に設定して CFS をイネーブルにします。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ステップ 4　[Config Action] ドロップダウン メニューを [commit] に設定して、CFS を使用してこのロールをコミットします。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

変更の廃棄

ペンディング データベースに行った変更を廃棄（abort）すると、コンフィギュレーション データベースは影響を受けず、ロックが解除されます。

Fabric Manager を使用してロールベース設定変更を廃棄する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Config Action] ドロップダウン メニューを [abort] に設定して、コミットされていないすべての変更を廃棄します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

配信のイネーブル化

Fabric Manager を使用してロールベース設定の配布をイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Global] ドロップダウン メニューを [enable] に設定して CFS 配布をイネーブルにします。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

セッションの消去

Fabric Manager を使用して強制的にファブリック内の既存のロール セッションを消去する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Config Action] ドロップダウン メニューを [clear] に設定して、ペンディング データベースを消去します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（注）　セッションを消去すると、ペンディング データベース内のすべての変更が失われます。

データベース マージに関する注意事項

ファブリックのマージではスイッチ上のロール データベースは変更されません。2 つのファブリックをマージし、それらのファブリックが異なるロール データベースを持つ場合は、ソフトウェアがアラート メッセージを発します。

- ファブリック全体のすべてのスイッチでロール データベースが同一であることを確認します。
- いずれのスイッチのロール データベースも、必ず必要なデータベースに編集してからコミットします。これによりファブリック内のすべてのスイッチ上のロール データベースの同期が保たれます。

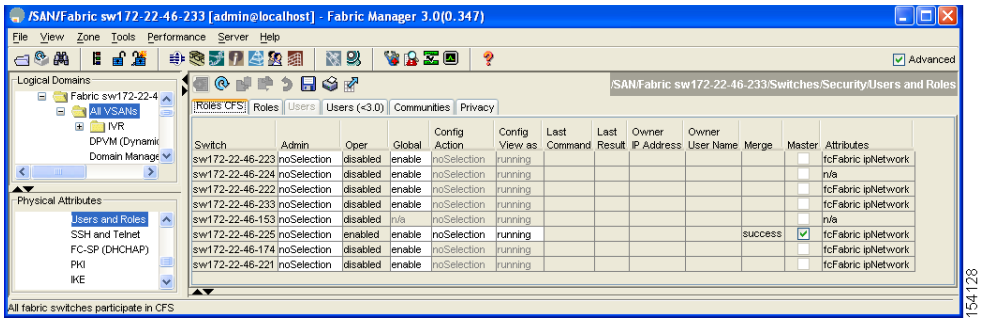
配布がイネーブルのときのロールの表示

ロールに対して配布がイネーブルのときは、ペンディング ロール データベース（配布される前のデータベース）かランニング データベースのいずれかを表示できます。

Fabric Manager を使用してロールを表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします（図 3-6 を参照）。

図 3-6　[Roles CFS] タブ



ステップ 2　[Config View AS] ドロップダウン メニューを [pending] に設定してペンディング データベースを表示するか、[Config View] ドロップダウン メニューを [running] に設定してランニング データベースを表示します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ユーザ アカウント

Cisco MDS 9000 ファミリ スイッチでは、すべてのユーザのアカウント情報がシステムに保管されます。ユーザの認証情報、ユーザ名、ユーザ パスワード、パスワードの有効期限、およびロール メンバーシップが、そのユーザのユーザ プロファイルに保存されます。

この章で説明するタスクを利用すると、ユーザの作成と既存ユーザのプロファイルの修正が行えます。これらのタスクはアドミニストレータにより定義された特権ユーザに制限されます。

次の条件を備えた強力なパスワードを設定する必要があります。

- 最低 8 文字の長さ
- 論理の一貫した文字が多数続かない（「abcd」など）
- 同じ文字が多数連続しない（「aaabbb」など）
- 辞書にある単語を含まない
- 大文字と小文字の両方が含まれている
- 数字が含まれている

強いパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注） クリア テキストのパスワードに含めることができるのは、アルファベットと数字だけです。ドル記号（$）やパーセント記号（%）などの特殊文字は使用できません。

