CHAPTER 7

ネットワーク リソースの管理

[Network Resources] ドロワでは、ACS に要求を発行するネットワーク内の要素、または要求処理の一環として ACS が対話する要素が定義されます。これらの要素には、要求を発行するネットワーク デバイス、および RADIUS プロキシとして使用される RADIUS サーバなどの外部サーバが含まれます。

ドロワを使用して、次の内容を設定できます。

- ネットワーク デバイス グループ：ネットワーク デバイスの論理的なグループ。設定すると、ポリシー条件で使用できます。
- ネットワーク デバイス：ACS ネットワークにアクセスする、ACS デバイス リポジトリ内のすべてのネットワーク デバイスの定義。
- デフォルトのネットワーク デバイス：特定の IP アドレスのデバイス定義が ACS で見つからなかった場合に、ACS によって RADIUS 要求または TACACS+ 要求に使用されるデフォルトのネットワーク デバイス定義。
- 外部プロキシ サーバ：RADIUS プロキシとして使用できる RADIUS サーバ。
- OCSP サービス：Online Certificate Status Protocol（OCSP）サービスが x.509 デジタル証明書の状態を検査するために使用され、証明書失効リスト（CRL）への代替として使用できます。

ネットワーク デバイスからネットワークへのアクセス要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、IP アドレスが一致するエントリを見つけます。次に、ACS はネットワーク デバイス定義から取得した秘密情報を共有秘密情報と比較します。

これらの情報が一致する場合は、そのネットワーク デバイスに関連付けられているネットワーク デバイス グループが取得され、ポリシー決定で使用できるようになります。ポリシー決定の詳細については、「「ACS 5.x ポリシー モデル」」を参照してください。

[Network Resources] ドロワには、次の項目が含まれています。

ネットワーク デバイス グループ

ACS では、デバイスのセットであるネットワーク デバイス グループ（NDG）を定義できます。NDG を使用すると、デバイスを論理的にグループ化でき（デバイスの場所、タイプなど）、それらのグループをポリシー条件で使用できます。

ACS では、デバイスの要求を受信すると、そのデバイスに関連付けられているネットワーク デバイス グループが取得され、ポリシー テーブルのネットワーク デバイス グループと比較されます。この方法を使用すると、複数のデバイスをグループ化し、同じポリシーを割り当てることができます。たとえば、特定の場所にあるすべてのデバイスをグループ化して、同じポリシーを割り当てることができます。

デバイス グループ階層は、ネットワーク デバイス グループが含まれた階層構造です。これらの 2 つ、つまり *Location* と *Device Type* は事前定義済みで、その名前は編集できますが、削除することはできません。ルートを含む最大 6 個の追加階層を追加できます。

NDG は、階層内の任意のノードと関連し、デバイスが関連付けられているエンティティです。これらのノードには、リーフノードだけでなく、階層内のあらゆるノードが該当します。

（注） ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。

関連トピック

- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）

ネットワーク デバイス グループの作成、複製、および編集

ネットワーク デバイス グループを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。追加のネットワーク デバイス グループを定義済みである場合は、それらのグループが [Network Device Groups] オプションの下の左側のナビゲーション ペインに表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するネットワーク デバイス グループの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス グループ名をクリックします。または、名前の隣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。

[Hierarchy - General] ページが表示されます。

ステップ 3　表 7-1 の説明に従って、[Hierarchy - General] ページのフィールドを変更します。

表 7-1　[Device Groups - General] ページのフィールド説明

フィールド	説明
Name	ネットワーク デバイス グループ（NDG）の名前を入力します。

表 7-1　[Device Groups - General] ページのフィールド説明 （続き）

Description	（任意）NDG の説明を入力します。
Root Node Name/Parent	NDG に関連付けられているルート ノードの名前を入力します。NDG は、反転ツリーとして構造化されており、ルート ノードは反転ツリーの最上部にあります。ルート ノード名には、NDG と同じ名前を指定できます。 NDG 名は、[Network Resources] ドロワで NDG をクリックすると表示されます。

ステップ 4　[Submit] をクリックします。

ネットワーク デバイス グループの設定が保存されます。[Network Device Groups] ページが表示され、新しいネットワーク デバイス グループ設定が示されます。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）
- 「階層内でのネットワーク デバイス グループの作成、複製、および編集」（P.7-4）
- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）

