CHAPTER 7

ユーザ アカウントの管理

Security Manager を使用するには、製品にログインして、個別のアカウントを作成する必要があります。Security Manager サーバ上で定義され、ローカル アカウントと呼ばれる Security Manager に特有のアカウントを作成することも、エンタープライズ ACS サーバを使用してユーザを認証することもできます。次のトピックで、ユーザ アカウントの作成方法と管理方法、ACS システムと製品の統合方法について説明します。

ユーザ権限のセットアップ

Cisco Security Manager が、ログイン前にユーザ名とパスワードを認証します。これらが認証されると、Security Manager がアプリケーション内のユーザ ロールを設定します。このロールによって、実行が認可されるタスクまたは操作のセットである権限（特権とも呼ばれる）が定義されます。特定のタスクまたはデバイスに対して認可されなかった場合は、関連するメニュー項目、目次内の項目、およびボタンが非表示またはディセーブルになります。加えて、選択した情報を表示したり、選択した操作を実行したりするための権限がないことを伝えるメッセージが表示されます。

Security Manager の認証と認可は、CiscoWorks サーバと Cisco Secure Access Control Server（ACS）のどちらかによって管理されます。デフォルトで、CiscoWorks は、認証と認可を管理しますが、CiscoWorks Common Services の [AAA Mode Setup] ページを使用して Cisco Secure ACS を変更できます。ACS 統合の詳細については、「Security Manager と Cisco Secure ACS の統合」（P.7-8）を参照してください。

Cisco Secure ACS を使用する重要なメリットは、特殊な権限セット（特定のポリシー タイプの設定だけをユーザに許可する場合など）を使用して非常に粒度の細かいユーザ ロールを作成できることと、Network Device Group（NDG; ネットワーク デバイス グループ）を設定することによって特定のデバイスにユーザを制限できることです。このような粒度の細かい特権は、CiscoWorks ローカル ユーザは使用できません。

ヒント Security Manager 権限ツリーの全体を表示するには、Cisco Secure ACS にログインしてから、ナビゲーション バーの [Shared Profile Components] をクリックします。詳細については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください。

次のトピックで、ユーザ権限について説明します。

Security Manager ACS 権限

Cisco Security Manager はデフォルトの ACS ロールと権限を提供します。デフォルト ロールをカスタマイズすることも、ニーズに合わせて追加のロールを作成することもできます。ただし、新しいロールを定義する場合、または、デフォルト ロールをカスタマイズする場合は、選択した権限が Security Manager アプリケーションの観点から適切であることを確認してください。たとえば、表示権限を伴わない変更権限を付与した場合、そのユーザはアプリケーションを使用できなくなります。

Security Manager 権限は次のカテゴリに分類されます。個々の権限に関する説明については、Cisco Secure ACS に統合されているオンライン ヘルプを参照してください（権限の表示方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください）。

- [View]：現在の設定の表示を可能にします。主な表示権限を次に示します。
  - [View] > [Policies]：さまざまなタイプのポリシーの表示を可能にします。このフォルダには、ファイアウォールや NAT などのさまざまなポリシー クラスの権限が含まれています。
  - [View] > [Objects]：さまざまなタイプのポリシー オブジェクトの表示を可能にします。このフォルダには、ポリシー オブジェクト タイプごとの権限が含まれています。
  - [View] > [Admin]：Security Manager 管理設定の表示を可能にします。
  - [View] > [CLI]：デバイス上で設定された CLI コマンドの表示と、展開しようとしているコマンドのプレビューを可能にします。
  - [View] > [Config Archive]: 設定アーカイブに保存されている設定の一覧表示を可能にします。デバイス設定や CLI コマンドは表示できません。
  - [View] > [Devices]：[Device] ビュー内のデバイスと関連情報（デバイス設定、プロパティ、割り当てなど）の表示を可能にします。NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。
  - [View] > [Device Managers]：Cisco IOS ルータ用の Cisco Router and Security Device Manager（SDM）など、あるデバイス専用のデバイス マネージャ（読み取り専用バージョン）の起動を可能にします。
  - [View] > [Topology]：[Map] ビューで設定されたマップの表示を可能にします。
- [Modify]：現在の設定の変更を可能にします。
  - [Modify] > [Policies]：さまざまなタイプのポリシーの変更を可能にします。このフォルダには、さまざまなポリシー クラスの権限が含まれています。
  - [Modify] > [Objects]：さまざまなタイプのポリシー オブジェクトの変更を可能にします。このフォルダには、ポリシー オブジェクト タイプごとの権限が含まれています。
  - [Modify] > [Admin]：Security Manager 管理設定の変更を可能にします。
  - [Modify] > [Config Archive]：設定アーカイブ内のデバイス設定の変更を可能にします。加えて、アーカイブへの設定の追加と設定アーカイブ ツールのカスタマイズを可能にします。
  - [Modify] > [Devices]：デバイスの追加と削除だけでなく、デバイスのプロパティと属性の変更を可能にします。追加するデバイスに関するポリシーを検出するには、[Import] 権限もイネーブルにする必要があります。加えて、[Modify] > [Devices] 権限をイネーブルにした場合は、[Assign] > [Policies] > [Interfaces] 権限もイネーブルになっていることを確認してください。NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。

  - [Modify] > [Hierarchy]：デバイス グループの変更を可能にします。
  - [Modify] > [Topology]：[Map] ビュー内のマップの変更を可能にします。
- [Assign]：デバイスと VPN へのさまざまなポリシー タイプの割り当てを可能にします。このフォルダには、さまざまなポリシー クラスの権限が含まれています。
- [Approve]：ポリシー変更と展開ジョブの承認を可能にします。
- [Control]：ping などのデバイスに対するコマンドの発行を可能にします。この権限は、接続診断に使用されます。
- [Deploy]：ネットワーク内のデバイスに対する設定変更の展開と、以前の展開設定に戻すためのロールバックの実施を可能にします。
- [Import]：すでにデバイス上に展開された設定の Security Manager へのインポートを可能にします。デバイスの表示特権とデバイスの変更特権も持っている必要があります。
- [Submit]：設定変更の送信と承認を可能にします。

ヒント

- 変更、割り当て、承認、インポート、制御、または展開権限を選択した場合は、対応する表示権限も選択する必要があります。そうしなかった場合は、Security Manager が正しく機能しません。
- ポリシーの変更権限を選択した場合は、対応するポリシーの割り当て権限と表示権限も選択する必要があります。
- その定義の一部としてポリシー オブジェクトを使用するポリシーを許可した場合は、これらのオブジェクト タイプに表示権限も付与する必要があります。たとえば、ルーティング ポリシーを変更するための権限を選択した場合は、ルーティング ポリシーに必要なオブジェクト タイプのネットワーク オブジェクトとインターフェイス ロールを表示するための権限も選択する必要があります。
- その定義の一部として他のオブジェクトを使用するオブジェクトを許可する場合も同様です。たとえば、ユーザ グループを変更するための権限を選択した場合は、ネットワーク オブジェクト、ACL オブジェクト、および AAA サーバ グループを表示するための権限も選択する必要があります。
- NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。NDG はポリシー権限に対して次のような影響を与えます。
  - ポリシーを表示するには、そのポリシーが割り当てられた少なくとも 1 つのデバイスに対する権限を持っている必要があります。
  - ポリシーを変更するには、そのポリシーが割り当てられたすべてのデバイスに対する権限を持っている必要があります。
  - VPN ポリシーを表示、変更、または割り当てるには、VPN トポロジ内のすべてのデバイスに対する権限を持っている必要があります。
  - デバイスにポリシーを割り当てるには、ポリシーが割り当てられた他のデバイスに対する権限を持っているかどうかに関係なく、そのデバイスの権限のみが必要です（上述したように、VPN ポリシーは例外です）。ただし、権限を持っていないデバイスに割り当てられているポリシーを変更することはできません。

