CHAPTER 9

ユーザ セキュリティの管理：ロールとスコープ

次のトピックでは、Cisco ANA でロール ベースのセキュリティ メカニズムと、ユーザに割り当てられているスコープ（ネットワーク要素グループ）を結合する二次元セキュリティ エンジンを実装する方法について説明します。さらには、ユーザ名やパスワードの定義など、Cisco ANA プラットフォームでのユーザの管理作業についても説明します。

ユーザ認証および権限付与の概要

Cisco ANA では、複数の方法を組み合せて、ユーザの認証および権限付与を管理します。

- *ユーザ認証*は、Cisco ANA によってローカルに、または LDAP アプリケーションを使用して外部的に管理できます。いずれかの方法を使用してユーザ アカウントとパスワードを検証し、Cisco ANA にログインできるユーザを管理できます。Cisco ANA を使用する場合、ユーザ情報とパスワードは Cisco ANA データベースに保存されます。外部 LDAP アプリケーションを使用する場合、パスワードは外部 LDAP サーバに保存されます。「外部認証」（P.9-2）を参照してください。
- *ユーザへの権限付与*は、*ユーザ アクセス ロール*と*スコープ*の組み合せで管理されます。
  - ユーザ アクセス ロールは、ユーザが Cisco ANA GUI クライアントで実行できる操作を制御します。ユーザのアカウントが作成されると、ユーザの *デフォルト権限*を指定するアクセス ロールがユーザに割り当てられます。詳細については、「ユーザ アクセス ロールとデフォルト権限」（P.9-2）を参照してください。
  - スコープは、管理者が作成するネットワーク要素のグループです。スコープが作成されると、ユーザに割り当てることができます。ユーザのデフォルト権限により、ユーザがスコープ内の Network Element（NE; ネットワーク要素）で実行できる操作が指定されます。これらの操作は、そのスコープに対するユーザの *セキュリティ レベル*として示されます。必要に応じて、スコープに対してより厳格なユーザ アクセス ロールをユーザに割り当てることができます。詳細については、「スコープ」（P.9-3）を参照してください。

たとえば、johnsmith というユーザに、すべてのネットワーク要素でソフトウェア イメージを更新できるユーザ アクセス ロール（またはデフォルト権限）があるとします。スイッチのグループを含む SanFrancisco というスコープを作成し、そのスコープに対してより厳しいセキュリティ アクセスを johnsmith に割り当てることができます。ユーザ johnsmith はスコープ SanFrancisco のスイッチを除き、すべてのネットワーク要素のソフトウェア イメージを更新できます。

ユーザ認証情報（ロールおよびスコープ）は、常に Cisco ANA データベースに保存されます。外部 LDAP サーバを使用する場合は、パスワードだけを保存します。

外部認証

外部認証とは、ユーザ認証およびパスワードが Cisco ANA ではなく、外部アプリケーションによって検証されることを意味します。Cisco ANA が認証を実行すると、Cisco ANA が Cisco ANA データベース内に保存されている情報をチェックしてユーザを検証します。LDAP アプリケーションを使用する場合、情報は外部 LDAP サーバによって検証されます。

外部認証を使用している Cisco ANA が LDAP サーバと通信できない場合は、root ユーザに限り Cisco ANA に再ログインできます。これは、root ユーザが LDAP の*緊急時ユーザ*であり、その検証を行えるのが Cisco ANA に限られるためです。root ユーザは、Cisco ANA にログインして、認証方式をローカル認証に変更し、その他のユーザがログインできるようにそのユーザ アカウントを編集できます。Cisco ANA では LDAP バージョン 3 を使用します。

外部認証を使用する場合、次の手順を行います。

- 必要なインストール前提条件を実行します。『*Cisco Active Network Abstraction 3.6.7 Installation Guide*』を参照してください。
- LDAP サーバと通信できるように Cisco ANA を設定します。「外部 LDAP サーバによるパスワード認証」（P.6-1）を参照してください。