ここで説明する内容は、次のとおりです。

- 「ユーザの作成に関する注意事項」（P.3-11）
- 「ユーザの設定」（P.3-12）
- 「ユーザの削除」（P.3-14）
- 「ユーザ アカウント情報の表示」（P.3-14）

ユーザの作成に関する注意事項

snmp-server user オプションで指定したパスフレーズと **username** オプションで指定したパスワードは同期されます。

デフォルトでは、明示的に期限を指定しないかぎりユーザ アカウントは無期限に有効になります。オプション **expire** を使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。日付は YYYY-MM-DD 形式で指定します。

ユーザを作成する際、次の点に注意してください。

- 次のワードは予約済みのため、ユーザ設定には使用できません。bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、sys
- ユーザ パスワードはスイッチ コンフィギュレーション ファイルに表示されません。
- パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードは大文字と小文字を区別します。Cisco MDS 9000 ファミリ スイッチでは、デフォルトのパスワードとして「admin」が使われることはなくなりました。強いパスワードを明確に設定する必要があります。

注意 注意：Cisco MDS NX-OS では、ユーザ名がアルファベットで始まる限り、リモートで作成するか（Terminal Access Controller Access Control device Plus [TACACS+] または Remote Access Dial-In User Service [RADIUS] を使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+ [プラス]、= [等号]、_ [下線]、- [ハイフン]、\ [バックスラッシュ]、および . [ピリオド]）を

使って作成したユーザ名がサポートされます。ローカル ユーザ名をすべて数字で作成したり、特殊文字（上記の特殊文字を除く）を使用して作成したりすることはできません。数字だけのユーザ名やサポートされていない特殊文字によるユーザ名が Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバに存在し、ログイン時に入力されると、そのユーザはアクセスを拒否されます。

ユーザの設定

Fabric Manager を使用して新しいユーザを設定する、または既存ユーザのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します（図 3-7 を参照）。

図 3-7　[Users] タブの下に表示されるユーザのリスト

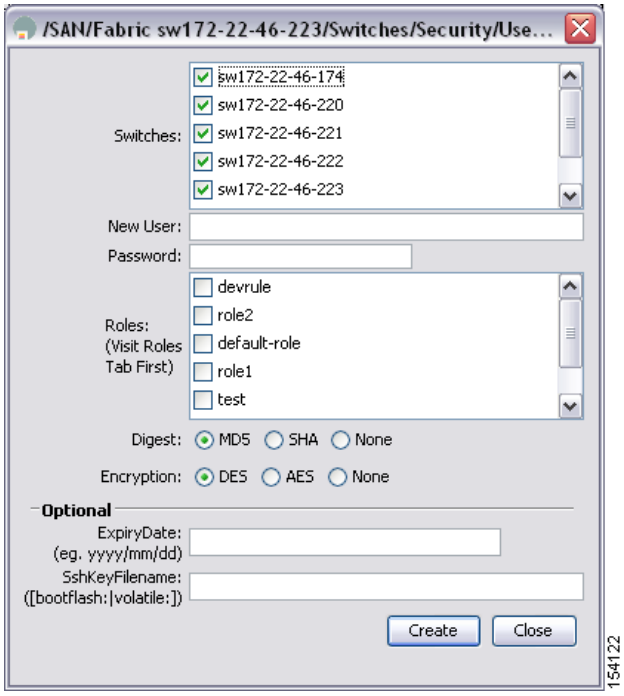
Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

ステップ 2　[Create Row] アイコンをクリックします。

[Create Users] ダイアログボックスが表示されます（図 3-8 を参照）。

図 3-8　[Create Users] ダイアログボックス



ステップ 3　（任意）[Switches] チェックボックスを変更して 1 つ以上のスイッチを指定することもできます。

ステップ 4　[New User] フィールドにユーザ名を入力します。

ステップ 5　[Role] ドロップダウン メニューからロールを選択します。ドロップダウン メニューから選択しない場合、新しいロール名をフィールドに入力することもできます。この場合には、前の手順に戻り、ロールを適切に設定します（「ユーザ アカウント」（P.3-10）を参照）。