CiscoWorks ロールについて

CiscoWorks Common Services 内で作成されたユーザには、1 つ以上のロールが割り当てられます。各ロールに割り当てられた権限によって、各ユーザが Security Manager 内で実行を認可される操作が決定されます。

次のトピックで、CiscoWorks ロールについて説明します。

- 「CiscoWorks Common Services デフォルト ロール」（P.7-4）
- 「CiscoWorks Common Services でのユーザに対するロールの割り当て」（P.7-4）

CiscoWorks Common Services デフォルト ロール

CiscoWorks Common Services には、Security Manager 用の次のデフォルト ロールが用意されています。

- **ヘルプ デスク**：ヘルプ デスク ユーザは、デバイス、ポリシー、オブジェクト、およびトポロジ マップを表示できます（ただし、変更はできません）。
- **アプルーバ**：表示権限に加えて、アプルーバは展開ジョブを承認または拒否できます。展開を実行できません。
- **ネットワーク オペレータ**：表示権限に加えて、ネットワーク オペレータは、CLI コマンドと Security Manager 管理設定を表示できます。ネットワーク オペレータは、設定アーカイブを変更したり、デバイスにコマンド（ping など）を発行したりすることもできます。
- **ネットワーク管理者**：ネットワーク管理者は、管理設定の変更を除く、すべての表示権限と変更権限を持っています。彼らは、デバイスとその上で設定されたポリシーを検出したり、デバイスにポリシーを割り当てたり、デバイスにコマンドを発行したりできます。ネットワーク管理者は、アクティビティを承認したり、ジョブを展開したりできません。ただし、他の人が承認したジョブは展開できます。

  （注） Cisco Secure ACS は、さまざまな権限セットを含むネットワーク管理者という名前のデフォルト ロールを特徴とします。詳細については、「Cisco Secure ACS ロールについて」（P.7-5）を参照してください。

- **システム管理者**：システム管理者は、変更、ポリシー割り当て、アクティビティとジョブの承認、検出、展開、およびデバイスに対するコマンドの発行を含む、すべての Security Manager 権限にアクセスできます。

Security Manager 権限と CiscoWorks ロールの関連付けについては、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.7-7）を参照してください。

ヒント

- 追加のアプリケーションがサーバ上にインストールされた場合に、追加のロール（データのエクスポートなど）が Common Services に表示される場合があります。データのエクスポート ロールは、サードパーティ開発者用であり、Security Manager では使用されません。
- CiscoWorks ロールの定義は変更できませんが、各ユーザに割り当てるロールを定義できます。詳細については、「CiscoWorks Common Services でのユーザに対するロールの割り当て」（P.7-4）を参照してください。
- CiscoWorks で権限テーブルを生成するには、[Server] > [Reports] > [Permission Report] を選択して、[Generate Report] をクリックします。

CiscoWorks Common Services でのユーザに対するロールの割り当て

CiscoWorks Common Services でユーザを定義するときに、そのユーザに付与するロールを選択する必要があります。ユーザに関するロール定義を変更することによって、そのユーザが Security Manager 内で実行を認可される操作タイプを変更します。たとえば、ヘルプ デスク ロールを割り当てた場合、

ユーザは表示操作に制限され、データを変更できません。ただし、ネットワーク オペレータ ロールを割り当てた場合、ユーザは設定アーカイブを変更することもできます。各ユーザに複数のロールを割り当てることができます。

ヒント　ユーザ権限を変更したら、Security Manager を再起動する必要があります。

関連トピック

- 「Security Manager ACS 権限」（P.7-2）
- 「Security Manager 内の権限とロールのデフォルトの関連付け」（P.7-7）
- 「CiscoWorks ロールについて」（P.7-3）

ステップ 1　Common Services で、[Server] > [Security] を選択して、目次から [Single-Server Trust Management] > [Local User Setup] を選択します。

ヒント　Security Manager から [Local User Setup] ページにアクセスするには、[Tools] > [Security Manager Administration] > [Server Security] を選択してから、[Local User Setup] をクリックします。

ステップ 2　次のいずれかを実行します。

- ユーザを作成するには、[Add] をクリックして、ユーザ名、パスワード、および電子メール アドレスを入力します。
- 既存のユーザのロールを変更するには、ユーザの横にあるチェックボックスをオンにして、[Edit] をクリックします。

ステップ 3　[User Information] ページで、ユーザに割り当てるロールを選択します。各ロールの詳細については、「CiscoWorks Common Services デフォルト ロール」（P.7-4）を参照してください。

ステップ 4　[OK] をクリックして変更を保存します。

ステップ 5　Security Manager を再起動します。

Cisco Secure ACS ロールについて

Cisco Secure ACS は、設定可能なアプリケーション固有のロールをサポートしているため、CiscoWorks よりも柔軟性の高い Security Manager 権限の管理を可能にします。各ロールは、Security Manager タスクに対する認可レベルを決定する権限セットで構成されます。Cisco Secure ACS で、各ユーザ グループに（およびオプションで個別のユーザにも）ロールを割り当てます。これによって、グループ内の各ユーザは、そのロールに対して定義された権限によって認可される操作を実行できます。

加えて、これらのロールを Cisco Secure ACS デバイス グループに割り当てて、デバイスのセットごとに権限を区別できるようにできます。

（注）　Cisco Secure ACS デバイス グループは、Security Manager デバイス グループとは無関係です。

次のトピックで、Cisco Secure ACS ロールについて説明します。

- 「Cisco Secure ACS デフォルト ロール」（P.7-6）
- 「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）

Cisco Secure ACS デフォルト ロール

Cisco Secure ACS には、CiscoWorks と同じロール（「CiscoWorks ロールについて」（P.7-3）を参照）に加えて、次のロールが含まれています。

- **セキュリティ アプルーバ**：セキュリティ アプルーバは、デバイス、ポリシー、オブジェクト、マップ、CLI コマンド、および管理設定を表示できます（ただし、変更はできません）。加えて、セキュリティ アプルーバは、アクティビティに含まれる設定変更を承認または拒否できます。彼らは、展開ジョブを承認または拒否できないだけでなく、展開を実行することもできません。
- **セキュリティ管理者**：表示権限が付与されていることに加えて、セキュリティ管理者は、デバイス、デバイス グループ、ポリシー、オブジェクト、およびトポロジ マップを変更できます。彼らは、デバイスと VPN トポロジにポリシーを割り当てたり、システムに新しいデバイスをインポートするための検出を実行したりすることもできます。
- **ネットワーク管理者**：表示権限に加えて、ネットワーク管理者は、設定アーカイブを変更したり、展開を実行したり、デバイスにコマンドを発行したりできます。

（注） Cisco Secure ACS ネットワーク管理者ロール内に含まれる権限は、CiscoWorks ネットワーク管理者ロール内に含まれる権限と同じではありません。詳細については、「CiscoWorks ロールについて」（P.7-3）を参照してください。

CiscoWorks と違って、Cisco Secure ACS を使用すれば、各 Security Manager ロールに関連付けられた権限をカスタマイズできます。デフォルト ロールの変更方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください。

Security Manager 権限と Cisco Secure ACS ロールの関連付けについては、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.7-7）を参照してください。

関連トピック

- 「Security Manager と Cisco Secure ACS の統合」（P.7-8）
- 「ユーザ権限のセットアップ」（P.7-1）

Cisco Secure ACS ロールのカスタマイズ

Cisco Secure ACS を使用すれば、各 Security Manager ロールに関連付けられた権限を変更できます。特定の Security Manager タスクを対象とする権限が付与された特殊なユーザ ロールを作成することによって、Cisco Secure ACS をカスタマイズすることもできます。

