ACS との Security Manager の統合

内容

概要

このドキュメントでは、Cisco Security Manager(CSM)とCisco Secure Access Control Server(ACS)を統合する方法について説明します。

Cisco Secure ACSは、管理対象ネットワークデバイスを設定するために、Cisco Security Managerなどの管理アプリケーションを使用するユーザにコマンド許可を提供します。コマンド許可のサポートは、一連の権限を含むCisco Security Managerのロールと呼ばれる固有のコマンド許可セットタイプによって提供されます。これらの権限は、特権とも呼ばれ、特定のロールを持つユーザがCisco Security Manager内で実行できるアクションを決定します。

Cisco Secure ACSは、管理アプリケーションとの通信にTACACS+を使用します。Cisco Security ManagerがCisco Secure ACSと通信するには、Cisco Secure ACSのCiscoWorksサーバを、TACACS+を使用するAAAクライアントとして設定する必要があります。さらに、Cisco Secure ACSにログインするために使用する管理者名とパスワードをCiscoWorksサーバに提供する必要があります。これらの要件を満たすと、Cisco Security ManagerとCisco Secure ACS間の通信の有効性が保証されます。

Cisco Security Managerは、Cisco Secure ACSと最初に通信するときに、Cisco ACSに対して、Cisco Secure ACS HTMLインターフェイスの[Shared Profile Components]セクションに表示されるデフォルトロールの作成を指示します。また、TACACS+によって認可されるカスタムサービスも指定します。このカスタムサービスは、HTMLインターフェイスの[Interface Configuration]セクションの[TACACS+ (Cisco IOS®)]ページに表示されます。次に、各Cisco Security Managerロールに含まれる権限を変更し、これらの権限をユーザおよびユーザグループに適用できます。

注：CSMはサポートされていないため、ACS 5.2と統合できません。

前提条件

要件

Cisco Secure ACSを使用するには、次のことを確認します。

- Cisco Security Managerで必要な機能を実行するために必要なコマンドを含むロールを定義します。
- ネットワークアクセス制限(NAR)には、NARをプロファイルに適用する場合に管理するデバイスグループ（またはデバイス）が含まれます。
- 管理対象デバイス名は、Cisco Secure ACSとCisco Security Managerで同じスペルおよび大文字で表記されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Security Managerバージョン3.0
- Cisco Secure ACS バージョン 3.3

注：ネットワーク環境にインストールする前に、互換性のあるCSMおよびACSバージョンを選択してください。たとえば、CiscoではCSM 3.0のみを使用してACS 3.3をテストし、それ以降のCSMバージョンでは停止しています。したがって、ACS 3.3でCSM 3.0を使用することをお勧めします。さまざまなソフトウェアバージョンの詳細については、「互換性マトリクス」の表を参照してください。

Cisco Security Managerバージョン	CS ACSバージョンのテスト
3.0.0 3.0.0 SP1	Windows 3.3(3)および4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1)および4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Solutions Engine v4.0(1) Windows 4.1(2)、4.1(3)、4.1(4)
3.1.1 SP1	Solutions Engine 4.0(1) Windows 4.1(4)
3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4)および4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows

	4.1(4)および4.2(0)
3.2.1	Solutions Engine 4.1(4) Windows 4.2(0)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco Security ManagerとCisco Secure ACSの統合

このセクションでは、Cisco Security ManagerとCisco Secure ACSを統合するために必要な手順について説明します。一部の手順には、いくつかのサブステップが含まれています。これらの手順とサブステップは、順番に実行する必要があります。このセクションでは、各ステップを実行するために使用される特定の手順についても説明します。