ステップ 6　[New Password] フィールドにユーザのパスワードを入力します。[Confirm Password] フィールドに同一の新しいパスワードを入力します。

ステップ 7　[Privacy] チェックボックスをオンにしてパスワード フィールドに入力し、管理トラフィックを暗号化します。

ステップ 8　エントリを作成するには、[Create] ボタンをクリックします。変更内容を保存せずにダイアログボックスを閉じるには、[Close] ボタンをクリックします。

Fabric Manager を使用した管理者パスワードの変更

Fabric Manager で管理者パスワードを変更する手順は、次のとおりです。

ステップ 1　コントロール パネルの [Open] タブをクリックします。

ステップ 2　パスワード フィールドを選択して、ファブリックの既存ユーザのパスワードを変更します。

ステップ 3　[Open] ボタンをクリックして、ファブリックに接続します。

（注）　ファブリックに接続した後に、新しいパスワードが保存されます。ユーザ名とパスワードのフィールドは、ファブリックの接続を解除した後に限り、[Fabric] タブで編集できます。

ユーザの削除

Fabric Manager を使用してユーザを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します。

ステップ 2　削除するユーザの名前をクリックします。

ステップ 3　[Delete Row] アイコンをクリックして選択したユーザを削除します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ユーザ アカウント情報の表示

Fabric Manager を使用して、設定したユーザ アカウントの情報を表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Users] タブをクリックします。に示す SNMP ユーザのリストが [Information] ペインに表示されます（図 3-9 を参照）。

図 3-9　[Users] タブの下に表示されるユーザのリスト

Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

SSH サービス

Cisco MDS 9000 ファミリのすべてのスイッチでは、Telnet サービスはデフォルトでイネーブルになります。Secure Shell（SSH; セキュア シェル）サービスを有効にする場合は、事前にサーバ キー ペアを生成してください（「SSH サーバ キー ペアの生成」（P.3-16）を参照）。

ここで説明する内容は、次のとおりです。

SSH について

SSH は Cisco NX-OS CLI にセキュアなコミュニケーションを提供します。次の SSH オプションに対する SSH キーを使用できます。

- SSH1
- Rivest, Shamir, Adelman（RSA）を使用する SSH2
- Digital System Algrorithm（DSA）を使用する SSH2

SSH サーバ キー ペアの概要

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用中の SSH クライアント バージョンに従って、SSH サーバ キー ペアを生成します。各キー ペアに指定するビット数の範囲は、768 ～ 2048 です。

SSH サービスでは、SSH バージョン 1 および 2 で使用するキー ペア タイプを 3 つの中から選択できます。

- **rsa1** オプションを使用すると、SSH バージョン 1 プロトコルに対応する RSA1 キー ペアが生成されます。
- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キー ペアが生成されます。
- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キー ペアが生成されます。