外部認証から Cisco ANA 認証に切り替える場合、ユーザ情報を LDAP サーバから Cisco ANA にインポートできます。この手順については、『*Cisco Active Network Abstraction 3.6.7 Installation Guide*』を参照してください。

ユーザ アクセス ロールとデフォルト権限

ユーザ アクセス ロースはユーザが Cisco ANA で実行を許可されている操作を管理します。ユーザ アカウントを作成する際に、1 つのセキュリティ アクセス ロールをアカウントに割り当てます。このロールによって、ユーザのデフォルト権限が決定します。デフォルト権限は、次のようにユーザが実行できる一般的な GUI の機能を決定します。

- Cisco ANA へのログイン
- Cisco ANA NetworkVision のアラーム管理
- マップの作成、削除、開始
- マップの配置、NE の追加、集約の管理、NE のマップへの追加、マップのバックグラウンドの設定
- ビジネス タグ管理

前述の例は、NE に何の設定もプロビジョニングも実行しません。ユーザがアクセスできるスコープを決定したら、スコープ（NE のリスト）をユーザのアカウントに追加し、スコープにセキュリティ アクセス ロールを割り当てます。これがユーザのスコープ セキュリティ レベルとなり、ユーザがスコープ内の NE に実行できる操作を管理します。スコープの詳細については、「スコープ」（P.9-3）を参照してください。

Cisco ANA では、ユーザに割り当ててシステム機能をイネーブルにするための定義済みのセキュリティ アクセス ロールを 5 つ用意しています（表 9-1 を参照。また、詳しい例は 表 9-2（P.9-4）を参照してください）。

表 9-1　ユーザ アクセス ロール

ロール	説明
Viewer	ネットワーク、リンク、イベント、インベントリを表示します。ネットワークおよびシステムの特権を必要としないシステム機能への読み込み専用アクセスだけが可能です。
Operator	アラームの管理、マップの操作、ネットワーク関連情報の表示、ビジネス アタッチメントの管理など、日常のビジネス業務のほとんどを実行します。
OperatorPlus	アラームのライフサイクルを管理します。
Configurator	Command Builder、Configuration Archive、NEIM、およびアクティベーション コマンドを使用して、サービスの設定およびアクティベーションに関連するタスクおよびテストを実行します。
Administrator	Cisco ANA のシステムおよびセキュリティを管理します。ユニット、AVM、および VNE の作成、ポーリング グループ、保護グループ、ユーザ、スコープ、およびマップの管理など、すべての管理的操作を実行します。

新しいユーザが Administrator として定義されると、このユーザが Cisco ANA Manage を使用してすべてのマップを開いたり、すべてのスコープを処理したり、システムを管理したりするなど、すべての管理的操作を実行できます。これらのアクティビティは、最も高い権限で実行します。Cisco ANA Manage は、複数の管理者をサポートします。管理ユーザにアクセス権限を定義する必要はありません。

スコープ

スコープは、管理される NE のグループです。ユーザは、割り当てられたスコープ内にある NE にだけアクセスできます。さらに、ユーザがアクセスできる NE およびそれらの NE で実行できる操作を決定する、スコープごとのユーザ アクセス ロールを指定します。Cisco ANA には、「All Managed Elements」という定義済みスコープがあります。このスコープは編集できません。ユーザ アクセス ロールの詳細については、「ユーザ アクセス ロールとデフォルト権限」（P.9-2）を参照してください。

スコープおよびロールをユーザに割り当てた後、ユーザは、次のようにスコープ内に含まれる NE にさまざまなアクティビティを実行できます。

- サービスをアクティブにする。
- NE、インベントリ、リンクのプロパティを表示する。
- カウンタの表示、使用率の表示、リフレッシュなど、高度なオプションを管理する。