次のステップを実行します。

1. **管理認証および認可モデルを計画します。**Cisco Security Managerを使用する前に、管理モデルを決定する必要があります。これには、使用する管理者ロールとアカウントの定義が含まれます。**ヒント**：潜在的な管理者のロールと権限を定義する場合は、ワークフローを有効にするかどうかを検討してください。この選択は、アクセスを制限する方法に影響します。
2. **Cisco Secure ACS、Cisco Security Manager、およびCiscoWorks Common Servicesをインストールします。**Cisco Secure ACSバージョン3.3をWindows 2000/2003サーバにインストールします。CiscoWorks Common ServicesとCisco Security Managerを別のWindows 2000/Windows 2003サーバにインストールします。詳細は、次のドキュメントを参照してください。Cisco Security Manager 3.0 のインストール ガイドCisco Secure ACS for Windows 3.3 インストール ガイド**注：CSMおよ**びACSソフトウェアのバージョンを選択する前に、「互換性マトリクス」の表を参照してください。
3. **Cisco Secure ACSで統合手順を実行します。**Cisco Security ManagerユーザをACSユーザとして定義し、計画されたロールに基づいてユーザグループに割り当て、すべての管理対象デバイス（およびCiscoWorks/Security Managerサーバ）をAAAクライアントとして追加し、管理制御ユーザを作成します。詳細は、『Cisco Secure ACSで実行される統合手順』を参照してください。
4. **CiscoWorks Common Servicesで統合手順を実行します。**Cisco Secure ACSで定義された管理者に一致するローカルユーザを設定し、そのユーザをシステムID設定に定義し、ACSをAAAセットアップモードとして設定します。詳細については、「CiscoWorksで実行される統合手順」を参照してください。
5. **Cisco Secure ACSのユーザグループへのロールの割り当て**Cisco Secure ACSで設定された各ユーザグループにロールを割り当てます。使用する手順は、ネットワークデバイスグループ(NDG)を設定しているかどうかによって異なります。詳細は、「Cisco Secure ACSでのユーザグループへのロールの割り当て」を参照してください。

Cisco Secure ACSで実行される統合手順

このセクションでは、Cisco Secure ACSをCisco Security Managerと統合するためにCisco Secure ACSで実行する必要がある手順について説明します。

1. Cisco Secure ACSでのユーザおよびユーザグループの定義
2. Cisco Secure ACSでのAAAクライアントとしての管理対象デバイスの追加
3. Cisco Secure ACSでの管理制御ユーザの作成

Cisco Secure ACSでのユーザおよびユーザグループの定義

Cisco Security Managerのすべてのユーザは、Cisco Secure ACSで定義され、それぞれの職務に適したロールを割り当てる必要があります。これを行う最も簡単な方法は、ACSで使用可能な各デフォルトロールに基づいて、ユーザを異なるグループに分割することです。たとえば、すべてのシステム管理者を1つのグループに、すべてのネットワークオペレータを別のグループに割り当てるなどです。ACSのデフォルトロールの詳細については、『Cisco Secure ACSのデフォルトロール』を参照してください。

さらに、システム管理者ロールに完全な権限が割り当てられた追加ユーザを作成する必要があります。このユーザに対して確立されたクレデンシャルは、後でCiscoWorksの[System Identity Setup]ページで使用されます。詳細については、「システムIDユーザーの定義」を参照してください。

この段階では、ユーザを別のグループに割り当てるだけです。これらのグループへのロールの実際の割り当ては、CiscoWorks、Cisco Security Manager、およびその他のアプリケーションがCisco Secure ACSに登録された後に実行されます。

ヒント：先に進む前に、CiscoWorks Common ServicesとCisco Security Managerを1台のWindows 2000/2003サーバにインストールしてください。別のWindows 2000/2003サーバにCisco Secure ACSをインストールします。