ネットワーク デバイス グループの削除

ネットワーク デバイス グループを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　削除するネットワーク デバイス グループの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
You have requested to delete a network device group. If this group is referenced from a
Policy or a Policy Element then the delete will be prohibited. If this group is referenced
from a network device definition, the network device will be modified to reference the
root node name group.
```

ステップ 3　[OK] をクリックします。

[Network Device Groups] ページが表示されます。このとき、削除されたネットワーク デバイス グループは表示されません。

階層内でのネットワーク デバイス グループの作成、複製、および編集

新しいネットワーク デバイス グループ ノード、または複製および編集されたネットワーク デバイス グループ ノードに対して親と子の関係を選択することによって、ネットワーク デバイス グループ ノード階層をニーズに従って配置できます。また、ネットワーク デバイス グループ ノードを階層から削除することもできます。

階層内でネットワーク デバイス グループ ノードを作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　新しいネットワーク デバイス グループを作成する [Location]、[Device Type]、または定義済みの別のネットワーク デバイス グループをクリックし、そのグループの階層に追加します。

[Network Device Group] 階層ページが表示されます。

ステップ 3　次のいずれかを実行します。

- [Create] をクリックします。選択済みのグループが存在する場合に [Create] をクリックすると、新しいグループは、選択済みの親グループの子になります。[Create] 画面で [Select] を選択して、階層内の親およびそのすべての子を移動できます。
- 複製するネットワーク デバイス グループ名の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス グループ名をクリックします。または、名前の隣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。

[Device Group - General] ページが表示されます。

ステップ 4　表 7-2 に従い、[Device Groups - General] ページのフィールドを変更します。

表 7-2　[Device Groups - General] ページのフィールド説明

フィールド	説明
Name	NDG の名前を入力します。
Description	（任意）NDG の説明を入力します。
Parent	NDG に関連付けられている親の名前を入力します。NDG は反転ツリーとして構造化されており、親の名前がツリーの最上部の名前となります。 [Select] をクリックして、[Groups] ダイアログボックスを開きます。このダイアログボックスで、グループの適切な親を選択できます。

ステップ 5　[Submit] をクリックします。

ネットワーク デバイス グループの新しい設定が保存されます。[Network Device Groups] 階層ページが表示され、新しいネットワーク デバイス グループ設定が示されます。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）

階層からのネットワーク デバイス グループの削除

ネットワーク デバイス グループを階層から削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　ネットワーク デバイス グループ ノードを編集する必要がある [Location]、[Device Type]、または定義済みの別のネットワーク デバイス グループをクリックします。

[Network Device Groups] ノード階層ページが表示されます。

ステップ 3　削除するノードを選択し、[Delete] をクリックします。

次のメッセージが表示されます。

```
You have requested to delete a network device group. If this group is referenced from a
Policy or a Policy Element then the delete will be prohibited. If this group is referenced
from a network device definition, the network device will be modified to reference the
root node name group.
```

ステップ 4　[OK] をクリックします。

（注）　グループのルート ノードは、NDG 階層から削除できません。削除しようとすると、次のエラー メッセージが表示されます。