表 9-2 では、各ユーザ アクセス ロールに基づいて、スコープ内の GUI クライアントでユーザが実行できる操作について説明しています。

表 9-2　ユーザ アクセス ロールに基づいて許可されるスコープと GUI の機能

ユーザ アクセス ロール	GUI クライアントで許可される操作	スコープ内で許可される操作
Administrator	次のようなプラットフォーム管理。 • Cisco ANA サーバ、AVM、トランスポート、VNE の管理。 • ポーリング グループ、保護グループ、クライアント ライセンス、サービスの免責事項など、グローバル設定の管理。 • DB セグメントの表示。 • スコープの作成および削除。 • ユーザ アカウントの管理。 • 静的トポロジ リンクの管理。 • Cisco ANA Manage または Cisco ANA NetworkVision からの VNE 管理。 次のマップ管理。 • すべてのユーザ マップの使用、編集、削除。	すべて。
Configurator	次のマップ管理。 • マップの作成。 高度なツール。 • クライアントから NE への直接の PING および Telnet。 • ポート アラームのイネーブル設定およびディセーブル設定。 • Cisco ANA Command Builder。	アクティブ化サービス。 • 管理対象 NE に対するアクティブ化コマンドの許可。
OperatorPlus	次のマップ管理。 • マップの新規作成と NE の追加。 • マップの編集、削除、および名前の変更。 • マップの保存。 マップの操作。 • 集約の作成および解除。 • マップ レイアウトの変更。 • 背景イメージの設定。 • ビジネス リンクの作成。	アラーム管理。 • OperatorPlus ロールが割り当てられたユーザのスコープ内の NE に属するアラームの通知、削除、およびクリア。 マップの操作。 • NE のビジネス タグの作成。 ネットワーク情報の表示。 • パス ツール トラフィック、レート、ドロップ、またはダイナミック データの表示。

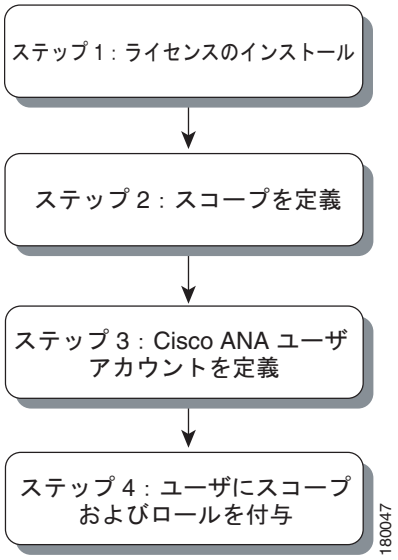
表 9-2　ユーザ アクセス ロールに基づいて許可されるスコープと GUI の機能 （続き）

ユーザ アクセス ロール	GUI クライアントで許可される操作	スコープ内で許可される操作
Operator	マップの操作。 • ビジネス タグの作成および削除。 アプリケーション。 • Cisco ANA EventVision の開始。	ネットワーク情報の表示。 • NE からのポート情報のリフレッシュ。
Viewer	アプリケーション。 • Cisco ANA NetworkVision および Cisco ANA EventVision へのログイン。 • ユーザ パスワードの変更。 • デバイス リストの表示。 • マップの表示。 • リンクのプロパティの表示。 • テーブル フィルタの使用。 • テーブルからのエクスポート。	ネットワーク情報およびビジネス タグ情報の表示。 • アラーム リスト、アラームのプロパティの表示、アラームの検索。 • アタッチメントの検索および表示。 • NE プロパティおよびコンポーネントの表示。 • 影響を受ける対象の算出および表示。 • ポート使用率グラフの表示。

ユーザおよびスコープの設定に必要な作業

図 9-1 および後続のテキストでは、Cisco ANA Manage を使用してセキュリティをカスタマイズする場合に必要な手順、およびその手順の実行順序について説明します。