（注） ユーザ権限を変更したら、Security Manager を再起動する必要があります。

関連トピック

- 「Security Manager ACS 権限」（P.7-2）
- 「Security Manager 内の権限とロールのデフォルトの関連付け」（P.7-7）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Shared Profile Components] をクリックします。

ステップ 2　[Shared Components] ページで [Cisco Security Manager] をクリックします。Security Manager 用に設定されたロールが表示されます。

ステップ 3　次のいずれかを実行します。

- ロールを作成するには、[Add] をクリックします。ロールの名前を入力して、オプションで、説明を入力します。
- 既存のロールを変更するには、そのロールをクリックします。

ステップ 4　権限ツリー内のチェックボックスをオン/オフして、そのロールに対する権限を定義します。

ツリーのブランチに対応するチェックボックスをオンにすると、そのブランチ内のすべての権限が選択されます。たとえば、[Assign] チェックボックスをオンにすると、すべての割り当て権限が選択されます。

個々の権限に関する説明がウィンドウに表示されます。詳細については、「Security Manager ACS 権限」（P.7-2）を参照してください。

ヒント　変更、承認、割り当て、インポート、制御、または展開権限を選択した場合は、対応する表示権限も選択する必要があります。そうしなかった場合は、Security Manager が正しく機能しません。

ステップ 5　[Submit] をクリックして変更を保存します。

ステップ 6　Security Manager を再起動します。

Security Manager 内の権限とロールのデフォルトの関連付け

表 7-1 に、Security Manager 権限、CiscoWorks Common Services ロール、および Cisco Secure ACS 内のデフォルト ロールの関連付けを示します。特定の権限に関する詳細については、「Security Manager ACS 権限」（P.7-2）を参照してください。

表 7-1　Security Manager 内のデフォルトの権限とロールの関連付け

権限	ロール							
	システム管理者	セキュリティ管理者（ACS）	セキュリティ アプルーバ（ACS）	ネットワーク管理者（CW）	ネットワーク管理者（ACS）	アプルーバ	ネットワーク オペレータ	ヘルプ デスク
表示権限								
デバイスの表示	可	可	可	可	可	可	可	可
ポリシーの表示	可	可	可	可	可	可	可	可
オブジェクトの表示	可	可	可	可	可	可	可	可
トポロジの表示	可	可	可	可	可	可	可	可
CLI の表示	可	可	可	可	可	可	可	不可
管理設定の表示	可	可	可	可	可	可	可	不可
設定アーカイブの表示	可	可	可	可	可	可	可	可

表 7-1　Security Manager 内のデフォルトの権限とロールの関連付け（続き）

権限	ロール							
	システム管理者	セキュリティ管理者（ACS）	セキュリティ アプルーバ（ACS）	ネットワーク管理者（CW）	ネットワーク管理者（ACS）	アプルーバ	ネットワーク オペレータ	ヘルプ デスク
デバイス マネージャの表示	可	可	可	可	可	可	可	不可
変更権限								
デバイスの変更	可	可	不可	可	不可	不可	不可	不可
階層の変更	可	可	不可	可	不可	不可	不可	不可
ポリシーの変更	可	可	不可	可	不可	不可	不可	不可
イメージの変更	可	可	不可	可	不可	不可	不可	不可
オブジェクトの変更	可	可	不可	可	不可	不可	不可	不可
トポロジの変更	可	可	不可	可	不可	不可	不可	不可
管理設定の変更	可	不可	不可	不可	不可	不可	不可	不可
設定アーカイブの変更	可	可	不可	可	可	不可	可	不可
その他の権限								
ポリシーの割り当て	可	可	不可	可	不可	不可	不可	不可
ポリシーの承認	可	不可	可	不可	不可	不可	不可	不可
CLI の承認	可	不可	不可	不可	不可	可	不可	不可
検出（インポート）	可	可	不可	可	不可	不可	不可	不可
展開	可	不可	不可	可	可	不可	不可	不可
制御	可	不可	不可	可	可	不可	可	不可
送信	可	可	不可	可	不可	不可	不可	不可

Security Manager と Cisco Secure ACS の統合

この項では、Cisco Secure ACS と Cisco Security Manager の統合方法について説明します。

Cisco Secure ACS は、Security Manager などの管理アプリケーションを使用しているユーザに管理対象ネットワーク デバイスを設定するためのコマンド認可を提供します。コマンド認可に対するサポートは、一連の権限が含まれる一意のコマンド認可セット タイプ（Security Manager ではロールと呼ばれている）によって提供されます。これらの権限（特権とも呼ばれる）によって、特定のロールを持つユーザが Security Manager 内で実行できるアクションが決定されます。

Cisco Secure ACS は、TACACS+ を使用して管理アプリケーションと通信します。Security Manager と Cisco Secure ACS が通信するためには､Cisco Secure ACS 内の 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。加えて、CiscoWorks サーバに Cisco Secure ACS へのログインに使用する管理者名とパスワードを提供する必要があります。これらの要件を満たすことによって、Security Manager と Cisco Secure ACS 間の通信の有効性が保証されます。

（注）　TACACS+ のセキュリティ メリットを理解するには、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

Security Manager が初めて Cisco Secure ACS と通信するときに、デフォルト ロールの作成を Cisco ACS に指示します。このロールは、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ます。また、TACACS+ による認可をカスタム サービスに指示します。このカスタム サービスは、HTML インターフェイスの [Interface Configuration] セクション内の [TACACS+ (Cisco IOS)] ページに表示されます。その後で、各 Security Manager ロールに含まれる権限を変更したり、これらのロールをユーザとユーザ グループに適用したりできます。

次のトピックで、Cisco Secure ACS と Security Manager の使用方法について説明します。

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）
- 「Cisco Secure ACS で実行する統合手順」（P.7-11）
- 「CiscoWorks で実行する統合手順」（P.7-17）
- 「Daemon Manager の再起動」（P.7-21）
- 「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）

ACS 統合要件

Cisco Secure ACS を使用するには、次の手順を完了する必要があります。

- Security Manager 内で必要な機能を実行するために必要な権限を含むロールを定義しました。
- Network Access Restriction（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）が含まれています。
- 管理対象デバイス名は、Cisco Secure ACS と Security Manager で綴りと大文字/小文字を合わせる必要があります。この制限は、表示名に適用され、デバイス上で定義されるホスト名には適用されません。ACS の命名制限は Security Manager の命名制限よりも厳密なため、先に、ACS 内でデバイスを定義する必要があります。
- PIX/ASA セキュリティ コンテキスト、FWSM、および IPS デバイスに関して満たさなければならないその他のデバイス表示名要件があります。これらについては、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.7-13）に記載されています。

ヒント

- 複数の Cisco Secure ACS サーバを使用するフォールトトレラントなインフラストラクチャの構築を強く推奨します。複数のサーバを使用することによって、いずれかの ACS サーバの通信機能が失われても、Security Manager 内の作業が継続できることの保証が支援されます。
- Cisco Secure ACS と統合できるのは 1 つのバージョンの Security Manager だけです。そのため、組織で 2 つの異なるバージョンの Security Manager が同時に使用されている場合は、2 つの異なる Cisco Secure ACS サーバとの統合を実施する必要があります。ただし、別の ACS を使用しなくても、新しいバージョンの Security Manager にアップグレードできます。
- Cisco Secure ACS 認証が使用されている場合でも、CiscoWorks Common Services ソフトウェアは Compact Database や Database Checkpoint などの CiscoWorks Common Services 固有のユーティリティのローカル認可を使用します。これらのユーティリティを使用するには、ユーザをローカルに定義して、適切な権限を付与する必要があります。