```
Selected node can be removed only with a root group.
```

ネットワーク デバイス グループ ノードが設定から削除されます。[Network Device Groups] 階層ページが表示されます。このとき、削除したデバイス グループ ノードは表示されません。

ネットワーク デバイスおよび AAA クライアント

ネットワークにアクセスする、ACS デバイス リポジトリ内のすべてのデバイスを定義する必要があります。ネットワーク デバイス定義は、特定の IP アドレス、またはサブネット内のすべての IP アドレスがネットワークにアクセスできるサブネット マスクに関連付けることができます。

デバイス定義には、ネットワーク デバイス グループ（NDG）へのデバイスの関連付けが含まれています。デバイスが TACACS+ または RADIUS を使用するかどうか、およびデバイスが Security Group Access デバイスであるかどうかも設定します。

（注）　サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。

デバイスおよびその設定をネットワーク デバイス リポジトリにインポートできます。

要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、一致する IP アドレスを持つデバイスを見つけ、次に、その秘密情報やパスワード情報をネットワーク デバイス定義から取得した情報と比較します。情報が一致すると、そのデバイスと関連付けられている NDG が取得され、ポリシー決定で使用されます。

Security Group Access のオプションをイネーブルにするには、Security Group Access ライセンスをインストールする必要があります。Security Group Access のオプションは Security Group Access ライセンスをインストールした場合にだけ表示されます。Security Group Access ライセンスの詳細については、「ライセンスの概要」（P.18-35）を参照してください。

ネットワーク デバイスの一括操作の表示および実行

ネットワーク デバイスおよび AAA クライアントを表示できます。これらは、ACS にアクセス要求を送信するデバイスです。アクセス要求は、TACACS+ または RADIUS を介して送信されます。

ネットワーク デバイスを表示およびインポートするには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Device] ページが表示され、すべての設定済みネットワーク デバイスが示されます。表 7-3 に、[Network Device] ページのフィールドの説明を示します。

表 7-3　[Network Device] ページのフィールドの説明

オプション	説明
Name	ACS でのユーザ指定のネットワーク デバイス名。名前をクリックして、関連付けられているネットワーク デバイスを編集します（「ネットワーク デバイス プロパティの表示」（P.7-15）を参照）。
IP Address	*表示のみ*。各ネットワーク デバイスの IP アドレスまたはサブネット マスクです。IPv4 または IPv6 タイプの最初の 3 個の IP アドレスがフィールドにそれぞれカンマ（,）で区切られて表示されます。 このフィールドにサブネット マスクが含まれている場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。次に例を示します。 IPv4：サブネットマスク 255.255.255.0 は 256 個の固有の IPv4 アドレスがあることを意味します。デフォルトでは、IPv4 のサブネット マスクの値は 32 です。 IPv6：サブネット マスク 2001:0DB8:0:CD30::/127 は 2 個の固有の IPv6 アドレスがあることを意味します。デフォルトでは、IPv6 のサブネット マスクの値は 128 です。 指定された IP アドレスの横に、除外された IP アドレスがある場合はそれを表示できます。
NDG: *string*	ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。追加のネットワーク デバイス グループを定義済みである場合は、それらのグループもここに示されます。
Description	*表示のみ*。ネットワーク デバイスの説明。

ステップ 2　次のいずれかを実行します。

- 新しいネットワーク デバイスを作成するには、[Create] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。
- 編集するネットワーク デバイスの隣にあるチェックボックスをオンにし、[Edit] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。

- 複製するネットワーク デバイスの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。
- 次のカテゴリに基づいてネットワーク デバイスを検索できます。
  - Name
  - IP Address
  - Description
  - NDG Location
  - Device Type

  完全な IP アドレス、またはワイルドカード「*」や [15-20] のような IP アドレス範囲を使用した IP アドレスを IP アドレスの検索フィールドに指定できます。ワイルドカード「*」と IP 範囲 [15-20] オプションは IP アドレスのすべての 4 オクテットに指定できます。IP アドレスで検索する場合は、[Equal] オプションのみが検索条件に表示されます。

（注）　IP アドレスまたは IP 範囲のアドレスを検索する際、検索結果は、検索の IP アドレス（または）IP 範囲のアドレスが除外された IP アドレス（または）範囲にある場合でも、検索条件に一致するすべてのレコードを表示します。

- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - Add：インポート ファイルからネットワーク デバイスのリストを単一ショットに追加する場合は、このオプションを選択します。
  - Update：ACS でのネットワーク デバイスのリストをインポート ファイル内のネットワーク デバイスに置き換えるには、このオプションを選択します。
  - Delete：インポート ファイルでリストされているネットワーク デバイスを ACS から削除するには、このオプションを選択します。

  詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

インポート ファイルの作成方法については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1055255.

ワンポイントアドバイス

ACS オブジェクトに対する一括での追加、編集、または削除操作を実行するには、そのオブジェクトのエクスポート ファイルを使用し、ヘッダー行を保持して、.csv インポート ファイルを作成できます。ただし、更新された名前または MAC アドレスを ACS オブジェクトに追加する場合は、特定の更新テンプレートをダウンロードして使用してください。また、NDG の場合、エクスポート テンプレートには NDG 名だけが含まれているため、他のプロパティを更新するには、NDG 更新テンプレートをダウンロードして使用してください。

関連トピック：

- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）
- 「階層内でのネットワーク デバイス グループの作成、複製、および編集」（P.7-4）

ネットワーク デバイスおよび AAA クライアントのエクスポート

（注）　エクスポート プロセスが正常に完了するように、ブラウザのポップアップ ブロッカーをオフにする必要があります。

ネットワーク デバイスのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Device] ページが表示されます。

ステップ 2　フィルタ条件および if 演算子 Match を選択し、検索するフィルタ基準をテキスト ボックスに入力します。

ステップ 3　[Go] をクリックします。

フィルタ基準と一致するレコードのリストが表示されます。このリストを .csv ファイルにエクスポートできます。

ステップ 4　[Export] をクリックして、レコードを .csv ファイルにエクスポートします。

システム メッセージ ボックスが表示され、ファイル転送中に .csv ファイルを暗号化するための暗号化パスワードを要求するプロンプトが表示されます。

エクスポート .csv ファイルを暗号化するには、[Password] チェックボックスをオンにして暗号化パスワードを入力します。任意で、転送中にファイルを暗号化しないことを選択できます。

ステップ 5　[Start Export] をクリックして、エクスポート プロセスを開始します。