図 9-1　セキュリティ フローのカスタマイズ



1. ライセンスをインストールする。これにより、インストールされているクライアント ライセンスに基づき、一定または不定期間におけるクライアントの数と BQL の接続性を、制御および監視できます。詳細については、「クライアント ライセンスの管理」（P.6-5）を参照してください。
2. スコープを定義する。ユーザが各ユーザ ロールに基づいて NE を表示および管理できるよう、特定の管理対象 NE をグループ化できます。詳細については、「スコープの作成および管理」（P.9-6）を参照してください。
3. Cisco ANA ユーザ アカウントを定義する。これにより、ユーザ アカウントを定義および管理できます。詳細については、「ユーザ アカウントの管理とユーザ アクセスの制御」（P.9-8）を参照してください。
4. スコープおよびロールをユーザに割り当てる。これにより、一般的なユーザ アカウント情報、各ユーザに割り当てられたスコープのリスト、スコープごとのセキュリティ アクセス ロールを管理できます。詳細については、「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照してください。

また、次の操作タスクを実行できます。

- 外部 LDAP サーバを使用してパスワードを保存し、ユーザを認証したい場合は、外部認証を設定する。詳細については、「外部 LDAP サーバによるパスワード認証」（P.6-1）を参照してください。
- ユーザがアクセスできる既存のマップを制御する。この機能は、デフォルトではディセーブル設定されており、ユーザがアクセスできるのは、ユーザ アカウントがイネーブルになった後に作成されたマップだけです。この機能をイネーブルにし、既存のマップに対するユーザ アクセスの設定を変更する方法については、「マップに対するユーザ アクセスの制御（[Maps] タブ）」（P.9-12）を参照してください。

スコープの作成および管理

Cisco ANA Manage を使用すると、各ユーザ ロールまたは権限に基づいて NE を表示および管理できるよう、特定の管理対象 NE をグループ化できます。

スコープが作成されたら、ユーザに割り当てることができます。複数のスコープを 1 人のユーザに割り当てることも、1 つのスコープを複数のユーザの割り当てることもできます。スコープをユーザに割り当てたら、ユーザに割り当てられたスコープの範囲内でユーザのロールを定義する、セキュリティ アクセス ロールを割り当てる必要があります。「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照してください。

次のトピックでは、スコープの管理方法について説明しています。

スコープの作成

スコープを作成するには、次の手順に従います。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Scopes] を選択します。

ステップ 2　次のいずれかの方法で、[New Scope] ダイアログボックスを開きます。

- [Scopes] を右クリックし、[New Scope] を選択します。
- [File] > [New Scope] を選択します。

- ツールバーにある [New Scope] をクリックします。

ステップ 3　[Scope] フィールドにスコープの名前を入力します。

ステップ 4　スコープに追加するデバイスを指定します。

- デバイスをスコープに追加するには、[Available Devices] リストから該当するデバイスを選択し、続いて [Add All] または [Add Selected] をクリックすると、デバイスが [Active Devices] リストに移動します。
- デバイスをスコープから削除するには、[Active Devices] リストからデバイスを選択し、続いて [Remove Selected] または [Remove All] をクリックすると、デバイスが [Available Devices] リストに移動します。

（注）　複数のデバイスを選択するには、Ctrl キーを使用します。

ステップ 5　[Active Devices] リストにスコープに追加するデバイスが表示されたら、[OK] をクリックします。このスコープが保存され、コンテンツ領域に表示されます。

スコープのプロパティの編集および表示

Cisco ANA Manage を使用して、スコープの詳細を編集または表示できます。

スコープのプロパティを編集または表示するには、次の手順に従います。

ステップ 1　ナビゲーション ペインで [Scopes] を選択します。

ステップ 2　コンテンツ領域で、編集または表示するスコープを選択します。

ステップ 3　次のいずれかの方法で、スコープの [Properties] ダイアログボックスを開きます。

- スコープを右クリックし、[Properties] を選択する。
- [File] > [Properties] を選択する。
- ツールバーにある [Properties] をクリックする。