関連トピック

- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）
- 「Security Manager と Cisco Secure ACS の統合」（P.7-8）

初期 Cisco Secure ACS セットアップ手順の概要

次の手順では、Cisco Secure ACS と Security Manager を使用して実行する必要のあるすべてのタスクの概要を示します。この手順には、各ステップの実行に使用されるより詳しい手順への参照が含まれています。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「Security Manager と Cisco Secure ACS の統合」（P.7-8）

ステップ 1　**管理認証および認可モデルを計画します。**

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、使用する予定の管理ロールとアカウントの定義も含まれます。

ヒント　潜在的管理者のロールと権限を定義するときに、イネーブルにするワークフローも考慮する必要があります。この選択は、アクセスの制限方法に影響します。

詳細については、次のマニュアルを参照してください。

- 「Cisco Secure ACS ロールについて」（P.7-5）
- 『*User Guide for Cisco Security Manager*』
- 『*User Guide for Cisco Secure Access Control Server*』

ステップ 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 をインストールします。別のサーバ上に CiscoWorks Common Services と Cisco Security Manager をインストールします。Cisco Secure ACS と Security Manager を同じサーバ上で実行しないでください。

詳細については、次のマニュアルを参照してください。

- 『*Release Notes for Cisco Security Manager*』（サポートされている Cisco Secure ACS のバージョンの詳細）
- 「Security Manager サーバ、Common Services、および AUS のインストール」（P.4-3）
- 『*Installation Guide for Cisco Secure ACS for Windows Server*』

ステップ 3　**Cisco Secure ACS で統合手順を実行します。**

Security Manager ユーザを ACS ユーザとして定義し、それらを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。

詳細については、「Cisco Secure ACS で実行する統合手順」（P.7-11）を参照してください。

ステップ 4　**CiscoWorks Common Services で統合手順を実行します。**

Cisco Secure ACS で定義されたシステム識別ユーザと一致するローカル ユーザを設定し、同じユーザをシステム識別セットアップ用に定義し、ACS を AAA セットアップ モードとして設定し、SMTP サーバとシステム管理者の電子メール アドレスを設定します。

詳細については、「CiscoWorks で実行する統合手順」（P.7-17）を参照してください。

ステップ 5　**Daemon Manager を再起動します。**

Security Manager サーバの Daemon Manager を再起動して、構成した AAA 設定を有効にします。

詳細については、「Daemon Manager の再起動」（P.7-21）を参照してください。

ステップ 6　**Cisco Secure ACS でユーザ グループにロールを割り当てます。**

Cisco Secure ACS で設定されたユーザ グループごとにロールを割り当てます。使用すべき手順は、Network Device Group（NDG; ネットワーク デバイス グループ）を設定したかどうかによって異なります。

詳細については、「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）を参照してください。

Cisco Secure ACS で実行する統合手順

次のトピックで、Cisco Security Manager と統合する場合に Cisco Secure ACS で実行すべき手順について説明します。列挙された順にタスクを実行します。これらの項で説明する手順の詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

1. 「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）
2. 「Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加」（P.7-13）
3. 「Cisco Secure ACS での管理制御ユーザの作成」（P.7-17）

Cisco Secure ACS でのユーザとユーザ グループの定義

Security Manager のすべてのユーザを Cisco Secure ACS で定義し、彼らの職務権限に応じたロールを割り当てる必要があります。この最も簡単な方法は、ACS で使用可能なデフォルト ロールに従ってユーザを複数のグループに分ける方法です。たとえば、すべてのシステム管理者をあるグループに割り当て、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といった具合です。ACS 内のデフォルト ロールの詳細については、「Cisco Secure ACS デフォルト ロール」（P.7-6）を参照してください。

デバイスに対するフル権限を持つシステム管理者ロールを割り当てる新しいユーザを作成する必要があります。このユーザに対して設定された資格情報が、後で、CiscoWorks の [System Identity Setup] ページで使用されます。「システム識別ユーザの定義」（P.7-18）を参照してください。

この段階で、ユーザを複数のグループに割り当てることはまれであることに注意してください。これらのグループに対する実際のロールの割り当ては、CiscoWorks、Security Manager、およびその他のアプリケーションが Cisco Secure ACS に登録された後で実行されます。

ヒント　この手順では、初期 Cisco Secure ACS 統合中のユーザ アカウントの作成方法について説明します。統合を完了したら、ユーザ アカウントを作成して、適切なグループに割り当てることができます。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）
- 「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）

ステップ 1　Cisco Secure ACS にログインします。

ステップ 2　次の手順を使用して、フル権限を持つユーザを設定します。ユーザとユーザ グループの設定時に使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

a. ナビゲーション バーの [User Setup] をクリックします。

b. [User Setup] ページで、新しいユーザの名前を入力して [Add/Edit] をクリックします。

ヒント　**admin** という名前のユーザは作成しないでください。admin ユーザは Security Manager のフォールバック ユーザです。ACS システムが何らかの理由で停止した場合は、admin アカウントを使用して Security Manager サーバ上の CiscoWorks Common Services にログインし、AAA モードを CiscoWorks ローカル認証に変更して、製品の使用を続けることができます。

c. [User Setup] の下の [Password Authentication] リストから認証方式を選択します。

d. 新しいユーザのパスワードを入力して確認します。

e. ユーザに割り当てるべきグループとして [Group 1] を選択します。

f. [Submit] をクリックしてユーザ アカウントを作成します。

ステップ 3　Security Manager ユーザごとにこのプロセスを繰り返します。ユーザは割り当てられたロールに基づいてグループに分けることを推奨します。

- 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 アプルーバ
- グループ 4：ネットワーク管理者
- グループ 5：アプルーバ
- 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たデフォルト権限の詳細については、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.7-7）を参照してください。ユーザ ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください。

（注）　この段階で、グループはどのロールも定義されていないユーザの集合でしかありません。統合プロセスが完了してから、各ユーザにロールを割り当てます。「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）を参照してください。

ステップ 4　CiscoWorks Common Services でシステム識別ユーザとして使用する新しいユーザを作成します。このユーザをシステム管理者グループに割り当て、デバイスに対するすべての特権を付与します。このユーザに対して設定された資格情報が、後で、CiscoWorks の [System Identity Setup] ページで使用されます。「システム識別ユーザの定義」（P.7-18）を参照してください。

ステップ 5　「Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加」（P.7-13）に進みます。

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

Security Manager にデバイスをインポートするには、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。加えて、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。

Security Manager が、Catalyst 6500/7600 デバイス用の FWSM を含むファイアウォール デバイス上で設定されたセキュリティ コンテキストを管理している場合は、それぞれのコンテキストを個別に Cisco Secure ACS に追加する必要があります。同様に、IPS デバイス上で定義されたすべての仮想センサーを追加する必要もあります。

管理対象デバイスを追加する方式は、NDG を作成して特定のデバイス セットの管理にユーザを制限するかどうかによって異なります。以下のように進めます。

- すべてのデバイスへのアクセスをユーザに許可する場合は、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.7-13）に記載されているようにデバイスを追加します。
- 特定の NDG へのアクセスだけをユーザに許可する場合は、「Security Manager で使用するネットワーク デバイス グループの設定」（P.7-14）に記載されているようにデバイスを追加します。

NDG を使用しないデバイスの AAA クライアントとしての追加

この手順では、デバイスを Cisco Secure ACS の AAA クライアントとして追加する方法について説明します。使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

ヒント　CiscoWorks/Security Manager サーバを AAA クライアントとして追加することを忘れないでください。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Network Configuration] をクリックします。

