



アクセスポリシーの管理

ACS 5.8 では、すべてのアクティビティはポリシーに従って実行されます。ポリシーは、主に、ポリシーの処理を決定する規則で構成されています。アクセス サービスを作成して、要求の認証および認可ポリシーを定義します。グローバル サービス セレクション ポリシーには、着信要求を処理するアクセス サービスを決定する規則が含まれています。

ポリシーとそれのすべての要素を設定するための基本的なワークフローについては、[サービスおよびポリシーの設定フロー \(3-19 ページ\)](#) をご参照ください。通常、ポリシー規則を設定する前に、ID、条件、認可、権限などの必要なすべての要素を設定する必要があります。

詳細については、次を参照してください。

- ID の管理については、[ユーザおよび ID ストアの管理 \(8-1 ページ\)](#) を参照してください。
- 条件の設定については、[ポリシー要素の管理 \(9-1 ページ\)](#) を参照してください。
- 認可と権限の設定については、[17 \(17-1 ページ\)](#) を参照してください。

ここでは、次の内容について説明します。

- [ポリシー作成フロー \(10-1 ページ\)](#)
- [ポリシーのカスタマイズ \(10-4 ページ\)](#)
- [サービス セレクション ポリシーの設定 \(10-5 ページ\)](#)
- [アクセス サービスの設定 \(10-11 ページ\)](#)
- [アクセス サービス ポリシーの設定 \(10-23 ページ\)](#)
- [複合条件の設定 \(10-41 ページ\)](#)
- [\[Security Group Access Control\] ページ \(10-47 ページ\)](#)
- [最大ユーザ セッション数 \(10-52 ページ\)](#)
- [ログイン試行失敗の最大回数のポリシー \(10-58 ページ\)](#)

Cisco Security Group Access 用の出力および NDAC ポリシーについては、[NDAC ポリシーの設定 \(4-26 ページ\)](#) を参照してください。

ポリシー作成フロー

ポリシー作成は、ネットワーク設定および個々のポリシーに対する改良の程度に依存します。ポリシー作成のエンドポイントは、サービス セレクション ポリシーの結果として実行されるアクセス サービスです。各ポリシーは規則に従って実行されます。

つまり、次を決定する必要があります。

- ネットワーク設定の詳細
- ポリシーを実装するアクセス サービス
- アクセス サービスを実行できる条件を定義する規則

ここでは、次の内容について説明します。

- [ネットワークの定義とポリシーの目的 \(10-2 ページ\)](#)
- [ポリシー作成フローのポリシー要素 \(10-3 ページ\)](#)
- [アクセス サービス ポリシーの作成 \(10-4 ページ\)](#)
- [サービス セレクション ポリシーの作成 \(10-4 ページ\)](#)

ネットワークの定義とポリシーの目的

ポリシー作成の最初の手順では、ポリシーを適用するデバイスとユーザを決定します。その後、ポリシー要素を設定できます。

基本的なポリシー作成では、Web インターフェイスの左側のナビゲーション ペインに表示されるドロワの順序に従って操作できます。一部のポリシー要素は他のポリシー要素に依存するため、ドロワの順序が役立ちます。ポリシー ドロワを順番に使用する場合、現在のドロワに必要な要素を、最初に前に戻って定義する必要がなくなります。

たとえば、ネットワーク設定の次の要素から簡単なデバイス管理ポリシーを作成できます。

- デバイス：ルータとスイッチ。
- ユーザ：ネットワーク エンジニア。
- デバイス グループ：デバイスを場所およびデバイス タイプでグループ化します。
- ID グループ：ネットワーク技術者を場所およびアクセス レベルでグループ化します。