[Properties] ダイアログボックスの詳細は、「スコープの作成および管理」（P.9-6）を参照してください。

ステップ 4　必要に応じて、プロパティを編集および表示します。

ステップ 5　[OK] をクリックします。[Properties] ダイアログボックスが閉じます。

スコープの削除

スコープが削除されると、スコープを割り当てられたすべてのユーザから削除されます。

スコープを削除するには、次の手順に従います。

ステップ 1　ナビゲーション ペインで [Scopes] を選択します。

ステップ 2　コンテンツ領域で、削除するスコープを選択します。

（注）　複数のスコープを選択するには、Ctrl キーを使用します。

ステップ 3　スコープを右クリックし、[Delete] を選択します。スコープが削除され、コンテンツ領域から除外されます。

ユーザ アカウントの管理とユーザ アクセスの制御

[Users] ブランチでは、ユーザ アカウントの定義および管理を行えます。これには、セキュリティ アクセス権限のほか、一般的なユーザ情報の管理、また必要に応じて強制的ログインの変更が含まれます。また、ユーザが最後にログインした時間も監視できます。

Cisco ANA での新しいユーザ アカウントの設定は、次の手順で行います。

1. ユーザ アカウントを作成し、GUI 機能に対するユーザのアクセスを制御するデフォルトの権限を割り当てます。「ユーザ アカウントの作成とデフォルト権限の割り当て」（P.9-8）を参照してください。
2. （任意）クライアント接続の最大数、およびパスワードの変更が必要になるタイミングを指定します。「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照してください。
3. スコープと、ネットワーク要素に対するユーザのアクセスを制御するスコープの権限を適用します。「スコープに対するユーザ権限とアクセスの制御（[Security] タブ）」（P.9-11）を参照してください。

ユーザ アカウントの作成とデフォルト権限の割り当て

次の定義済みシステム デフォルトで、新しいユーザを作成します。

- スコープはまだ、ユーザに割り当てられていません。
- 接続数は無制限です。
- パスワードは 30 日ごとに変更する必要があります。
- 最大ログイン試行回数は 5 回です。

ユーザ アカウントを定義するには、次の手順に従います。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Users] を選択します。

ステップ 2　次のいずれかの方法で [Users] ダイアログボックスを開きます。

- [Users] を右クリックして、[New User] を選択する。
- [File] > [New User] を選択する。
- ツールバーにある [New User] をクリックする。

（注）　[Show Password Rules] をクリックして、現在のパスワード ルールを表示します。

ステップ 3　新しいユーザを定義するために必要となる次の情報を入力します。

フィールド	説明
[User Name]	ログインに使用する新しいユーザの名前を入力します。 **（注）**　ユーザ名は一意で、最大 20 文字です。特殊文字は使用できません。
[Full Name]	（任意）ユーザのフルネームを入力します。 **（注）**　有効なエントリは最大 20 文字です。特殊文字は使用できません。
[Description]	（任意）ユーザについての説明を適宜入力してください。
[Non-ANA Authentication Only]	オンにすると、Cisco ANA は、外部 LDAP サーバによって検証できるパスワードを持つユーザだけログインを許可します。[password] フィールドはディセーブルになります （外部認証が使用される場合、ボックスはデフォルトでオンになります。「外部 LDAP サーバによるパスワード認証」（P.6-1）を参照してください）。
[Password]	新しい Cisco ANA パスワードを入力します。パスワードは Cisco ANA データベースに保存されます （[Non-ANA Authentication Only] チェックボックスがオンの場合、このフィールドはディセーブルです）。パスワードは、次の基準を満たさなければなりません。 • 8 ～ 20 文字で、数字を 1 つ以上使用する。 • 特殊文字は使用しない。 • ユーザ名、またはその反転を使用しない。
[Confirm Password]	新しい Cisco ANA パスワードを再入力します。
[Role]	ドロップダウン リストから、ユーザのデフォルト権限となるセキュリティ アクセス ロールを選択します。 **（注）**　この権限は、NE に関連のないアクティビティまたは操作にだけ適用されます。ユーザが実行できる機能の詳細については、「ユーザ アクセス ロールとデフォルト権限」（P.9-2）を参照してください。
[Force Password Change at Next Login]	このチェックボックスはデフォルトでオンとなっており、ユーザは次回ログイン時、ユーザ パスワードの変更を強制されます （[Non-ANA Authentication Only] チェックボックスがオンの場合、このフィールドはディセーブルです）。