1. Cisco Secure ACSにログインします。
2. 完全な権限を持つユーザを設定します。ナビゲーション・**バーのユ**ーザー設定をクリックします。[ユーザー設定]ページで、新しいユーザーの名前を入力し、[追加/編集]を**クリックします**。[User Setup]の[Password Authentication]リストから認証方法を選択します。新しいユーザのパスワードを入力して確認します。ユーザー**が割り当**てられているグループとして[グループ1]を選択します。[**Submit**]をクリック**し**、ユーザアカウントを作成します。
3. 各Cisco Security Managerユーザに対してステップ2を繰り返します。各ユーザに割り当てられているロールに基づいて、ユーザをグループに分割することをお勧めします。グループ1：システム管理者グループ2：セキュリティ管理者グループ3：セキュリティ承認者グループ4：ネットワーク管理者グループ5：承認者グループ6：ネットワークオペレータグループ7：ヘルプデスク各ロールに関連付けられるデフォルト権限の詳細については、表を参照してください。ユーザロールのカスタマイズの詳細は、『Cisco Secure ACSロールのカスタマイズ』を参照してください。**注：この段階**では、グループ自体はロール定義のないユーザの集合です。統合プロセスの完了後、各グループにロールを割り当てます。詳細は、「Cisco Secure ACSでのユーザグループへのロールの割り当て」を参照してください。
4. 追加ユーザを作成し、このユーザをシステム管理者グループに割り当てます。このユーザに対して確立されたクレデンシャルは、後でCiscoWorksの[System Identity Setup]ページで使用されます。詳細については、「システムIDユーザーの定義」を参照してください。

5. Cisco Secure ACSで[Add Managed Devices as AAA Clients]に進みます。

Cisco Secure ACSでのAAAクライアントとしての管理対象デバイスの追加

Cisco Security Managerへのデバイスのインポートを開始する前に、Cisco Secure ACSで各デバイスをAAAクライアントとして設定する必要があります。さらに、CiscoWorks/Security Managerサーバ をAAAクライアントとして設定する必要があります。

ファイアウォールデバイスに設定されたセキュリティコンテキスト（Catalyst 6500/7600デバイス用のFWSMに設定されたセキュリティコンテキストなど）をCisco Security Managerが管理する場合、各コンテキストをCisco Secure ACSに個別に追加する必要があります。

管理対象デバイスを追加するために使用する方法は、ネットワークデバイスグループ(NDG)を使用する特定のデバイスセットをユーザが管理することを制限するかどうかによって異なります。次のいずれかの項を参照してください。

- ユーザがすべてのデバイスにアクセスできるようにするには、「デバイスをNDGのないAAAクライアントとして追加する」の説明に従って、デバイスを追加します。
- ユーザが特定のNDGのみにアクセスできるようにするには、「Security Managerで使用するネットワークデバイスグループの構成」の説明に従ってデバイスを追加します。

NDGのないAAAクライアントとしてのデバイスの追加

この手順では、Cisco Secure ACSのAAAクライアントとしてデバイスを追加する方法について説明します。利用可能なすべてのオプションに関する完全な情報は、『ネットワーク構成』の「AAAクライアントの設定」セクションを参照してください。

注：CiscoWorks/Security Managerサーバ をAAAクライアントとして追加してください。

1. Cisco Secure ACSのナビゲーションバーの**Network Configuration**をクリックします。
2. AAA Clientsテーブル**の下の**[Add Entry]をクリックします。
3. [Add AAA Client]ページで、AAAクライアントのホスト名（最大32文字）を入力します。AAAクライアントのホスト名は、Cisco Security Managerでデバイスに使用する表示名と一致している必要があります。たとえば、Cisco Security Managerでデバイス名にドメイン名を追加する場合、ACSのAAAクライアントのホスト名は**<device_name>.<domain_name>である必要があります**。CiscoWorksサーバに名前を付ける場合は、完全修飾ホスト名を使用することを推奨します。ホスト名を正しく入力してください。ホスト名では大文字と小文字は区別されません。セキュリティコンテキストに名前を付ける場合は、コンテキスト名(**_<context_name>**)をデバイス名に追加します。FWSMの場合、次に命名規則を示します。FWSMブレード：**<chassis_name>_FW_<slot_number>**セキュリティコンテキスト：**<chassis_name>_FW_<slot_number>_<context_name>**
4. [AAA Client IP Address]フィールドにネットワークデバイスのIPアドレスを入力します。
5. [Key]フィールドに共有秘密を入力します。
6. [Authenticate Using]**リストから[TACACS+ (Cisco IOS)]**を選択します。
7. [**Submit**]をクリックして、変更を保存します。追加したデバイスが[AAA Clients]テーブルに表示されます。
8. 手順1 ~ 7を繰り返して、デバイスを追加します。
9. すべてのデバイスを追加したら、[**Submit** + Restart]**をクリックします**。
10. 「Cisco Secure ACSでの管理制御ユーザの作成」に進みます。