ポリシーの結果は、各サイトの管理スタッフに適用されます。

- 自分のサイトのデバイスに対するフル アクセス
- 他のすべてのデバイスに対する読み取り専用アクセス
- スーパーバイザの場合はすべてに対するフル アクセス

ポリシー自体は、ネットワーク操作およびデバイス管理ポリシー内の特権を持つ管理者に適用されます。ユーザ（ネットワーク技術者）は、内部 ID ストアに格納されます。

ポリシー結果は、アクセス要求に応じて適用された認可と権限です。これらの認可と権限は、ポリシー要素としても設定されます。

ポリシー作成フロー：次の手順

- [ポリシー作成フローのポリシー要素 \(10-3 ページ\)](#)
- [アクセス サービス ポリシーの作成 \(10-4 ページ\)](#)
- [サービス セレクション ポリシーの作成 \(10-4 ページ\)](#)

ポリシー作成フローのポリシー要素

Web インターフェイスには、デバイス グループや ID グループの定義に使用できる次のデフォルトが用意されています。

- すべてのロケーション
- すべてのデバイス タイプ
- すべてのグループ

作成する場所、デバイス タイプ、および ID グループは、これらのデフォルトの子です。基本的なデバイス管理ポリシーの構築ブロックを作成するには、次の手順を実行します。

-
- ステップ 1** ネットワーク リソースを作成します。[Network Resources] ドロワで、次を作成します。
- [All Locations] > [East]、[West]、[HQ] など、場所のデバイス グループ
 - [All Device Types] > [Router]、[Switch] など、デバイス タイプのデバイス グループ
 - [EAST-ACCESS-SWITCH]、[HQ-CORE-SWITCH]、[WEST-WAN-ROUTER] など、AAA クライアント (AAA スイッチとルータのクライアント、それぞれのアドレス、およびそれぞれのプロトコル)
- ステップ 2** ユーザおよび ID ストアを作成します。[Users and Identity Stores] ドロワで、次を作成します。
- ID グループ (Network Operations および Supervisor)
 - 特定のユーザおよび ID グループとの関連付け ([Name]、[Identity Group]、[Password] など)
- ステップ 3** デバイス管理の認可と権限を作成します。[Policy Elements] ドロワで、次を作成します。
- フルアクセス、読み取り専用などの特定の特権 ([Shell Profiles] 内)
 - アクセスを許可または拒否するコマンドセット ([Command Sets] 内)
-

このポリシーでは、次の構築ブロックが作成されます。

- 次のようなネットワーク デバイス グループ (NDG)。
 - 場所 : East、HQ、West
 - デバイス タイプ : Router、Switch
- 次のような ID グループ。
 - ネットワーク運用サイト : East、HQ、West
 - アクセス レベル : フルアクセス
- デバイス : ネットワーク デバイス グループに割り当てられているルータとスイッチ。
- ユーザ : ID グループに割り当てられている内部 ID ストア内のネットワーク技術者。
- シェル プロファイル : 各管理者に適用できる、次のような特権。
 - 完全な特権
 - 読み取り専用の特権
- コマンドセット : 各管理者に対して認可を許可または拒否。

ポリシー作成フロー : 前の手順

- [ネットワークの定義とポリシーの目的 \(10-2 ページ\)](#)

ポリシー作成フロー：次の手順

- [アクセス サービス ポリシーの作成 \(10-4 ページ\)](#)
- [サービス セレクション ポリシーの作成 \(10-4 ページ\)](#)

アクセス サービス ポリシーの作成

基本要素を作成したあと、ID グループと特権を含むアクセス ポリシーを作成できます。たとえば、次のデータを使用する認可および認証ポリシーが含まれる、NetOps というデバイス管理用のアクセス サービスを作成できます。

- Supervisor ID グループのユーザ：すべての場所にあるすべてのデバイスに対する完全な特権を持ちます。
- East、HQ、および West ID グループのユーザ：対応する East、HQ、および West デバイスグループのデバイスに対する完全な特権を持ちます。
- 一致しない場合：アクセスを拒否します。