ステップ 4　[Create] をクリックします。新しいユーザ名とデフォルトのセキュリティ アクセス ロールがコンテンツ領域に表示されます。

基本のユーザ アカウントが作成されます。設定を検証する方法について、「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照してください。スコープがユーザに割り当てられるまで、ネットワーク要素は表示されません。「スコープに対するユーザ権限とアクセスの制御（[Security] タブ）」（P.9-11）を参照してください。

ユーザ情報の変更とアカウントの無効化（[General] タブ）

ユーザ アカウントを作成した後、ユーザ プロパティを表示して [General] タブを選択すると、アカウント作成時に入力した情報が表示されます。ユーザの GUI クライアント接続数を制御、または特定の時間の後にパスワードの変更を強制することにより、アカウントをさらに調整できます。次の手順に従って、ユーザ アカウントをディセーブルにしたり、再度イネーブルにしたりできます。

一般的なユーザ情報を表示または編集するには、次の手順に従います。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Users] を選択します。

ステップ 2　目的のユーザを右クリックして、[Properties] を選択します。

[General] タブがデフォルトで選択された状態で、[Properties] ダイアログボックスが表示されます。

ステップ 3　必要に応じて全般プロパティを編集します。

フィールド	説明
[User Name]	現在のユーザ名。ユーザ名は変更できません。
[Last Login]	ユーザが最後にログインした日時が表示されます。
[Full Name]	ユーザのフルネーム。
[Description]	ユーザに関する説明が表示されます。
[Enable Account]	このチェックボックスをオンにすると、ユーザ アカウントがイネーブルになります。チェックボックスをオフにすると、ユーザ アカウントがディセーブルになります。ログイン数が指定された数を超えると、（[Limit Connections] オプションがイネーブルの場合）ユーザ アカウントが自動的にロックされます。ユーザのアカウントは、手動でいつでもロックまたはロック解除できます。アカウントがロックされているユーザは、システムにログインできません。
[Non-ANA Authentication Only]	オンにすると、Cisco ANA は、外部 LDAP サーバによって検証できるパスワードを持つユーザだけログインを許可します。このダイアログボックスの [Password] フィールドの入力されたパスワードはディセーブルとなり、Cisco ANA がローカル認証に切り替えた場合でも、ユーザはログインできなくなります （外部認証が使用される場合、ボックスはデフォルトでオンになります。「外部 LDAP サーバによるパスワード認証」（P.6-1）を参照してください）。 このチェックボックスをオフにすると、Cisco ANA がローカル認証で使用する新しいパスワードを要求します。パスワードは Cisco ANA データベースに保存され、[Force Password] フィールドがアクティブになります。
[Limit Connections to]	ユーザが一度にアクセスできる Cisco ANA クライアント アプリケーションのインスタンス数。たとえば、接続数が 10 に制限されている場合、ユーザは同時に Cisco ANA Manage に 5 つのインスタンス、Cisco ANA NetworkVision に 5 つのインスタンスを使用できます。10 のインスタンスを使用している状態でユーザが Cisco ANA EventVision のインスタンスを開こうとすると、その試行は拒否されます。