セキュリティマネージャで使用するネットワークデバイスグループの設定

Cisco Secure ACSでは、管理対象の特定のデバイスを含むネットワークデバイスグループ(NDG)を設定できます。たとえば、各地域のNDGまたは組織構造に一致するNDGを作成できます。NDGをCisco Security Managerとともに使用すると、管理する必要があるデバイスに応じて、異なるレベルの権限をユーザに提供できます。たとえば、NDGでは、ユーザAのシステム管理者権限をヨーロッパにあるデバイスに、ヘルプデスク権限をアジアにあるデバイスに割り当てることができます。その後、ユーザBに逆の権限を割り当てることができます。

NDGはユーザに直接割り当てられません。NDGは、ユーザグループごとに定義したロールに割り当てられます。各NDGは1つのロールにのみ割り当てることができますが、各ロールには複数のNDGを含めることができます。これらの定義は、選択したユーザグループの設定の一部として保存されます。

次のトピックでは、NDGを設定するために必要な基本的な手順について説明します。

- NDG機能のアクティブ化
- NDGの作成
- NDGおよびロールとユーザグループの関連付け

NDG機能のアクティブ化

NDGを作成してデバイスを入力する前に、NDG機能をアクティブにする必要があります。

1. Cisco Secure ACSのナビゲーションバーのInterface Configurationをクリックします。
2. [詳細オプション]をクリックします。
3. 下にスクロールし、[ネットワークデバイスグループ]チェックボックスをオンにします。
4. [Submit] をクリックします。
5. [NDGの作成]に進みます。

NDGの作成

この手順では、NDGを作成し、デバイスを入力する方法について説明します。各デバイスは1つのNDGにのみ属することができます。

注：CiscoWorks/Security Managerサーバを含む特別なNDGを作成することをお勧めします。

1. ナビゲーション・バーの[Network Configuration]をクリックします。すべてのデバイスは最初は[未割り当て(Not Assigned)]の下に配置され、NDGに配置されなかったすべてのデバイスが保持されます。[未割り当て(Not Assigned)]はNDGではないことに注意してください。
2. NDGの作成：[エントリの追加]をクリックします。[New Network Device Group]ページでNDGの名前を入力します。最大長は 24 文字です。スペースは使用できます。**バージョン4.0以降の場合はオプション**：NDGのすべてのデバイスで使用するキーを入力します。NDGにキーを定義すると、NDG内の個々のデバイスに対して定義されたキーが上書きされます。[Submit]をクリックし、NDGを保存します。さらにNDGを作成するには、手順a ~ dを繰り返します。
3. NDGにデバイスを入力します。[Network Device Groups]領域でNDGの名前をクリックします。[AAA Clients]領域で[Add Entry]をクリックします。NDGに追加するデバイスの詳細を定義し、[送信]をクリックします。詳細は、「NDGのないAAAクライアントとしてのデバイス

の追加」を参照してください。手順bとcを繰り返して、残りのデバイスをNDGに追加します。[Not Assigned]カテゴリに残すことができるデバイスは、デフォルトのAAAサーバだけです。最後のデバイスを設定したら、[送信+**再起動]をクリックします**。
4. 「Cisco Secure ACSでの管理制御ユーザの作成」に進みます。

Cisco Secure ACSでの管理制御ユーザの作成

Cisco Secure ACSの[Administration Control]ページを使用して、CiscoWorks Common ServicesでAAAセットアップモードを定義するときに使用する管理者アカウントを定義します。詳細は、「CiscoWorksでのAAAセットアップモードの設定」を参照してください。

1. Cisco Secure ACSのナビ**ゲーションバーで**[Administration Control]をクリックします。
2. [管理者の追**加]をクリックします**。
3. [Add Administrator]ページで、管理者の名前とパスワードを入力します。
4. この管理者に完全な管理アクセス権を付与するには、[Administrator Privileges]領域で[Grant All]をクリックします。
5. [**Submit**]をクリックし、管理者を作成します。