ステップ 2　[AAA Clients] テーブルの下で [Add Entry] をクリックします。

ステップ 3　[Add AAA Client] ページで AAA クライアントのホスト名（32 文字以下）を入力します。AAA クライアントのホスト名は、Security Manager 内でデバイスとして使用する予定の表示名と一致させる*必要があります*。

たとえば、Security Manager でドメイン名をデバイス名に付加する場合は、ACS 内の AAA クライアントのホスト名を **<device_name>.<domain_name>** にする必要があります。

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。ホスト名の綴りが正しいことを確認してください（ホスト名は大文字と小文字が区別されません）。

その他の命名規則を次に示します。

- PIX または ASA セキュリティ コンテキスト、あるいは、FWSM 経由で検出された FWSM セキュリティ コンテキスト：**<parent_display_name>_<context_name>**
- FWSM ブレード：**<chassis_name>_FW_<slot_number>**
- シャーシ経由で検出された FWSM セキュリティ コンテキスト：**<chassis_name>_FW_<slot_number>_<context_name>**
- IPS センサー：**<IPSParentName>_<virtualSensorName>**

ステップ 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。デバイスに IP アドレスが設定されていない場合（仮想センサーや仮想コンテキストなど）は、アドレスの代わりに単語の **dynamic** を入力します。

（注）　マルチホーム デバイス（複数の NIC が実装されたデバイス）を追加している場合は、各 NIC の IP アドレスを入力します。各アドレスの間で Enter を押します。加えて、Security Manager サーバ上の gatekeeper.cfg ファイルを変更する必要があります。

ステップ 5　[Key] フィールドに共有秘密キーを入力します。

ステップ 6　[Authenticate Using] リストから [TACACS+ (Cisco IOS)] を選択します。

ステップ 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] テーブル内に表示されます。

ステップ 8　このプロセスを繰り返して、新しいデバイスを追加します。

ステップ 9　追加したデバイスを保存するには、[Submit + Restart] をクリックします。

ステップ 10　「Cisco Secure ACS での管理制御ユーザの作成」（P.7-17）に進みます。

Security Manager 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 を使用すれば、特定の管理対象デバイスを含む NDG を設定できます。たとえば、地理的地域別の NDG や組織構造と一致する NDG を作成できます。NDG を Security Manager と一緒に使用すれば、管理対象デバイスに応じて、さまざまなレベルの権限をユーザに付与できます。たとえば、NDG を使用することによって、User A に、ヨーロッパに設置されたデバイスに対するシステム管理者権限とアジアに設置されたデバイスに対するヘルプ デスク権限を割り当てることができます。その後で、正反対の権限を User B に割り当てることができます。

NDG は直接ユーザに割り当てられません。それどころか、NDG は、ユーザ グループごとに定義されたロールに割り当てられます。各 NDG は 1 つのロールにしか割り当てることができませんが、各ロールに複数の NDG を含めることができます。これらの定義は、選択されたユーザ グループの定義の一部として保存されます。

ヒント

- 各デバイスは 1 つの NDG のメンバーにしかなれません。
- NDG は、Security Manager で設定可能なデバイス グループに*関連付けられません*。
- NDG の管理方法については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

次のトピックで、NDG の設定に関する基本的な情報とステップについて説明します。

NDG とユーザ権限

NDG はユーザを特定のデバイス セットに制限するため、次のように、ポリシー権限に影響します。

- ポリシーを表示するには、そのポリシーが割り当てられた少なくとも *1* つのデバイスに対する権限を持っている必要があります。
- ポリシーを変更するには、そのポリシーが割り当てられた*すべて*のデバイスに対する権限を持っている必要があります。
- VPN ポリシーを表示、変更、または割り当てるには、VPN トポロジ内の*すべて*のデバイスに対する権限を持っている必要があります。
- デバイスにポリシーを割り当てるには、ポリシーが割り当てられた他のデバイスに対する権限を持っているかどうかに関係なく、そのデバイスの権限のみが必要です（上述したように、VPN ポリシーは例外です）。ただし、権限を持っていないデバイスに割り当てられているポリシーを変更することはできません。

（注）　オブジェクトを変更するには、そのオブジェクトを使用しているすべてのデバイスに対する変更権限を持っている必要は*ありません*。ただし、そのデバイス上で定義されたデバイス レベルのオブジェクトの上書きを変更するには、特定のデバイスに対する変更権限を持っている必要があります。

関連トピック

- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.7-14）
- 「ユーザ権限のセットアップ」（P.7-1）

NDG 機能のアクティブ化

NDG を作成して、デバイスを追加するには、NDG 機能をアクティブにする必要があります。

関連トピック

- 「NDG の作成」（P.7-15）
- 「NDG とロールのユーザ グループへの関連付け」（P.7-22）
- 「NDG とユーザ権限」（P.7-15）
- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.7-14）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Interface Configuration] をクリックします。

ステップ 2　[Advanced Options] をクリックします。

ステップ 3　スクロール ダウンしてから、[Network Device Groups] チェックボックスをオンにします。

ステップ 4　[Submit] をクリックします。

ステップ 5　「NDG の作成」（P.7-15）に進みます。

NDG の作成

この手順では、NDG を作成して、デバイスを追加する方法について説明します。各デバイスは 1 つの NDG にしか属することができません。

ヒント　CiscoWorks/Security Manager サーバを含む特別な NDG を作成することを強く推奨します。

始める前に

「NDG 機能のアクティブ化」（P.7-15）に記載されているように、NDG 機能をアクティブにします。

関連トピック

- 「NDG とロールのユーザ グループへの関連付け」（P.7-22）
- 「NDG とユーザ権限」（P.7-15）
- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.7-14）

ステップ 1　ナビゲーション バーで、[Network Configuration] をクリックします。

最初は、すべてのデバイスが Not Assigned に配置されます。この場所には、NDG 内に存在しなかったすべてのデバイスが保存されます。Not Assigned は NDG でないことに注意してください。

ステップ 2　NDG を作成します。

a.　[Add Entry] をクリックします。

b.　[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。スペースを含めることができます。

c.　（オプション）NDG 内のすべてのデバイスで使用されるキーを入力します。NDG 用のキーを定義すると、NDG 内の個別のデバイスに対して定義されたすべてのキーが上書きされます。

d.　[Submit] をクリックして NDG を保存します。

e.　このプロセスを繰り返して、新しい NDG を作成します。

ステップ 3　NDG にデバイスを追加します。各デバイスは 1 つの NDG のメンバーにしかなれないことに注意してください。

a.　[Network Device Groups] エリアで、NDG の名前をクリックします。

b.　[AAA Clients] エリアで、[Add Entry] をクリックします。

c.　NDG に追加するデバイスの詳細を定義してから、[Submit] をクリックします。詳細については、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.7-13）を参照してください。

d.　このプロセスを繰り返して、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を検討すべき唯一のデバイスが、デフォルト AAA サーバです。

e.　最後のデバイスを設定したら、[Submit + Restart] をクリックします。

ステップ 4　「Cisco Secure ACS での管理制御ユーザの作成」（P.7-17）に進みます。

ヒント　Cisco Secure ACS と CiscoWorks Common Services の統合プロセスが完了しなければ、ロールを各 NDG に関連付けることができません。「NDG とロールのユーザ グループへの関連付け」（P.7-22）を参照してください。

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 の AAA セットアップ モードの定義に使用される管理者アカウントを定義します。Security Manager は、このアカウントを使用して、ACS サーバにアクセスしてアプリケーションを登録したり、デバイス グループ メンバシップとグループ セットアップを問い合わせたり、その他の基本的な ACS とのデータのやり取りを行ったりします。詳細については、「CiscoWorks での AAA セットアップ モードの設定」（P.7-19）を参照してください。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 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。