[Export Progress] ウィンドウが表示され、エクスポート プロセスの進行状況が表示されます。このプロセスでエラーが発生した場合は、そのエラーが [Export Progress] ウィンドウに表示されます。

エクスポート プロセスは、このプロセス中にいつでも終了することができます。エクスポート プロセスを打ち切るまでのすべてのレポートがエクスポートされます。再開するには、エクスポート プロセスを最初からやり直す必要があります。

ステップ 6　エクスポート プロセスの完了後、[Save File] をクリックして、エクスポート ファイルをローカル ディスクに保存します。

エクスポート ファイルは、export.zip として圧縮された .csv ファイルです。

ネットワーク リソースおよびユーザに関する一括操作の実行

ファイル操作機能を使用して、データベースで次の項目に対して一括操作（追加、更新、および削除）を実行できます。

- 内部ユーザ
- 内部ホスト
- ネットワーク デバイス

一括操作の場合は、ACS から .csv ファイル テンプレートをダウンロードし、追加、更新、または削除するレコードを .csv ファイルに追加し、そのファイルをローカル ディスクに保存する必要があります。Download Template 機能を使用して、.csv ファイルが要件に準拠するようにします。

ユーザ、内部ホスト、およびネットワーク デバイス用の .csv テンプレートは、それぞれのタイプに固有のテンプレートです。たとえば、[Users] ページからアクセスしてダウンロードしたテンプレートは、内部ホストやネットワーク デバイスの追加には使用できません。.csv ファイルは次の要件に準拠している必要があります。

- 最初のレコード（.csv ファイルの最初の行）の内容は変更しないでください。
- 各レコードに対して使用するのは 1 行だけです。
- フィールドに改行文字を埋め込まないでください。
- 英語以外の言語では、.csv ファイルを utf-8 符号化で符号化するか、Unicode をサポートするフォントを使用して保存します。

一括操作を開始する前に、ブラウザのポップアップ ブロッカーがディセーブルになっていることを確認します。

ステップ 1　Web インターフェイスの [Users]、[Network Devices]、または [MAC Address] ページで、[File Operations] をクリックします。

[Operation] ダイアログボックスが表示されます。

ステップ 2　.csv ファイル テンプレートがない場合は、[Next] をクリックして、.csv ファイル テンプレートをダウンロードします。

ステップ 3　テンプレートベースの .csv ファイルをローカル ディスクにすでに作成している場合は、次の操作のいずれかをクリックします。

- Add：.csv ファイル内のレコードを、ACS で現在使用可能なレコードに追加します。
- Update：ACS のレコードを .csv ファイルのレコードで上書きします。
- Delete：.csv ファイル内のレコードを ACS のリストから削除します。

ステップ 4　[Next] をクリックして、次のページに移動します。

ステップ 5　[Browse] をクリックして、.csv ファイルに移動します。

ステップ 6　インポート プロセス時にエラーが発生した場合に ACS で実行するオプションを次の中から選択します。

- 残りのレコードの処理を続行します。処理に成功したレコードだけがインポートされます。
- 残りのレコードの処理を停止します。エラーの発生前にインポートが成功したレコードだけがインポートされます。

ステップ 7　.csv ファイルが GPG 形式で暗号化されている場合は、[Password] チェックボックスをオンにして、.csv ファイルを暗号化するためのパスワードを入力します。

ステップ 8　[Finish] をクリックして、一括操作を開始します。

[Import Progress] ウィンドウが表示されます。このウィンドウを使用して、一括操作の進行状況を監視します。.csv ファイルのレコードのデータ転送失敗が表示されます。

[Abort] ボタンをクリックして、進行中のデータのインポートを停止できますが、転送に成功したデータはデータベースから削除されません。

操作が完了すると、[Save Log] ボタンがイネーブルになります。

ステップ 9　[Save Log] をクリックして、ログ ファイルをローカル ディスクに保存します。

ステップ 10　[OK] をクリックして、[Import Progress] ウィンドウを閉じます。

システムに一度に送信できる .csv ファイルは 1 つだけです。操作が進行中である場合、追加の操作は、最初の操作が完了するまで成功しません。

インポート ファイルの作成方法については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1055255.

ワンポイントアドバイス　ACS オブジェクトに対する一括での追加、編集、または削除操作を実行するには、そのオブジェクトのエクスポート ファイルを使用し、ヘッダー行を保持して、.csv インポート ファイルを作成できます。ただし、更新された名前または MAC アドレスを ACS オブジェクトに追加するには、特定の更新テンプレートをダウンロードして使用してください。また、NDG の場合、エクスポート テンプレートには NDG 名だけが含まれているため、他のプロパティを更新するには、NDG 更新テンプレートをダウンロードして使用してください。

ネットワーク リソースおよびユーザのエクスポート

ネットワーク リソースまたはユーザのリストをエクスポートするには、次の手順を実行します。

ステップ 1　Web インターフェイスの [Users]、[Network Devices]、または [MAC Address] ページで、[Export] をクリックします。

[Network Device] ページが表示されます。

ステップ 2　フィルタ条件および if 演算子 Match を選択し、検索するフィルタ基準をテキスト ボックスに入力します。

ステップ 3　[Go] をクリックします。

フィルタ基準と一致するレコードのリストが表示されます。これらのレコードを .csv ファイルにエクスポートできます。

ステップ 4　[Export] をクリックして、レコードを .csv ファイルにエクスポートします。

システム メッセージ ボックスが表示され、ファイル転送中に .csv ファイルを暗号化するための暗号化パスワードを要求するプロンプトが表示されます。

エクスポート .csv ファイルを暗号化するには、[Password] チェックボックスをオンにして暗号化パスワードを入力します。任意で、転送中にファイルを暗号化しないことを選択できます。

ステップ 5　[Start Export] をクリックして、エクスポート プロセスを開始します。

[Export Progress] ウィンドウが表示され、エクスポート プロセスの進行状況が表示されます。このプロセスでエラーが発生した場合は、そのエラーが [Export Progress] ウィンドウに表示されます。

エクスポート プロセスは、このプロセス中にいつでも終了することができます。エクスポート プロセスを終了すると、終了までのすべてのレポートがエクスポートされます。再開する場合は、エクスポート プロセスを最初からやり直す必要があります。

ステップ 6　エクスポート プロセスの完了後、[Save File] をクリックして、エクスポート ファイルをローカル ディスクに保存します。

エクスポート ファイルは、export.zip として圧縮された .csv ファイルです。

ネットワーク デバイスの作成、複製、および編集

一括インポート機能を使用すると、多数のネットワーク デバイスを 1 回の操作でインポートできます。詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。または、このトピックで説明する手順を使用して、ネットワーク デバイスを作成できます。

ネットワーク デバイスを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Devices] ページが表示され、設定済みのネットワーク デバイスがある場合は、そのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するネットワーク デバイス名の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス名をクリックします。または、名前の隣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。

新しいネットワーク デバイスを作成している場合は、ネットワーク デバイス作成プロセスの最初のページが表示されます。ネットワーク デバイスを複製または編集している場合は、選択したデバイスの [Network Device Properties] ページが表示されます。