注：管理者を構成する際に使用できるオプションの詳細については、「管理者および管理ポリシー」を参照してください。

CiscoWorksで実行される統合手順

このセクションでは、Cisco Security Managerと統合するためにCiscoWorks Common Servicesで実行する手順について説明します。

- CiscoWorksでのローカルユーザの作成
- システムアイデンティティユーザの定義
- CiscoWorksでのAAAセットアップモードの設定

Cisco Secure ACSで実行する統合手順を完了したら、次の手順を実行します。Common Servicesは、Cisco Security Manager、Auto-Update Server、IPS Managerなどのインストール済みアプリケーションをCisco Secure ACSに実際に登録します。

CiscoWorksでのローカルユーザの作成

CiscoWorks Common Servicesの[Local User Setup]ページを使用して、以前Cisco Secure ACSで作成した管理者と重複するローカルユーザアカウントを作成します。このローカルユーザアカウントは、後でシステムIDの設定に使用されます。詳細については、を参照してください。

注：続行する前に、Cisco Secure ACSで管理者を作成してください。手順については、「Cisco Secure ACSでのユーザおよびユーザグループの定義」を参照してください。

1. デフォルトの管理者ユーザアカウントを使用して**CiscoWorksにロ**グインします。
2. Common Servicesから**Server > Securityの順に選択**し、目次から**Local User Setup**を選択します。
3. [Add] をクリックします。
4. Cisco Secure ACSで管理者を作成したときに入力した名前とパスワードを入力します。Cisco Secure ACSのユーザおよびユーザグループの定義の手順4を参照してください。
5. [データのエクスポート(Export Data)]を除き、[ロール(Roles)]のすべてのチェックボックス

をオンにします。
6. 「OK」をクリックして、ユーザーを作成します。

システムアイデンティティユーザの定義

CiscoWorks Common Servicesの[System Identity Setup]ページを使用して、同じドメインに属するサーバと同じサーバ上にあるアプリケーションプロセス間の通信を可能にする、System Identityユーザと呼ばれる信頼ユーザを作成します。アプリケーションは、ローカルまたはリモートのCiscoWorksサーバ上のプロセスを認証するために、System Identityユーザを使用します。これは、ユーザがログインする前にアプリケーションを同期する必要がある場合に特に便利です。

さらに、System Identityユーザは、プライマリタスクがログインしたユーザに対してすでに承認されている場合に、サブタスクを実行するためによく使用されます。たとえば、Cisco Security Managerでデバイスを編集するには、Cisco Security ManagerとCommon Services DCRの間でアプリケーション間通信が必要です。ユーザに編集タスクの実行が許可されると、System IdentityユーザがDCRを起動するために使用されます。

ここで設定するSystem Identityユーザは、ACSで設定した管理（完全）権限を持つユーザと同じである必要があります。これを行わないと、Cisco Security Managerで設定されているすべてのデバイスとポリシーを表示できなくなります。

注：先に進む前に、CiscoWorks Common Servicesでこの管理者と同じ名前とパスワードを使用してローカルユーザを作成します。手順については、「CiscoWorksでのローカルユーザの作成」を参照してください。

1. 「サーバ」>「セキュリティ」を選択し、**目次から「マルチサーバー信頼管理」>「システムID設定」**を選択します。
2. Cisco Secure ACS用に作成した管理者の名前を入力します。Cisco Secure ACSのユーザおよびユーザグループの定義の手順4を参照してください。
3. このユーザのパスワードを入力して確認します。
4. [Apply] をクリックします。

CiscoWorksでのAAAセットアップモードの設定

必要なポートと共有秘密キーを含むAAAサーバとしてCisco Secure ACSを定義するには、CiscoWorks Common Servicesの[AAA Setup Mode]ページを使用します。さらに、最大2つのバックアップサーバを定義できます。

これらの手順では、Cisco Works、Cisco Security Manager、IPS Manager（およびオプションでAuto-Update Server）をCisco Secure ACSに実際に登録します。