注意　SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

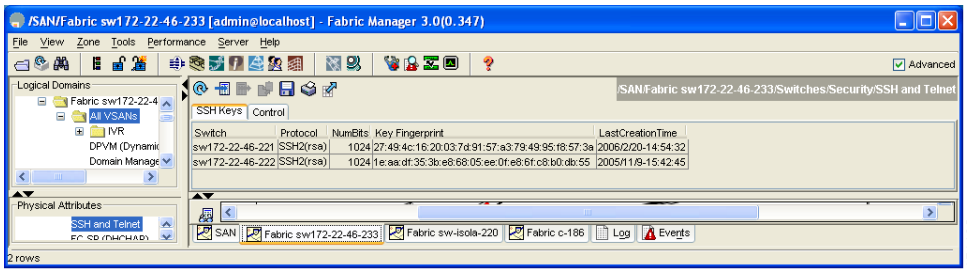
SSH サーバ キー ペアの生成

SSH サーバ キー ペア を生成する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

図 3-10 に示す設定が [Information] ペインに表示されます。

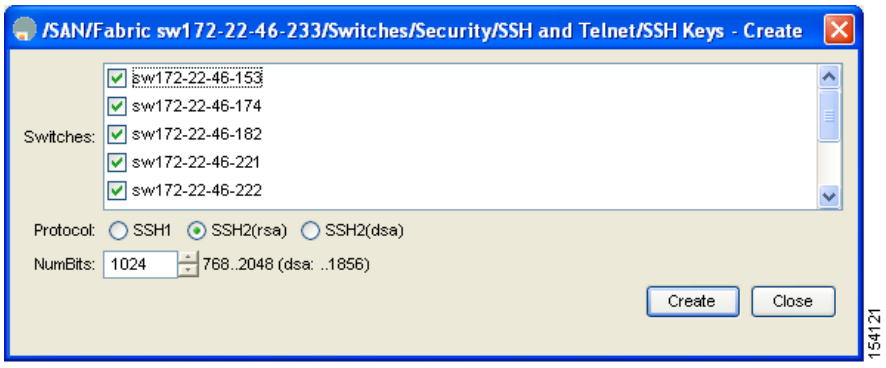
図 3-10　SSH および Telnet の設定



ステップ 2　[Create Row] アイコンをクリックします。

図 3-11 で示す [SSH and Telnet Key - Create] ダイアログボックスが表示されます。

図 3-11　[Create SSH and Telnet] ダイアログ ボックス



ステップ 3　この SSH キー ペアに割り当てるスイッチにチェックを入れます。

ステップ 4　表示された [Protocols] リストからキー ペアのオプション タイプを選択します。表示されるプロトコルは SSH1、SSH2（rsa）、SSH2（dsa）です。

ステップ 5　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 6　これらのキーを生成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

（注）　1856 DSA NumberKeys は、Cisco MDS NX-OS ソフトウェア バージョン 4.1(1) 以降を実行しているスイッチではサポートされません。

生成したキー ペアの上書き

必要なバージョンに対して SSH キー ペア オプションが生成済みの場合は、スイッチでそれまでのキー ペアを上書きすることができます。

Fabric Manager を使用して 前回生成した キー ペア を上書きする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

[Information] ペインに設定が表示されます。

ステップ 2　上書きするキーを選択して [Delete Row] アイコンをクリックします。

ステップ 3　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

ステップ 4　[Create Row] アイコンをクリックします。

[SSH and Telnet Key - Create] ダイアログボックスが表示されます。

ステップ 5　この SSH キー ペアを割り当てるスイッチにチェックを入れます。

ステップ 6　[Protocols] オプション ボタンで、キー ペアのオプション タイプを選択します。

ステップ 7　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 8　これらのキーを生成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

SSH または Telnet サービスのイネーブル化

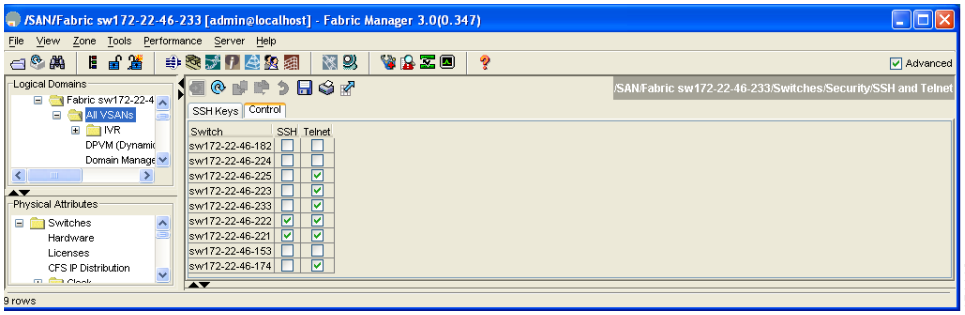
デフォルトでは、SSH サービスはディセーブルです。SSH を設定すると、Fabric Manager は SSH を自動的にイネーブルにします。

Fabric Manager を使用して SSH をイネーブルまたはディセーブルにする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

ステップ 2　[Control] タブを選択し、図 3-12 のように各スイッチの [SSH] チェックボックス、または [Telnet] チェックボックスをオンにします。