ステップ 3　必要に応じてフィールドを変更します。フィールドの説明については、「ネットワーク デバイスおよび AAA クライアントの設定」（P.7-11）を参照してください。

ステップ 4　[Submit] をクリックします。

新しいネットワーク デバイス設定が保存されます。[Network Devices] ページが表示され、新しいネットワーク デバイス設定が示されます。

関連トピック

- 「ネットワーク デバイスの一括操作の表示および実行」（P.7-6）
- 「ネットワーク デバイスおよび AAA クライアントの設定」（P.7-11）

ネットワーク デバイスおよび AAA クライアントの設定

このページを表示するには、[Network Resources] > [Network Devices and AAA Clients] を選択してから、[Create] をクリックします。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成

オプション	説明
General	
Name	ネットワーク デバイスの名前。ネットワーク デバイスを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Description	ネットワーク デバイスの説明。
Network Device Groups	

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
Location	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Location ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
IP Address ネットワーク デバイスに関連付けられる IP アドレスとサブネット マスク。単一の IP アドレスを入力するか、範囲を定義するかを選択します。	
Single IP Address	単一の IP アドレスを入力することを選択します。IP アドレスは IPv4 または IPv6 にできます。アドレスがサポートされる形式で入力されると、ACS 5.4 はその IP アドレスを検証します。入力された形式が正しくない場合は、エラー メッセージを表示します。 **（注）**　IPv6 アドレスは、TACACS+ プロトコルだけでサポートされています。
IP Range(s) By Mask	IP アドレス範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。このフィールドでサブネット マスクを使用する場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。デフォルトでは、IPv4 のサブネット マスクの値は 32、IPv6 の値は 128 です。 最初の 6 個の IP アドレスがフィールドに表示されます。それ以外に設定されている IP アドレスを表示するには、スクロール バーを使用します。 IP アドレスの範囲を指定する場合は、ワイルドカード用のマスクだけが必要となります。アスタリスク（*）はワイルドカードとして使用できません。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
IP Range	IP アドレスの単一または複数の範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブネットを除外できます。 IP アドレスの範囲を指定するにはハイフン（-）を使用できます。最大 40 個の IP アドレスが単一の IP 範囲で許可されます。 ワイルドカードで IP アドレスを追加することもできます。ワイルド カードとしてアスタリスク（*）を使用できます。 IP アドレス範囲の入力例をいくつか次に示します。 • 単一範囲：10.77.10.1-10,,,, 192.120.10-12.10 • 複数範囲：10.*.1-20.10, 192.1-23.*.100-150 • 範囲から除外：10.10.1-255.* exclude 10.10.10-200.100-150 動的なデバイス IP アドレス範囲（たとえば、1-5.*.7.9）を使用すると、ランタイムと管理の両方のパフォーマンスに影響する可能性があります。 したがって、可能な限り IP アドレスとサブネット マスクを使用することを推奨します。動的 IP アドレス範囲は、範囲を IP アドレスおよびサブネット マスクを使用して記述できない場合にのみ使用する必要があります。 **（注）**　ワイルドカードを使用する AAA クライアントは、4.x から 5.x. に移行されます。 **（注）**　ACS 5.4 は、IPv6 範囲をサポートしていません。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。 IPv4 または IPv6 の IP アドレスを使用する場合には [TACACS+] をオンにします。
TACACS+ Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が使用されます。
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 IPv6 アドレスを使用する場合は、このオプションをオフにします。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
RADIUS Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。それぞれのキーは一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。キー ラップのデフォルトのキー モードは、16 進数ストリングです。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用されます。ASCII モードでは、キーの長さを正確に 16 文字で入力し、16 進数モードでは 32 文字で入力します。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。
Security Group Access	Cisco Security Group Access 機能をイネーブルにした場合にだけ表示されます。ネットワーク デバイスで Security Group Access 機能を使用する場合にオンにします。ネットワーク デバイスがシード デバイス（Security Group Access ネットワーク内の最初のデバイス）である場合、[RADIUS] チェックボックスもオンにする必要があります。
Use Device ID for Security Group Access Identification	Security Group Access の識別にデバイス ID を使用する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、次のフィールド（Device ID）がディセーブルになります。
Device ID	このデバイスの Security Group Access の識別に使用される名前。デフォルトでは、設定済みのデバイス名を使用できます。別の名前を使用する場合は、[Use device name for Security Group Access identification] チェックボックスをオフにして、[Identification] フィールドに名前を入力します。
Password	Security Group Access 認証パスワード。
Security Group Access Advanced Settings	追加の Security Group Access フィールドを表示する場合にオンにします。
Other Security Group Access devices to trust this device (SGA trusted)	デバイスのピア デバイスすべてによってこのデバイスが信頼されるかどうかを指定します。デフォルトはオンです。ピア デバイスでこのデバイスが信頼され、このデバイスから受信するパケットの SGT は変更されません。 このチェックボックスをオフにした場合、ピア デバイスによって、このデバイスからのパケットが関連するピア SGT で塗り替えられます。
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	ピア認可ポリシーの有効期限を指定します。ACS によって、この情報はピア ポリシー要求への応答でデバイスに返されます。デフォルトは 1 日です。
Download SGACL lists every: Weeks Days Hours Minutes Seconds	SGACL リストの有効期限を指定します。ACS によって、この情報は SGACL リストの要求への応答でデバイスに返されます。デフォルトは 1 日です。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