1. **Server > Securityの順に選択**し、目次から**AAA Mode Setup**を選択します。
2. [Available Login Modules]の下の[**TACACS+**]チェックボックスをオンにします。
3. AAAタイプ**として**[ACS]を選択します。
4. [Server Details]領域に、最大3台のCisco Secure ACSサーバのIPアドレスを入力します。セカンダリサーバとターシャリサーバは、プライマリサーバに障害が発生した場合のバックアップとして機能します。**注：設定されているすべてのTACACS+サーバが応答しない場合は**、admin CiscoWorks Localアカウントでログインし、AAAモードをNon-ACS/CiscoWorks Localに戻す必要があります。TACACS+サーバがサービスに復元されたら、AAAモードをACSに戻す必要があります。

5. [Login]領域で、Cisco Secure ACSの[Administration Control]ページで定義した管理者の名前を入力します。詳細については、「Cisco Secure ACSでのAdministration Controlユーザの作成」を参照してください。
6. この管理者のパスワードを入力して確認します。
7. Security ManagerサーバをCisco Secure ACSのAAAクライアントとして追加したときに入力した共有秘密キーを入力して確認します。「NDGを使用しないAAAクライアントとしてデバイスを追加する」のステップ5を参照してください。
8. Cisco Security Managerおよびその他のインストール済みアプリケーションをCisco Secure ACSに登録するには、[Register all installed applications with ACS]チェックボックスをオンにします。
9. Apply をクリックして、設定を保存します。経過表示バーに登録の進行状況が表示されます。登録が完了すると、メッセージが表示されます。
10. Cisco Security Managerを任意のACSバージョンと統合する場合は、Cisco Security Manager Daemon Managerサービスを再起動します。手順については、 Restart the Daemon Managerを参照してください。**注：**CSM 3.0.0以降、ACS 3.3(x)はパッチが多く適用され、サポート終了(EOL)が発表されたため、テストを終了しました。したがって、CSMバージョン3.0.1以降に適切なACSバージョンを使用する必要があります。詳細は、「互換性マトリックス」の表を参照してください。
11. 各ユーザグループにロールを割り当てるには、Cisco Secure ACSに再度ログインします。手順については、「Cisco Secure ACSのユーザグループへのロールの割り当て」を参照してください。**注：ここで**設定したAAA設定は、CiscoWorks Common ServicesまたはCisco Security Managerをアンインストールしても保持されません。また、再インストール後にこの設定をバックアップおよび復元することはできません。したがって、いずれかのアプリケーションの新しいバージョンにアップグレードする場合は、AAAセットアップモードを再設定し、Cisco Security ManagerをACSに再登録する必要があります。このプロセスは、差分更新には必要ありません。AUSなどの追加アプリケーションをCiscoWorksの上にインストールする場合は、新しいアプリケーションとCisco Security Managerを再登録する必要があります。

Daemon Managerを再起動します

この手順では、Cisco Security ManagerサーバのDaemon Managerを再起動する方法について説明します。設定したAAA設定を有効にするには、これを行う必要があります。その後、Cisco Secure ACSで定義されたクレデンシャルを使用してCiscoWorksに再度ログインできます。

1. Cisco Security Managerサーバがインストールされているマシンにログインします。
2. **[Start] > [Programs] > [Administrative Tools] > [Services]の順に選択して**、[Services]ウィンドウを開きます。
3. 右側のペインに表示されるサービスのリストから、**[Cisco Security Manager Daemon Manager]を選択します。**
4. ツールバーの**[サービスの**再開]ボタンをクリックします。
5. Cisco Secure ACSの[Assign Roles to User Groups]に進みます。

Cisco Secure ACSのユーザグループへのロールの割り当て

CiscoWorks、Cisco Security Manager、およびその他のインストール済みアプリケーションをCisco Secure ACSに登録した後、Cisco Secure ACSで以前に設定した各ユーザグループにロールを割り当てることができます。これらのロールは、各グループのユーザがCisco Security

Managerで実行できるアクションを決定します。

ユーザグループにロールを割り当てるために使用する手順は、NDGが使用されているかどうかによって異なります。

- NDGのないユーザグループへのロールの割り当て
- NDGおよびロールとユーザグループの関連付け

NDGのないユーザグループへのロールの割り当て

この手順では、NDGが定義されていない場合にデフォルトロールをユーザグループに割り当てる方法について説明します。詳細は、『Cisco Secure ACSのデフォルトロール』を参照してください。