図 3-12　[SSH and Telnet] の [Control] タブ



ステップ 3　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

（注）　SSH を介してスイッチにログインし、**aaa authentication login default none** CLI コマンドを発行した場合は、ログインするために 1 つ以上のキー ストロークを入力する必要があります。キーストロークを 1 つも入力せずに **Enter** キーを押すと、ログインは拒否されます。

デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリ スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出処と完全性を保証する 1 つのデータ項目です。安全を保証された通信を行うための暗号キーを含み、提出者の身元を確認するために信頼できる Certification Authority（CA; 認証局）により「署名」されています。X.509 デジタル証明書のサポートは、認証のために DSA または RSA のアルゴリズムも提供します。

証明書インフラストラクチャは Secure Socket Layer（SSL）をサポートする最初の証明書を使用し、セキュリティ インフラストラクチャにより照会または通知の形で返信を受け取ります。証明書が信頼できる CA のいずれかにより発行されている場合に、証明書の確認が成功します。

X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかにスイッチを設定できますが、両方に設定することはできません。いずれかに設定されている場合、その認証が失敗するとパスワードが求められます。

CA およびデジタル証明書の詳細については、第 6 章「CA およびデジタル証明書の設定」を参照してください。

ユーザの作成または更新

他のユーザの権限を変更できるのは、network-admin ユーザだけです。

Fabric Manager を使用して新しいユーザを設定する、または既存ユーザのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザ情報を表示します。

ステップ 2　ユーザを作成するには、[Create Row] アイコンをクリックします。

[Create Users] ダイアログボックスが表示されます。

ステップ 3　このユーザにアクセスを許可するスイッチを選択します。

ステップ 4　新しいユーザ名とパスワードを割り当てます。

（注）　ユーザ アカウント名には、数字以外の文字を含める必要があります。

ステップ 5　この新しいユーザに割り当てるロールを選択します。

ステップ 6　作成または更新するユーザのダイジェストおよび暗号化を選択します。

ステップ 7　（任意）ユーザの有効期限と SSH ファイル名を入力します。

ステップ 8　ユーザを作成するには、[Create] ボタンをクリックします。変更を廃棄するには、[Close] ボタンをクリックします。

管理者パスワードの回復

次の 2 つの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザ名で CLI を使用する
- スイッチの電源を再投入する

（注）　管理者パスワードの回復については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

Cisco ACS サーバの設定

Cisco Access Control Server（ACS）は、TACACS+ および RADIUS プロトコルを利用して、セキュアな環境を作り出す AAA サービスを提供します。AAA サーバを使用する際のユーザ管理は、通常 Cisco ACS を使用して行われます。図 3-13、図 3-14、図 3-15、および図 3-16 に、TACACS+ または RADIUS を利用した ACS サーバの network-admin ロールおよび複数のロールのユーザ セットアップ設定の様子を示します。

注意　TACACS+ か RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS NX-OS は、すべて数字のユーザ名をサポートしません。名前がすべて数字のローカル ユーザは作成できません。すべて数字のユーザ名が AAA サーバに存在し、ログインの際に入力しても、そのユーザはログインできません。

（注）　cisco-av-pair に指定されている各ロールは MDS に存在する必要があります。存在しない場合、ユーザには network-operator ロールが設定されます。