フィールド	説明
[Force Password Change After]	チェックボックスをオンにすると、指定した日数を経過した後、パスワードの変更が強制されます。このチェックボックスをオフにすると、ユーザは現在のパスワードを保持できます。 チェックボックスがオンの場合、パスワード変更を強制されるまでの日数を入力します ([Non-ANA Authentication Only] チェックボックスがオンの場合、このフィールドはディセーブルです)。
[Force Password Change at Next Login]	このチェックボックスをオンにすると、ユーザは次回ログイン時にパスワード変更を強制されます。このオプションは、いつでも設定できます ([Non-ANA Authentication Only] チェックボックスがオンの場合、このフィールドはディセーブルです)。

ステップ 4　[Apply] をクリックして、エントリを適用します。

ステップ 5　[OK] をクリックして [Properties] ダイアログボックスを閉じるか、[Security] タブをクリックしてユーザにスコープを割り当てます （詳細については、「スコープに対するユーザ権限とアクセスの制御（[Security] タブ）」（P.9-11）を参照してください)。

スコープに対するユーザ権限とアクセスの制御（[Security] タブ）

[Security] タブを使用すると、ユーザのスコープとセキュリティ アクセス ロールを適用して、アプリケーションおよび NE を表示および管理するユーザの機能を管理できます。スコープが割り当てられるまでは、ネットワーク要素を表示できません。ネットワーク要素へのアクセス レベルであるスコープは、次の手順で指定した設定によって制御されます。

（注）　ユーザは、さまざまなスコープのさまざまなセキュリティ アクセス ロールを持つことができます。

スコープおよびセキュリティ レベルをユーザに割り当てるには、次の手順に従います。

ステップ 1　Cisco ANA で [User] ブランチを選択します。

ステップ 2　目的のユーザを右クリックして、[Properties] を選択します。

[User Properties] ダイアログボックスが表示されます。

ステップ 3　[Security] タブをクリックします。

ステップ 4　[Default] ドロップダウン リストで、ユーザのデフォルトのセキュリティ レベルを選択します。デフォルトでは、新しいユーザにはビューア セキュリティ アクセス ロールが割り当てられます。ここで選択するレベルは、[ANA Users] コンテンツ領域テーブルに表示される値です。

ステップ 5　[Add] をクリックして、ユーザのアクティブな権限にスコープを追加します。[Security Level] ダイアログが表示されます。

ステップ 6　目的のスコープを選択し、ユーザのこのスコープ内の適切なセキュリティレベルを選択します。

フィールド	説明
[Available Scopes]	定義済みのスコープと割り当てられていないスコープをすべて表示します。
[Security Level]	定義済みスコープのセキュリティ アクセス ロールを表示します。詳細については、「スコープ」（P.9-3）を参照してください。

ステップ 7　[OK] をクリックします。スコープが、[Security] タブの [Active Rights] リストに追加されます。

ステップ 8　[Apply] をクリックし、[OK] をクリックします。[Properties] ダイアログボックスが閉じます。

マップに対するユーザ アクセスの制御（[Maps] タブ）

[Maps] タブを使用して、既存のマップに対するユーザのアクセスを制御します。

（注）　この機能は、デフォルトではディセーブルです。

Cisco ANA NetworkVision にログインする場合、新しいユーザには既存マップを表示する権限はありません。アクセスできるのは、今後作成するマップだけです。ただし、管理者は、この機能をイネーブルにし、手動でマップを割り当てることによって、既存のマップを新しいユーザに割り当てることができます。

この機能をイネーブルにするには、次の手順に従います。

ステップ 1　ゲートウェイ サーバにユーザ sheer でログインします。

ステップ 2　~sheer/Main ディレクトリに移動します。

ステップ 3　次のコマンド（1 行）を実行します。

```
# ./runRegTool.sh -gs localhost set 127.0.0.1
site/mmvm/services/securitymanager/map-security-enabled true
```

ステップ 4　ゲートウェイ サーバが成功のメッセージを返したら、ゲートウェイを再起動します。

マップをユーザに割り当てるには、次の手順に従います（この機能をイネーブルした後）。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Users] を選択します。