Download environment data every: Weeks Days Hours Minutes Seconds	環境データの有効期限を指定します。ACS によって、この情報は環境データの要求への応答でデバイスに返されます。デフォルトは 1 日です。
Re-authentication every: Weeks Days Hours Minutes Seconds	dot1x（.1x）再認証期間を指定します。ACS によって、これはサプリカントに対して設定され、この情報はオーセンティケータに返されます。デフォルトは 1 日です。

ネットワーク デバイス プロパティの表示

[Network Resources] > [Network Devices and AAA Clients] を選択してから、デバイス名をクリックします、または、デバイス名の隣にあるチェックボックスをオンにして [Edit] または [Duplicate] をクリックします。

[Network Devices and AAA Clients Properties] ページが表示され、表 7-5 で説明されている情報が示されます。

表 7-5　[Network Devices and AAA Clients Properties] ページ

オプション	説明
Name	ネットワーク デバイスの名前。ネットワーク デバイスを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Description	ネットワーク デバイスの説明。
Network Device Groups	
Location: Select	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付けるネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type: Select	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
IP Address	
ネットワーク デバイスに関連付けられる IP アドレスおよびサブネット マスク。単一の IP アドレスを入力するか、範囲を定義するかを選択します。	
Single IP Address	単一の IP アドレスを入力することを選択します。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
IP Range(s) By Mask	IP アドレス範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。このフィールドでサブネット マスクを使用する場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。 最初の 6 個の IP アドレスがフィールドに表示されます。それ以外に設定されている IP アドレスを表示するには、スクロール バーを使用します。 IP アドレスの範囲を指定する場合は、ワイルドカード用のマスクだけが必要となります。ワイルドカードとしてアスタリスク（*）は使用できません。
IP Range	IP アドレスの単一または複数の範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブネットを除外できます。 IP アドレスの範囲を指定するにはハイフン（-）を使用できます。ワイルドカードで IP アドレスを追加することもできます。ワイルド カードとしてアスタリスク（*）を使用できます。 IP アドレス範囲の入力例をいくつか次に示します。 • 単一範囲：10.77.10.1-10,,,, 192.120.10-12.10 • 複数範囲：10.*.1-20.10, 192.1-23.*.100-150 • 範囲から除外：10.10.1-255.* exclude 10.10.10-200.100-150 動的なデバイス IP アドレス範囲（たとえば、1-5.*.7.9）を使用すると、ランタイムと管理の両方のパフォーマンスに影響する可能性があります。 したがって、可能な限り IP アドレスとサブネット マスクを使用することを推奨します。動的 IP アドレス範囲は、範囲を IP アドレスおよびサブネット マスクを使用して記述できない場合にのみ使用する必要があります。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。
TACACS+ Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が使用されます。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。
RADIUS Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用します。入力するキーの長さは、ASCII モードで 16 文字、16 進数モードで 32 文字となります。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。
Security Group Access	Cisco Security Group Access 機能をイネーブルにした場合にだけ表示されます。ネットワーク デバイスで Security Group Access 機能を使用する場合にオンにします。ネットワーク デバイスがシード デバイス（Security Group Access ネットワーク内の最初のデバイス）である場合、[RADIUS] チェックボックスもオンにする必要があります。
ID	このデバイスの Security Group Access の識別に使用される名前。デフォルトでは、設定済みのデバイス名を使用できます。別の名前を使用する場合は、[Use device name for Security Group Access identification] チェックボックスをオフにして、[Identification] フィールドに名前を入力します。
Password	Security Group Access 認証パスワード。
Security Group Access Advanced Settings	追加の Security Group Access フィールドを表示する場合にオンにします。
Other Security Group Access devices to trust this device	デバイスのピア デバイスすべてによってこのデバイスが信頼されるかどうかを指定します。デフォルトはオンです。ピア デバイスでこのデバイスが信頼され、このデバイスから受信するパケットの SGT は変更されません。 このチェックボックスをオフにした場合、ピア デバイスによって、このデバイスからのパケットが関連するピア SGT で塗り替えられます。
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	ピア認可ポリシーの有効期限を指定します。ACS によって、この情報はピア ポリシー要求への応答でデバイスに返されます。デフォルトは 1 日です。
Download SGACL lists every: Weeks Days Hours Minutes Seconds	SGACL リストの有効期限を指定します。ACS によって、この情報は SGACL リストの要求への応答でデバイスに返されます。デフォルトは 1 日です。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
Download environment data every: Weeks Days Hours Minutes Seconds	環境データの有効期限を指定します。ACS によって、この情報は環境データの要求への応答でデバイスに返されます。デフォルトは 1 日です。
Re-authentication every: Weeks Days Hours Minutes Seconds	dot1x（.1x）再認証期間を指定します。ACS によって、これはサプリカントに対して設定され、この情報はオーセンティケータに返されます。デフォルトは 1 日です。

関連トピック：

- 「ネットワーク デバイスの一括操作の表示および実行」（P.7-6）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

ネットワーク デバイスの削除

ネットワーク デバイスを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Devices] ページが表示され、設定済みのネットワーク デバイスのリストが示されます。

ステップ 2　削除するネットワーク デバイスの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Network Devices] ページが表示されます。このとき、削除されたネットワーク デバイスは表示されません。ネットワーク デバイスがデバイス リポジトリから削除されます。

デフォルトのネットワーク デバイスの設定

要求の処理時に、ACS はネットワーク デバイス リポジトリを検索して、その要求で示されている IP アドレスと一致する IP アドレスを持つネットワーク デバイスを見つけます。この検索で一致するアドレスが見つからなかった場合、ACS では、RADIUS 要求または TACACS+ 要求に対して、デフォルトのネットワーク デバイス定義を使用します。