図 3-13　RADIUS を使用する場合の network-admin ロールの設定

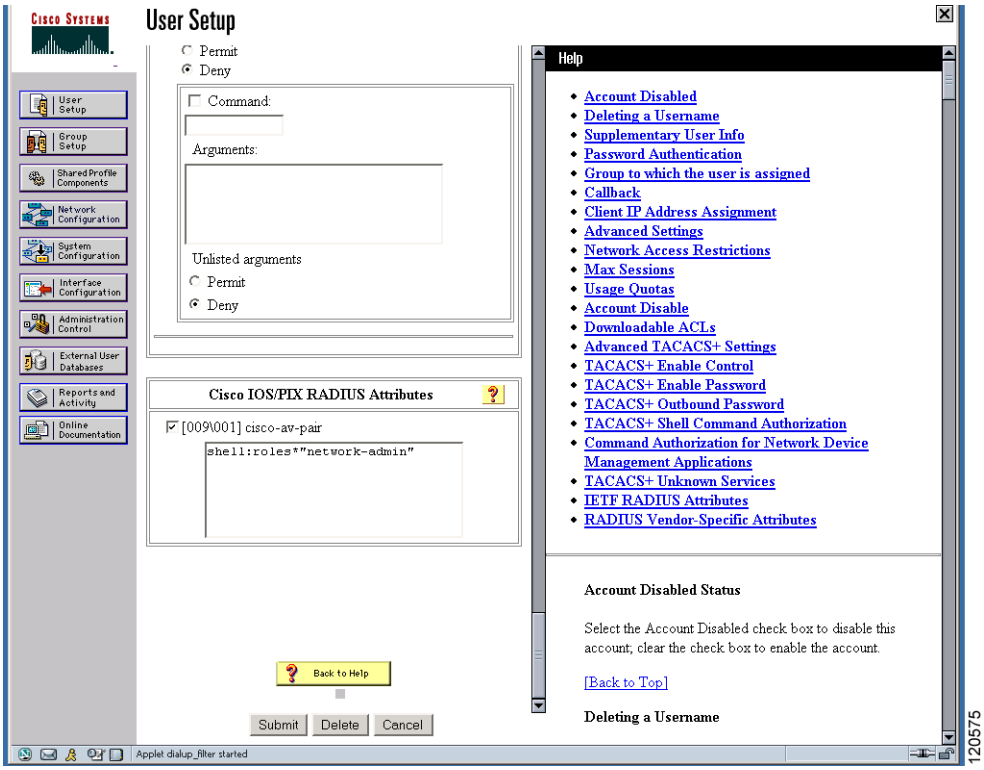


図 3-14　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

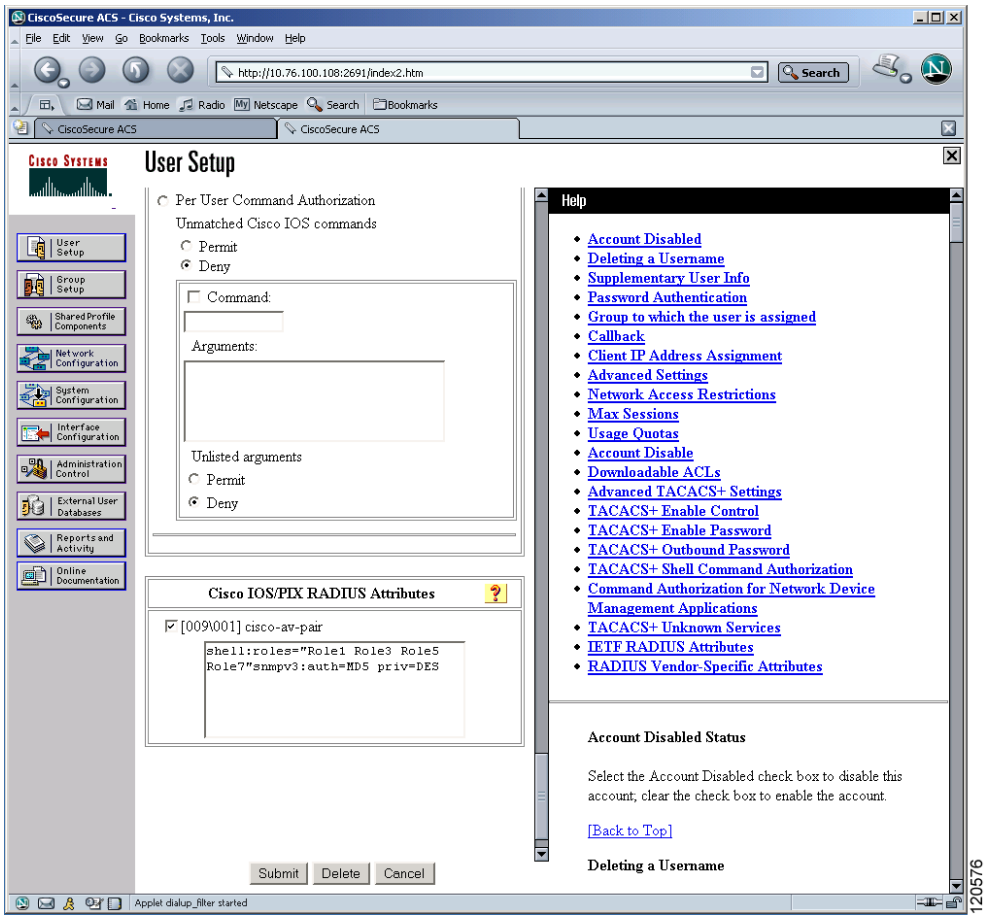


図 3-15　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

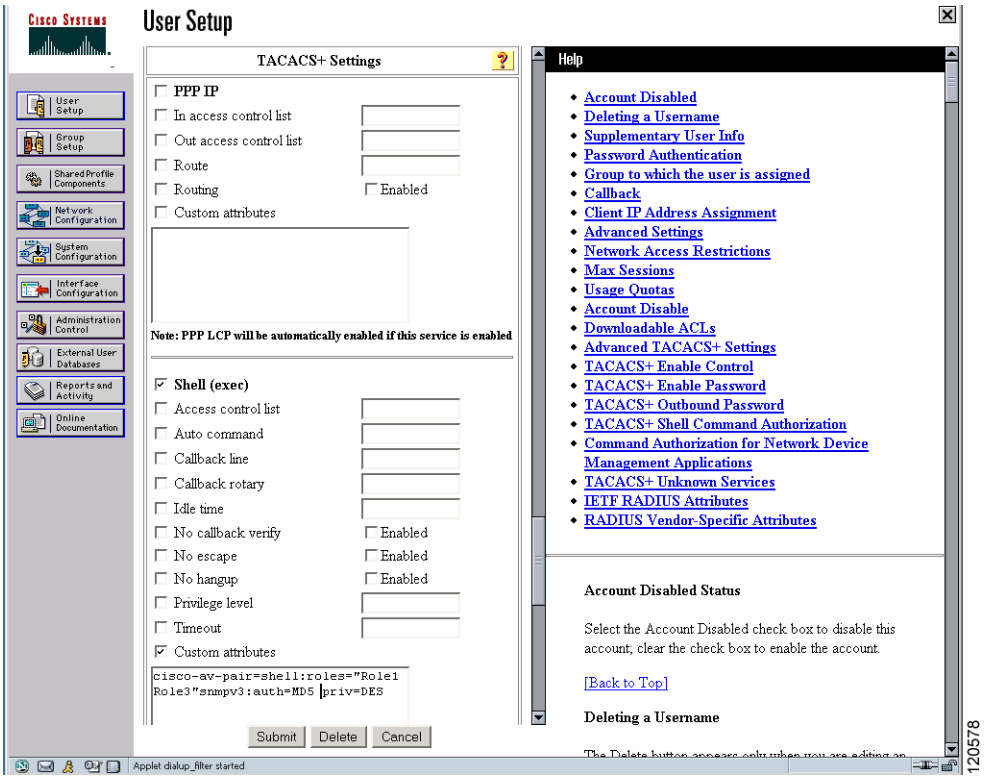