ステップ 2　目的のユーザを右クリックして、[Properties] を選択します。

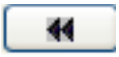
[User Properties] ダイアログボックスが表示されます。

ステップ 3　[Maps] タブをクリックします。

[Maps] タブは、次の 2 つの部分で構成されています。

- 左側には、ユーザに割り当てられていない、データベース内の使用できるすべてのマップのリストが表示されます。
- 右側には、ユーザに割り当てられ、ユーザが Cisco ANA NetworkVision で開いたり管理できるすべてのマップが表示されます。

[Map] タブの使用できるマップのリストと割り当てられたマップのリストの間に、次のボタンが表示されます。

ボタン	説明
	選択したマップを [Assigned Maps] リストに移動します。
	使用できるマップ リスト全体を [Assigned Maps] リストに移動します。
	選択したマップを、[Assigned Maps] リストから [Available Map] リストに移動します。
	[Assigned Map] リスト全体を [Available Map] リストに移動します。

ステップ 4　[Available Maps] リストからマップを選択し、該当するボタンをクリックして [Assigned Maps] リストのマップをユーザに追加します。

（注）　複数の行を選択するには、Ctrl キーを使用します。

ステップ 5　必要に応じて、該当するボタンを使用し、2 つのリストの間でマップを選択して移動します。

ステップ 6　[OK] をクリックして、ユーザの割り当てられたマップを確定します。

Cisco ANA ユーザ アカウントの削除

ユーザ アカウントを削除するには、次の手順に従います。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Users] を選択します。

ステップ 2　コンテンツ領域で、削除するユーザ アカウントを選択します。

（注）　複数の行を選択するには、Ctrl キーを使用します。

ステップ 3　ユーザを右クリックし、[Delete] を選択します。選択したユーザが削除され、コンテンツ領域に表示されなくなります。

ユーザの Cisco ANA パスワードの変更

ユーザの Cisco ANA パスワードは、Cisco ANA Manage を使用していつでも変更できます。この場合、ユーザは次回ログイン時にパスワード変更を強制されます。「パスワードの変更：管理者の手順」（P.9-14）を参照してください。

次の手順は、Cisco ANA を使用してユーザを検証する場合にだけ適用されます。外部 LDAP アプリケーションを使用してパスワードを管理している場合、LDAP サーバでパスワードを変更する必要があります。

現在のユーザもパスワードの変更できます。このシナリオでは、ユーザは新しいパスワードを検証するために以前のパスワードを入力する必要があります。「パスワードの変更：ユーザの手順」（P.9-14）を参照してください。

パスワードの変更：管理者の手順

管理者としてユーザのパスワードを変更するには、次の手順に従います。

ステップ 1　[Cisco ANA Manage] ウィンドウで [Users] を選択します。

ステップ 2　コンテンツ領域で、パスワードを変更するユーザを選択します。

ステップ 3　目的のユーザを右クリックして、[Change Password] を選択します。[Change Password] ダイアログボックスが表示されます。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに新しいパスワードを入力します。

ステップ 5　[OK] をクリックします。確認用のメッセージが表示されます。

ステップ 6　[OK] をクリックします。[Change Password] ダイアログボックスが閉じます。

パスワードの変更：ユーザの手順

Cisco ANA Manage を使用して、現在のユーザがパスワードを変更できます。

ユーザとしてパスワードを変更するには、次の手順に従います。

ステップ 1　[Tools] > [Change User Password] を選択します。[Change User Password] ダイアログボックスが表示されます。

ステップ 2　[Old Password] フィールドに旧パスワードを入力します。

ステップ 3　[New Password] フィールドと [Confirm Password] フィールドに新しいパスワードを入力します。

ステップ 4　[OK] をクリックします。確認用のメッセージが表示されます。

ステップ 5　[OK] をクリックします。[Change User Password] ダイアログボックスが閉じます。