ステップ 2　[Add Administrator] をクリックします。

ステップ 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。

ステップ 4　次の管理者特権を選択します。

- [Users and Group Setup] の下
  - グループ内のユーザに対する読み取りアクセス
  - これらのグループの読み取りアクセス
- [Shared Profile Components] の下
  - デバイス コマンド セット タイプの作成
- ネットワーク設定

ステップ 5　[Submit] をクリックして管理者を作成します。管理者の設定時に使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

CiscoWorks で実行する統合手順

Cisco Secure ACS での統合タスク（「Cisco Secure ACS で実行する統合手順」（P.7-11）を参照）が完了したら、CiscoWorks Common Services でいくつかのタスクを完了する必要があります。Common Services は、Cisco Security Manager や Auto Update Server などのインストール対象アプリケーションの Cisco Secure ACS への登録を実行します。

次のトピックで、Cisco Security Manager と統合する場合に CiscoWorks Common Services で実行すべき手順について説明します。

- 「CiscoWorks でのローカル ユーザの作成」（P.7-18）
- 「システム識別ユーザの定義」（P.7-18）
- 「CiscoWorks での AAA セットアップ モードの設定」（P.7-19）
- 「ACS ステータス通知用の SMTP サーバとシステム管理者の電子メール アドレスの設定」（P.7-20）

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、Cisco Secure ACS で作成されたシステム識別ユーザ（「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）を参照）と全く同じローカル 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、システム識別セットアップに使用されます。詳細については、「システム識別ユーザの定義」（P.7-18）を参照してください。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 1　**admin** ユーザ アカウントを使用して CiscoWorks にログインします。

ステップ 2　Common Services で [Server] > [Security] を選択して、TOC から [Local User Setup] を選択します。

ヒント　Security Manager クライアントからこのページにアクセスするには、[Tools] > [Security Manager Administration] > [Server Security] を選択して [Local User Setup] をクリックします。

ステップ 3　[Add] をクリックします。

ステップ 4　Cisco Secure ACS でシステム識別ユーザを作成したときに入力したものと同じ名前とパスワードを入力します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）を参照してください。

ステップ 5　[Roles] の下のチェックボックスをすべてオンにします。

ステップ 6　[OK] をクリックしてユーザを作成します。

システム識別ユーザの定義

CiscoWorks Common Services の [System Identity Setup] ページを使用して、同じサーバ上に配置された同じドメインおよびアプリケーション プロセスに属しているサーバ間通信をイネーブルにする信頼ユーザ（システム識別ユーザと呼ばれる）を作成します。アプリケーションは、システム識別ユーザを使用して、リモート CiscoWorks サーバ上のプロセスを認証します。これは、特に、ユーザのログイン前に、アプリケーションの同期化が必要な場合に役立ちます。

加えて、システム識別ユーザは、プライマリ タスクがすでにログイン ユーザに対して認可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。

ここで設定したシステム識別ユーザは、CiscoWorks ではローカル ユーザとして（すべてのロールが割り当てられる）、ACS ではデバイスに対するすべての特権を持つユーザとして定義される必要もあります。必要な特権を持つユーザを選択しなかった場合は、Security Manager で設定されたすべてのデバイスとポリシーを表示できない可能性があります。先に進む前に次の手順を実行したことを確認してください。

- 「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）
- 「CiscoWorks でのローカル ユーザの作成」（P.7-18）

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 1　Common Services で、[Server] > [Security] を選択して、TOC から [Multi-Server Trust Management] > [System Identity Setup] を選択します。

ヒント　Security Manager クライアントからこのページにアクセスするには、[Tools] > [Security Manager Administration] > [Server Security] を選択して [System Identity Setup] をクリックします。

ステップ 2　Cisco Secure ACS で作成したシステム識別ユーザの名前を入力します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）を参照してください。

ステップ 3　このユーザのパスワードを入力して確認します。

ステップ 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

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

この手順は、CiscoWorks と Security Manager（およびオプションの Auto Update Server）の Cisco Secure ACS への登録を実行します。

ヒント　CiscoWorks Common Services または Cisco Security Manager をアンインストールした場合は、ここで設定した AAA セットアップが保存されません。加えて、この設定はバックアップして再インストール後に復元できません。そのため、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 モードを再設定して、Security Manager を ACS に再登録する必要があります。増分アップデートの場合は、このプロセスが必要ありません。AUS などの新しいアプリケーションを CiscoWorks 上にインストールする場合は、その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。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 1　Common Services で、[Server] > [Security] を選択して、TOC から [AAA Mode Setup] を選択します。

ヒント　Security Manager クライアントからこのページにアクセスするには、[Tools] > [Security Manager Administration] > [Server Security] を選択して [AAA Mode Setup] をクリックします。

ステップ 2　[Available Login Modules] の下で [TACACS+] を選択します。

ステップ 3　AAA タイプとして [ACS] を選択します。

ステップ 4　最大 3 つの Cisco Secure ACS サーバの IP アドレスを [Server Details] エリアに入力します。セカンダリ サーバとターシャリ サーバは、プライマリ サーバで障害が発生した場合のバックアップとして機能します。すべてのサーバで同じバージョンの Cisco Secure ACS が実行している必要があります。

（注）　設定されたすべての TACACS+ サーバが応答しなかった場合は、*admin* CiscoWorks ローカル アカウントを使用してログインしてから、AAA モードを Non-ACS/CiscoWorks Local に変更する必要があります。TACACS+ サーバのサービスが回復されたら、AAA モードを ACS に変更する必要があります。

ステップ 5　[Login] エリアで、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 での管理制御ユーザの作成」（P.7-17）を参照してください。

ステップ 6　この管理者のパスワードを入力して確認します。

ステップ 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 を使用しないデバイスの AAA クライアントとしての追加」（P.7-13）を参照してください。

ステップ 8　[Register all installed applications with ACS] チェックボックスをオンにして、Security Manager とその他のインストール済みアプリケーションを Cisco Secure ACS に登録します。

ステップ 9　[Apply] をクリックして設定値を保存します。経過表示バーに登録の進捗が表示されます。登録が完了するとメッセージが表示されます。

ステップ 10　Cisco Security Manager の Daemon Manager サービスを再起動します。「Daemon Manager の再起動」（P.7-21）を参照してください。

ステップ 11　Cisco Secure ACS に再ログインしてロールを各ユーザ グループに割り当てます。「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）を参照してください。

ACS ステータス通知用の SMTP サーバとシステム管理者の電子メール アドレスの設定

すべての ACS サーバが使用不能になった場合は、Security Manager でタスクを実行できません。ログイン ユーザは、ACS 認可が必要なタスクを実行しようとすると、強制的に（変更を保存する機会を与えられずに）アプリケーションからログアウトされます。

SMTP サーバとシステム管理者を識別するように Common Services を設定した場合は、すべての ACS サーバが使用不能になったときに、Security Manager から管理者に電子メール メッセージが送信されます。これによって、すぐに対処すべき問題が警告されます。管理者は、Common Services から非 ACS 関連イベントに関する電子メール メッセージを受け取ることもあります。

ヒント　Security Manager は、展開ジョブの完了、アクティビティの承認、ACL 規則の期限切れなどのイベント タイプに関する電子メール通知を送信できます。ここで設定する SMTP サーバはこれらの通知にも使用されますが、送信者の電子メール アドレスは Security Manager で設定されます。このような電子メール アドレスの設定方法については、このバージョンの製品の『*User Guide for Cisco Security Manager*』か、クライアントのオンライン ヘルプを参照してください。