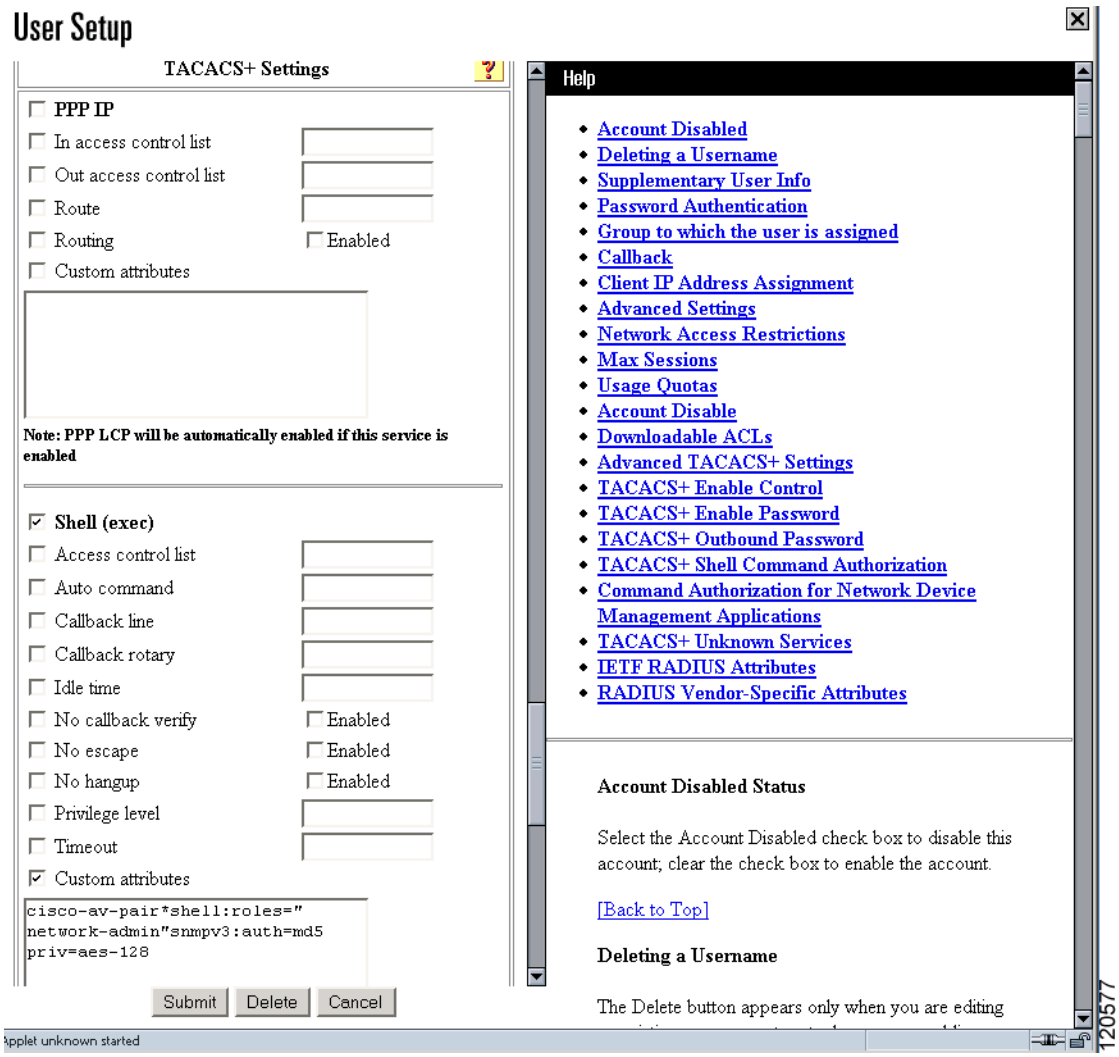


図 3-16　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定値

表 3-1 はすべてのスイッチにおけるスイッチ セキュリティ機能のデフォルト設定です。

表 3-1　デフォルト スイッチ セキュリティ設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク オペレータ（network-operator）
AAA 設定サービス	ローカル
認証用ポート	1812
アカウンティング用ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバ タイムアウト	1 秒
RADIUS サーバ再試行	1 回

表 3-1　デフォルト スイッチ セキュリティ設定 （続き）

パラメータ	デフォルト
TACACS+	ディセーブル
TACACS+ サーバ	設定なし
TACACS+ サーバ タイムアウト	5 秒
AAA サーバへの配布	ディセーブル
ロールに対する VSAN ポリシー	許可
ユーザ アカウント	有効期限なし（設定しない場合）
パスワード	なし
アカウンティング ログ サイズ	250 KB
SSH サービス	ディセーブル
Telnet サービス	イネーブル