デフォルトのネットワーク デバイスによって、使用する共有秘密情報が定義され、また、デフォルトのネットワーク デバイス定義を使用する、RADIUS 要求または TACACS+ 要求のための NDG 定義も提供されます。

[Network Resources] > [Default Network Device] を選択して、デフォルトのネットワーク デバイスを設定します。[Default Network Device] ページが表示され、表 7-6 で説明されている情報が表示されます。

表 7-6　[Default Network Device] ページ

オプション	説明
Default Network Device	
デフォルトのデバイス定義は、デバイスの IP アドレスと一致する特定のデバイス定義が見つからなかった場合に任意で使用できます。	
Default Network Device Status	ドロップダウン リスト ボックスから [Enabled] を選択して、デフォルトのネットワーク デバイスをアクティブ状態にします。
Network Device Groups	
Location	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Location ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。
Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が ACS で使用されます。
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。
Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。

表 7-6　[Default Network Device] ページ （続き）

オプション	説明
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用します。入力するキーの長さは、ASCII モードで 16 文字、16 進数モードで 32 文字となります。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

外部プロキシ サーバの使用

ACS 5.4 は、RADIUS および TACACS+ サーバとしても RADIUS および TACACS+ プロキシ サーバとしても機能できます。プロキシ サーバとして機能する場合、ACS は NAS から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS または TACACS+ サーバに転送します。

ACS は要求の結果を受け入れて NAS に返します。ACS が要求を外部 RADIUS または TACACS+ サーバに転送するように、この外部 RADIUS または TACACS+ サーバを ACS で設定する必要があります。タイムアウト時間および接続試行回数を定義できます。

ACS は、複数の外部 RADIUS または TACACS+ サーバへのプロキシ サーバとして同時に機能できます。

RADIUS プロキシ サーバはループ シナリオを処理できるのに対し、TACACS+ プロキシ サーバはできません。

（注）　ここで設定した外部 RADIUS または TACACS+ サーバは、RADIUS または TACACS+ プロキシ サーバ タイプのアクセス サービスで使用できます。

ここでは、次の内容について説明します。

- 「外部プロキシ サーバの作成、複製、および編集」（P.7-21）
- 「外部プロキシ サーバの削除」（P.7-22）

外部プロキシ サーバの作成、複製、および編集

外部プロキシ サーバを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [External Proxy Servers] を選択します。

[External Proxy Servers] ページが表示され、設定されているサーバのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する外部プロキシ サーバの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する外部プロキシ サーバ名をクリックします。または、名前の隣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。

[External Proxy Servers] ページが表示されます。

ステップ 3　表 7-7 に従い、[External Proxy Servers] ページのフィールドを編集します。

表 7-7　[External Policy Servers] ページ

オプション	説明
General	
Name	外部 RADIUS または TACACS+ サーバの名前。
Description	（任意）外部 RADIUS または TACACS+ サーバの説明。
Server Connection	
Server IP Address	外部 RADIUS または TACACS+ サーバの IP アドレス。これは、IPv4 または IPv6 アドレスにできます。アドレスがサポートされる形式で入力されると、ACS 5.4 はその IP アドレスを検証します。入力された形式が正しくない場合は、エラー メッセージを表示します。
Shared Secret	外部 RADIUS または TACACS+ サーバの認証に使用される、ACS と外部 RADIUS または TACACS+ サーバ間の共有秘密情報。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。 [Show/Hide] ボタンはプレーン テキストまたは非表示の形式の共有秘密を表示するために利用できます。
Advanced Options	
RADIUS	RADIUS プロキシ サーバを作成することを選択します。RADIUS は IPv4 アドレスのみをサポートします。
TACACS+	TACACS+ プロキシ サーバを作成することを選択します。TACACS+ は、IPv4 アドレスおよび IPv6 アドレスをサポートします。
Cisco Secure ACS	デフォルトの選択。RADIUS と TACACS+ の両方をサポートします。IPv4 アドレスを使用する場合に、[Cisco Secure ACS] を選択できます。
Authentication Port	RADIUS 認証ポート番号。デフォルト値は 1812 です。
Accounting Port	RADIUS アカウンティング ポート番号。デフォルト値は 1813 です。
Server Timeout	ACS が外部 RADIUS サーバからの応答を待つ秒数。デフォルトは 5 秒です。有効な値の範囲は 1 ～ 999 です。

表 7-7　[External Policy Servers] ページ （続き）

オプション	説明
Connection Attempts	ACS が外部 RADIUS サーバへの接続を試みる回数。デフォルトは 3 回に設定されています。有効値は 1 ～ 99 です。
Connection Port	TACACS+ 接続ポート。デフォルトは 49 です。
Network Timeout	ACS が外部 TACACS+ サーバからの応答を待つ秒数。デフォルトは 20 秒です。

ステップ 4　[Submit] をクリックして変更を保存します。

外部プロキシ サーバの設定が保存されます。[External Proxy Server] ページが表示され、新しい設定が示されます。

（注） ACS で未知の RADIUS 属性を転送する場合は、プロキシの VSA を定義する必要があります。

関連トピック

- 「RADIUS および TACACS+ プロキシ サービス」（P.3-7）
- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）
- 「アクセス サービスの一般プロパティの設定」（P.10-13）
- 「外部プロキシ サーバの削除」（P.7-22）

外部プロキシ サーバの削除

外部プロキシ サーバを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [External Proxy Servers] を選択します。

[External Proxy Servers] ページが表示され、設定されているサーバのリストが示されます。

ステップ 2　削除する外部 RADIUS または TACACS+ サーバの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[External Proxy Servers] ページが表示されます。このとき、削除されたサーバは表示されません。

OCSP サービスの使用