ステップ 1　Common Services で、[Server] > [Admin] をクリックして、目次から [System Preferences] を選択します。

ステップ 2　[System Preferences] ページで、Security Manager が使用可能な SMTP サーバのホスト名または IP アドレスを入力します。SMTP サーバは、電子メール メッセージの送信に対してユーザ認証を要求できません。

ステップ 3　CiscoWorks が電子メールの送信に使用可能な電子メール アドレスを入力します。これは、Security Manager の通知の送信に使用される電子メール アドレスと同じにする必要はありません。

ACS サーバが使用不能になると、このアカウントに（およびこのアカウントから）メッセージが送信されます。

ステップ 4　[Apply] をクリックして、変更を保存します。

Daemon Manager の再起動

この手順では、Security Manager サーバの Daemon Manager の再起動方法について説明します。この操作は、構成した AAA 設定値を有効にするために行う必要があります。そうすれば、Cisco Secure ACS で定義された資格情報を使用して CiscoWorks に再ログインできます。

関連トピック

- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）
- 「ACS 統合要件」（P.7-9）

ステップ 1　Security Manager サーバがインストールされたマシンにログインします。

ステップ 2　[Start] > [Programs] > [Administrative Tools] > [Services] を選択して [Services] ウィンドウを開きます。

ステップ 3　右ペインに表示されたサービスのリストから、[Cisco Security Manager Daemon Manager] を選択します。

ステップ 4　ツールバーで [Restart Service] ボタンをクリックします。

ステップ 5　「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.7-21）に進みます。

Cisco Secure ACS でのユーザ グループへのロール割り当て

CiscoWorks、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 に登録したら、Cisco Secure ACS で設定したユーザ グループのそれぞれにロールを割り当てることができます。これらのロールによって、各グループ内のユーザが Security Manager で実行を許可されるアクションが決定されます。

ユーザ グループにロールを割り当てる手順は、NDG が使用されるかどうかによって異なります。

- 「NDG を使用しないユーザ グループへのロールの割り当て」（P.7-21）
- 「NDG とロールのユーザ グループへの関連付け」（P.7-22）

NDG を使用しないユーザ 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のユーザ グループへのデフォルト ロールの割り当て方法について説明します。詳細については、「Cisco Secure ACS デフォルト ロール」（P.7-6）を参照してください。

始める前に

- デフォルト ロールごとにユーザ グループを作成します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）を参照してください。

- 次のトピックに記載された手順を実行します。
  - 「Cisco Secure ACS で実行する統合手順」（P.7-11）
  - 「CiscoWorks で実行する統合手順」（P.7-17）

関連トピック

- 「CiscoWorks ロールについて」（P.7-3）
- 「Cisco Secure ACS ロールについて」（P.7-5）

ステップ 1　Cisco Secure ACS にログインします。

ステップ 2　ナビゲーション バーの [Group Setup] をクリックします。

ステップ 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（「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.7-11）を参照）してから、[Edit Settings] をクリックします。

ヒント　グループ名を意味のある名前に変更して、正しいグループを特定しやすいようにすることができます。グループを選択して、[Rename Group] をクリックし、名前を変更します。

ステップ 4　このグループにシステム管理者ロールを割り当てます。

a. [TACACS+ Settings] の下の [CiscoWorks] エリアまでスクロール ダウンします。

b. 最初の [Assign] オプションを選択して、CiscoWorks ロールのリストから [System Administrator] を選択します。

c. [Cisco Security Manager Shared Services] エリアまでスクロール ダウンします。

d. 最初の [Assign] オプションを選択して、Cisco Secure ACS ロールのリストから [System Administrator] を選択します。

e. [Submit] をクリックして、グループ設定を保存します。

ステップ 5　残りのロールに対してこのプロセスを繰り返して、各ロールを適切なユーザ グループに割り当てます。

Cisco Secure ACS でセキュリティ アプルーバ ロールまたはセキュリティ管理者ロールを選択するときは、最も近い CiscoWorks ロールとしてネットワーク管理者を選択することを推奨します。

ACS 内のデフォルト ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください。

NDG とロールのユーザ グループへの関連付け

NDG とロールを関連付けて Security Manager で使用する場合は、[Group Setup] ページの次の 2 か所で定義を作成する必要があります。

- [CiscoWorks] エリア
- [Cisco Security Manager] エリア

各エリア内の定義は、できるだけ細部まで一致する必要があります。CiscoWorks Common Services 内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、できるだけ近い定義を作成するようにします。

Security Manager で使用されるユーザ グループごとの関連付けを作成する必要があります。たとえば、西部地域のサポート担当者を含むユーザ グループがある場合は、そのユーザ グループを選択して、西部地域内のデバイスを含む NDG とヘルプ デスク ロールを関連付けることができます。

始める前に

NDG 機能をアクティブにして、NDG を作成します。「Security Manager で使用するネットワーク デバイス グループの設定」（P.7-14）を参照してください。

関連トピック

- 「ACS 統合要件」（P.7-9）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.7-10）

ステップ 1　ナビゲーション バーの [Group Setup] をクリックします。

ステップ 2　[Group] リストからユーザ グループを選択してから、[Edit Settings] をクリックします。

ヒント　グループ名を意味のある名前に変更して、正しいグループを特定しやすいようにすることができます。グループを選択して、[Rename Group] をクリックし、名前を変更します。

ステップ 3　CiscoWorks 内で使用する NDG とロールをマップします。

a. [Group Setup] ページで、[TACACS+ Settings] の下の [CiscoWorks] エリアまでスクロール ダウンします。

b. [Assign a Ciscoworks on a per Network Device Group Basis] を選択します。

c. [Device Group] リストから NDG を選択します。

d. この NDG を関連付けるべきロールを 2 つ目のリストから選択します。

e. [Add Association] をクリックします。関連付けが [Device Group] ボックスに表示されます。

f. このプロセスを繰り返して、新しい関連付けを作成します。

g. 関連付けを削除するには、[Device Group] からそれを選択して、[Remove Association] をクリックします。

ステップ 4　[Cisco Security Manager] エリアまでスクロール ダウンして、以前のステップで定義した関連付けにできるだけ近い関連付けを作成します。

（注）　Cisco Secure ACS でセキュリティ アプルーバ ロールまたはセキュリティ管理者ロールを選択するときは、最も近い CiscoWorks ロールとしてネットワーク管理者を選択することを推奨します。

ステップ 5　[Submit] をクリックして設定値を保存します。

ステップ 6　このプロセスを繰り返して、残りのユーザ グループ用の NDG を定義します。

ステップ 7　作成した関連付けを保存するには、[Submit + Restart] をクリックします。

ACS 内のデフォルト ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.7-6）を参照してください。

Security Manager と ACS の相互作用のトラブルシューティング

次のトピックで、Security Manager と Cisco Secure ACS の相互作用のやり方が原因で発生する可能性のある一般的な問題の解決方法について説明します。

複数のバージョンの Security Manager と 1 つの ACS の使用

1 つの Cisco Secure ACS と 2 つの異なるバージョンの Security Manager を一緒に使用できません。たとえば、Security Manager 3.3.1 と Cisco Secure ACS を統合してから、別の部署で既存のインストールをアップグレード*せずに* Security Manager 4.0 の使用を計画している場合は、Security Manager 4.0 と、Security Manager 3.3.1 用に使用されているものとは別の ACS を統合する必要があります。

既存の Security Manager インストールをアップグレードすれば、同じ Cisco Secure ACS を使用し続けることができます。必要に応じて、権限設定が更新されます。

ACS モードで認証に失敗する

Security Manager または CiscoWorks Common Services にログインしようとして続けて認証が失敗する場合は、Common Services を使用して Cisco Secure ACS を認証用の AAA サーバとして設定していたとしても、次の手順を実行します。