注：次の手順に進む前に、

- 各デフォルトロールのユーザグループを作成します。手順については、「Cisco Secure ACSでのユーザおよびユーザグループの定義」を参照してください。
- Cisco Secure ACSで実行される統合手順およびCiscoWorksで実行される統合手順に記載されている手順を実行します。

次のステップを実行します。

1. Cisco Secure ACSにログインします。
2. ナビゲーション・バーの[グループ設定]をクリックします。
3. リストからシステム管理者用のユーザグループを選択します。Cisco Secure ACSのユーザとユーザグループの定義のステップ2を参照し、[設定の編集]をクリックします。

NDGおよびロールとユーザグループの関連付け

Cisco Security Managerで使用するロールにNDGを関連付ける場合、[Group Setup]ページで次の2つの場所に定義を作成する必要があります。

- CiscoWorksエリア
- Cisco Security Managerエリア

各領域の定義は、可能な限り一致している必要があります。CiscoWorks Common Servicesに存在しないカスタムロールまたはACSロールを関連付ける場合は、そのロールに割り当てられた権限に基づいて、できるだけ同等のロールを定義してみてください。

Cisco Security Managerで使用するユーザグループごとに関連付けを作成する必要があります。たとえば、Westernリージョンのサポート担当者を含むユーザグループがある場合、そのユーザグループを選択し、そのリージョンのデバイスを含むNDGをヘルプデスクの役割に関連付けることができます。

注：続行する前に、NDG機能をアクティブにしてNDGを作成してください。詳細については、「Security Managerで使用するネットワークデバイスグループの構成」を参照してください。

1. ナビゲーション・バーの[グループ設定]をクリックします。
2. [グループ]リストからユーザグループを選択し、[設定の編集]をクリックします。
3. CiscoWorksで使用するNDGとロールのマッピング：[Group Setup]ページで、[TACACS+ Settings]の下の[CiscoWorks]エリアまでスクロールします。[Assign a **CiscoWorks on a**

Network Device Group Based]を選択します。[Device Group]リストからNDGを選択します。2番目のリストから、このNDGを関連付けるロールを選択します。[関連付けの追**加]をクリックします。**関連付けが[デバイスグループ(Device Group)]ボックスに表示されます。追加の関連付けを作成するには、手順c ~ eを繰り返します。**注：関連付けを**削除するには、デバイスグループから関連付けを選択し、[Remove Association]をクリックします。

4. [Cisco Security Manager]領域までスクロールし、ステップ3で定義した関連付けとできるだけ一致する関連付けを作成します。**注：**Cisco Secure ACSで[Security Approver]または[Security Administrator]ロールを選択する場合は、最も近い同等のCiscoWorksロールとして[Network Administrator]を選択することをお勧めします。
5. [**Submit**]をクリックして、設定を保存します。
6. 手順2 ~ 5を繰り返して、ユーザグループの残りの部分のNDGを定義します。
7. NDGとロールを各ユーザグループに関連付けた後、[送信+再起**動]をクリックします。**

トラブルシュート

1. Cisco Security Managerへのデバイスのインポートを開始する前に、Cisco Secure ACSで各デバイスをAAAクライアントとして設定する必要があります。さらに、CiscoWorks/Security ManagerサーバをAAAクライアントとして設定する必要があります。
2. 失敗した試行ログを受信すると、Cisco Secure ACSで作成者がエラーで失敗します。
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   この問題を解決するには、ACSのデバイス名が完全修飾ドメイン名である必要があります。

関連情報

- Cisco Security Access Control Server for Windowsに関するサポートページ
- Cisco Security Manager のサポート ページ
- Cisco Secure Access Control Server for Windows
- Cisco Secure ACS 4.1 の設定ガイド
- Cisco Secure ACS オンライン トラブルシューティング ガイド 4.1
- セキュリティ製品に関する Field Notice (CiscoSecure ACS for Windows を含む)
- テクニカル サポートとドキュメント – Cisco Systems