ACS 5.4 では、新しいプロトコル、Online Certificate Status Protocol（OCSP）が導入されています。これは、x.509 デジタル証明書の状態を検査するために使用されます。このプロトコルは、証明書失効リスト（CRL）の代替として使用できます。また、CRL の処理時に生じる問題に対処することもできます。

ACS 5.4 は HTTP で OCSP サービスと通信して、認証における証明書の状態を検証します。OCSP は再利用可能なコンフィギュレーション オブジェクトで設定され、OCSP は、ACS で設定されている任意の認証局（CA）証明書から参照できます。複数の CA のオブジェクトが同じ OCSP サービスを参照できます。

ACS で最大 2 台の OCSP サーバを設定できます。これらはプライマリおよびセカンダリ OCSP サーバと呼ばれます。ACS はプライマリ OCSP サーバとの通信中にタイムアウトが発生した場合にセカンダリ OCSP サーバと通信します。

OCSP は、特定の証明書要求に次の 3 つの値を返す可能性があります。

- Good：証明書は使用に適しています。
- Revoked：証明書は取り消されています。
- Unknown：証明書ステータスは不明です。
  特定の証明書 CA を処理するように OCSP が設定されていない場合、証明書のステータスは不明です。この場合、証明書は不明な証明書として扱われます。つまり、検証プロセスは *Reject the request if no status* フラグを検査します。要求が拒否されないようにフラグがセットされている場合、OCSP は証明書が ACS に設定されているかどうかの検査を CRL まで続けます。

ACS は、すべての OCSP 応答をキャッシュします。これは、パフォーマンスを最大化し、OCSP サーバの負荷を軽減するためです。OCSP の検証時に、ACS はキャッシュの関連情報を最初に検索します。関連情報が見つからない場合、ACS は OCSP サーバへの接続を確立します。ACS は各 OCSP サービスのすべての OCSP レコードの有効期間を定義します。また、各 OCSP 応答に、新しい要求を行うまでの間隔を定義する存続可能時間があります。各キャッシュ エントリは、存続可能時間またはキャッシュ有効期間のいずれか短い方の間、保持されます。この OCSP サービスに関連付けられたすべてのキャッシュ レコードを取りクリアするには、[Clear Cache] をクリックします。[Clear Cache] は、分散型システムのセカンダリ ACS サーバのレコードもクリアします。

ACS は、キャッシュされた応答データベースのレプリケーションをサポートしません。キャッシュは永続的でないため、キャッシュされた応答は、ACS アプリケーションを再起動した後でクリアされます。

ここでは、次の内容について説明します。

- 「OCSP サーバの作成、複製、および編集」（P.7-23）
- 「OCSP サーバの削除」（P.7-25）

OCSP サーバの作成、複製、および編集

OCSP サーバを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [OCSP Services] を選択します。

[OCSP Services] ページが表示され、設定されている OCSP サーバのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する OCSP サーバの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する OCSP サーバ名をクリックします。または、名前の隣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。

[OCSP Servers] ページが表示されます。

ステップ 3　表 7-8 に従い、[OCSP Servers] ページのフィールドを編集します。

表 7-8　[OCSP Servers] ページ

オプション	説明
Name	OCSP サーバの名前。
Description	（任意）OCSP サーバの説明。
Server Connection	
Enable Secondary Server	[Always Access Primary Server First] および [Failback] オプションなどのセカンダリ サーバ設定を有効にするには、このチェックボックスをオンにします。
Always Access Primary Server First	プライマリ サーバから直前の応答がなかった場合でも、セカンダリ サーバに進む前にプライマリ サーバを最初に確認するには、このオプションを有効にします。
Failback To Primary Server	プライマリが完全にダウンしたときにセカンダリ サーバを指定した時間だけ使用するには、このオプションを有効にします。時間の範囲は 1 ～ 999 分です。
Primary Server	
URL	プライマリ サーバの URL または IP アドレスを入力します。
Enable Nonce Extension Support	OCSP 要求にナンスを使用する場合に、このチェックボックスをオンにします。 このオプションは、OCSP 要求にランダムな番号を含めます。このオプションを選択すると、要求に含まれる番号と応答で受信される番号を比較します。ナンスは、古い通信が再利用されないようにします。 ナンスは Windows 2008 サーバで設定できます。ACS サーバからのナンスが Windows サーバと一致しない場合、Windows は無許可応答を返します。そのため、ACS は要求に失敗し、これを不明な証明書であると見なします。
Validate Response Signature	OCSP 応答側に応答に次のシグニチャの 1 つを含めるように指示するには、このチェックボックスをオンにします。 • CA 証明書 • CA 証明書とは別の証明書 ACS は、OCSP 応答署名に基づいて、応答の証明書を検証します。OCSP 応答署名が見つからない場合、ACS は応答に失敗し、証明書のステータスを判断できません。
Network Timeout	ACS がプライマリ OCSP サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は、1 ～ 999 秒です。
Secondary Server	
URL	セカンダリ サーバの URL または IP アドレスを入力します。
Enable Nonce Extension Support	OCSP 要求にナンスを使用する場合に、このチェックボックスをオンにします。 このオプションは、OCSP 要求にランダムな番号を含めます。このオプションを選択すると、要求に含まれる番号と応答で受信される番号を比較します。ナンスは、古い通信が再利用されないようにします。 ナンスは Windows 2008 サーバで設定できます。ACS サーバからのナンスが Windows サーバと一致しない場合、Windows は無許可応答を返します。そのため、ACS は要求に失敗し、これを不明な証明書であると見なします。
Validate Response Signature	OCSP 応答側に応答に次のシグニチャの 1 つを含めるように指示するには、このチェックボックスをオンにします。 • CA 証明書 • CA 証明書とは別の証明書 ACS は、OCSP 応答署名に基づいて、応答の証明書を検証します。OCSP 応答署名が見つからない場合、ACS は応答に失敗し、証明書のステータスを判断できません。

表 7-8　[OCSP Servers] ページ （続き）

オプション	説明
Network Timeout	ACS がプライマリ OCSP サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値の範囲は 1 ～ 999 です。
Response Cache	
Cache Entry Time To Live	新しい OCSP 要求を行うまでの間隔を定義します。分単位の値を入力します。デフォルト値は 300 分です。
Clear Cache	すべての関連する認証局に選択された OCSP サービスのキャッシュをクリアします。 [Clear Cache] オプションでは、展開内のこの OCSP サービスに関連付けられているすべてのノードと対話できます。このオプションは、選択すると更新された状態も表示します。

ステップ 4　[Submit] をクリックして変更を保存します。

OCSP サーバの設定が保存されます。[OCSP Server] ページが表示され、新しい設定が示されます。

関連トピック

- 「OCSP サーバの削除」（P.7-25）

OCSP サーバの削除

OCSP サーバを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [OCSP Services] を選択します。

[OCSP Services] ページが表示され、設定されている OCSP サーバのリストが示されます。

ステップ 2　削除する OCSP サーバの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[OCSP Servers] ページが表示されます。このとき、削除されたサーバは表示されません。