- ACS サーバと、Common Services と Security Manager を実行しているサーバ間の接続が確立されていることを確認します。
- 使用しているユーザ資格情報（ユーザ名とパスワード）が ACS 内で定義されており、適切なユーザ グループに割り当てられていることを確認します。
- ACS の [Network Configuration] ページで、Common Services サーバが AAA クライアントとして定義されていることを確認します。Common Services（[AAA Mode Setup] ページ）と ACS（[Network Configuration]）で定義された共有秘密キーが一致することを確認します。
- Common Services の [AAA Mode Setup] ページで、各 ACS サーバの IP アドレスが正しく定義されていることを確認します。
- ACS の [Administration Control] ページで、正しいアカウントが定義されていることを確認します。

- Common Services の [AAA Mode Setup] ページにアクセスして、Common Services と Security Manager（および AUS などの他のインストール済みアプリケーション）が Cisco Secure ACS に登録されていることを確認します。
- ACS で [Administration Control] > [Access Setup] に移動して、ACS が HTTPS 通信用に設定されていることを確認します。
- ACS ログに「key mismatch」エラーが書き込まれている場合は、Security Manager サーバが NDG のメンバーとして定義されているかどうかを確認します。その場合は、NDG 用のキーが事前に定義されていれば、そのキーが Security Manager サーバを含む NDG 内の個々のデバイスに対して定義されたキーよりも優先されることに注意してください。NDG 用に定義されたキーが、Security Manager サーバの秘密キーと一致することを確認します。

読み取り専用アクセスが付与されたシステム管理者

フル権限を持つシステム管理者としてログインしたにもかかわらず、Security Manager のすべてのポリシー ページに読み取り専用アクセスしかできない場合は、Cisco Secure ACS で次の手順を実行します。

- （NDG を使用している場合）Cisco Secure ACS のナビゲーション バーの [Group Setup] をクリックしてから、システム管理者ユーザ ロールが CiscoWorks と Cisco Security Manager の*両方*の必要なすべての NDG（特に、Common Services/Security Manager サーバを含む NDG）に関連付けられていることを確認します。
- ナビゲーション バーの [Network Configuration] をクリックしてから、次の手順を実行します。
  - Common Services/Security Manager サーバが Not Assigned（デフォルト）グループに割り当てられていないことを確認します。
  - Common Services/Security Manager サーバが RADIUS ではなく TACACS+ を使用するように設定されていることを確認します。TACACS+ は、2 台のサーバ間でサポートされている唯一のセキュリティ プロトコルです。

（注）　TACACS+ または RADIUS 用に Security Manager で管理するネットワーク デバイス（ルータ、スイッチ、ファイアウォールなど）を設定できます。

ACS の変更が Security Manager に表示されない

Security Manager と Cisco Secure ACS 4.x を使用している場合は、Security Manager サーバ上の Security Manager または CiscoWorks Common Services にログインしたときに ACS からの情報がキャッシュされます。Security Manager にログイン中に Cisco Secure ACS の [Network Configuration] と [Group Setup] で変更を加えた場合は、Security Manager で、その変更が、すぐに表示されない、または、すぐに有効にならない可能性があります。Security Manager と Common Services をログアウトしてそれらのウィンドウを閉じてから、再度ログインして、ACS からの情報をリフレッシュする必要があります。

ACS で変更を加える必要がある場合は、ログアウトして Security Manager ウィンドウを閉じてから、製品に再ログインする方法がベスト プラクティスです。

（注）　Cisco Secure ACS 3.3 はサポートされていませんが、このバージョンの ACS を使用している場合は、Windows サービスを開いて Cisco Security Manager Daemon Manager サービスを再起動し、ACS の変更を Security Manager に表示させる必要があります。

ACS で設定されたデバイスが Security Manager に表示されない

Cisco Secure ACS 上で設定したデバイスが Security Manager に表示されない場合は、デバイスの表示名に伴う問題だと思われます。

Security Manager で定義するデバイスの表示名は、そのデバイスを AAA クライアントとして追加したときに ACS で設定した名前と一致する*必要があります*。このことは、特に、ドメイン名を使用する場合に重要です。Security Manager でドメイン名をデバイス名に付加する場合は、ACS 内の AAA クライアントのホスト名を **<device_name>.<domain_name>** にする必要があります（例：pixfirewall.cisco.com）。

Cisco Secure ACS が到達不能になった後の Security Manager での作業

Cisco Secure ACS が到達不能な場合は、Security Manager セッションが影響を受けます。そのため、複数の Cisco Secure ACS サーバを使用するフォールトトレラントなインフラストラクチャの構築を検討する必要があります。複数のサーバを使用することによって、いずれかの ACS サーバの通信機能が失われても、Security Manager 内の作業が継続できることの保証が支援されます。

セットアップに Cisco Secure ACS が 1 つしか含まれておらず、ACS が到達不能になった場合でも Security Manager での作業を継続する場合は、Security Manager サーバ上でのローカル AAA 認証に切り替えることができます。

手順

AAA モードに変更するには、次の手順を実行します。

ステップ 1　**admin** CiscoWorks ローカル アカウントを使用して Common Services にログインします。

ステップ 2　[Server] > [Security] > [AAA Mode Setup] を選択してから、AAA モードを Non-ACS/CiscoWorks Local に変更します。これによって、ローカル Common Services データベースとその組み込みロールを使用して認証と認可を実行できます。ローカル認証を利用するには、AAA データベース内にローカル ユーザを作成する必要があります。

ステップ 3　[Change] をクリックします。

Cisco Secure ACS へのアクセスの復元

Cisco Secure ACS がダウンしたために Security Manager にアクセスできなくなった場合は、次の手順を実行します。

- ACS サーバ上で Windows サービスを起動して、CSTacacs サービスと CSRadius サービスが稼動しているかどうかを確認します。必要に応じて、これらのサービスを再起動します。
- CiscoWorks Common Services で次の手順を実行します。

ステップ 1　**admin** ユーザとして Common Services にログインします。

ステップ 2　DOS ウィンドウを開いて、*NMSROOT*¥**bin¥perl ResetLoginModule.pl** を実行します。

ステップ 3　Common Services を終了してから、**admin** ユーザとして再度ログインします。

ステップ 4　[Server] > [Security] > [AAA Mode Setup] に移動してから、AAA モードを [Non-ACS] > [CW Local] モードに変更します。

ステップ 5　Windows サービスを開いて、Cisco Security Manager Daemon Manager サービスを再起動します。

マルチホーム デバイスに伴う認証の問題

Cisco Secure ACS に追加されたマルチホーム デバイス（複数の Network Interface Card（NIC）が実装されたデバイス）が設定できない場合は、ユーザ ロールにデバイスの変更権限が含まれていたとしても、そのデバイスの IP アドレスの入力方法に伴う問題が発生する可能性があります。

マルチホーム デバイスを Cisco Secure ACS の AAA クライアントとして定義する場合は、NIC ごとの IP アドレスを定義してください。入力するたびに Enter を押します。詳細については、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.7-13）を参照してください。

NAT 境界の背後に設置されたデバイスに伴う認証の問題

Cisco Secure ACS に追加された NAT 前または NAT 後の IP アドレスを持つデバイスを設定できない場合は、ユーザ ロールにデバイスの変更権限が含まれていたとしても、設定した IP アドレスに伴う問題が発生する可能性があります。

デバイスが NAT 境界の背後に設置されている場合は、Cisco Secure ACS の AAA クライアント設定でデバイスのすべての IP アドレス（NAT 前と NAT 後を含む）を定義してください。ACS への AAA クライアント設定の追加方法については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。