ポリシー作成フロー：前の手順

- [ネットワークの定義とポリシーの目的 \(10-2 ページ\)](#)
- [ポリシー作成フローのポリシー要素 \(10-3 ページ\)](#)

ポリシー作成フロー：次の手順

- [サービス セレクション ポリシーの作成 \(10-4 ページ\)](#)

サービス セレクション ポリシーの作成

ACS は、さまざまなアクセス使用例に対応しています。たとえば、デバイス管理、無線アクセス、ネットワーク アクセス コントロールなどがあります。これらの使用例それぞれについてアクセス ポリシーを作成できます。サービス セレクション ポリシーでは、着信要求に適用するアクセス ポリシーを決定します。

たとえば、TACAC+ プロトコルを使用するアクセス要求に NetOps アクセス サービスを適用するサービス セレクション規則を作成できます。

ポリシー作成フロー：前の手順

- [ネットワークの定義とポリシーの目的 \(10-2 ページ\)](#)
- [ポリシー作成フローのポリシー要素 \(10-3 ページ\)](#)
- [アクセス サービス ポリシーの作成 \(10-4 ページ\)](#)

ポリシーのカスタマイズ

ACS ポリシー規則には、条件と結果が含まれています。ポリシーの規則の定義を開始する前に、ポリシーに含める条件のタイプを設定する必要があります。この手順はポリシーのカスタマイズと呼ばれます。選択した条件タイプは、[Policy] ページに表示されます。[Policy] ページに表示される条件タイプだけを適用できます。ポリシー条件の詳細については、[ポリシー条件の管理 \(9-1 ページ\)](#) を参照してください。

デフォルトでは、[Policy] ページには複合式の条件カラムが1つ表示されます。複合条件の詳細については、[複合条件の設定 \(10-41 ページ\)](#) を参照してください。


Security Group Access 機能を実装している場合は、認可ポリシーの結果をカスタマイズすることもできます。



注意

すでに規則を定義している場合は、規則で条件のカスタマイズ時に削除する条件が使用されていないことを確認してください。条件カラムを削除すると、そのカラムに存在するすべての設定済み条件が削除されます。

ポリシーをカスタマイズするには、次の手順を実行します。

- ステップ 1** カスタマイズする [Policy] ページを開きます。手順は次のとおりです。
- サービスセレクションポリシーの場合は、[Access Policies] > [Service Selection Policy] を選択します。
 - アクセスサービスポリシーの場合は、[Access Policies] > [Access Services] > *service* > *policy* を選択します。*service* はアクセスサービスの名前、*policy* はカスタマイズするポリシーの名前です。
- ステップ 2** [Policy] ページで [Customize] をクリックします。
- 条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。
-  **(注)** ID 関連の属性は、サービスセレクションポリシー内の条件としては使用できません。
- ステップ 3** 条件を [Available] リストボックスと [Selected] リストボックスの間で移動します。
- ステップ 4** [OK] をクリックします。
- 選択した条件が [Conditions] カラムに表示されます。
- ステップ 5** [Save Changes] をクリックします。

ポリシーの設定：次の手順

- [サービスセレクションポリシーの設定 \(10-5 ページ\)](#)
- [アクセスサービスポリシーの設定 \(10-23 ページ\)](#)

サービスセレクションポリシーの設定

サービスセレクションポリシーでは、着信要求を処理するアクセスサービスを決定します。すべての要求に同じアクセスサービスを適用する単純なポリシー、またはルールベースのサービスセレクションポリシーを設定できます。

ルールベースのポリシーでは、各サービスセレクション規則に1つ以上の条件、および着信要求に適用されるアクセスサービスである結果が含まれます。サービスセレクションポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。

ここでは、次の内容について説明します。

- [単純なサービスセレクションポリシーの設定 \(10-6 ページ\)](#)
- [サービスセレクション規則の作成、複製、および編集 \(10-8 ページ\)](#)



(注) 単純なポリシーを作成および保存してからルールベースのポリシーに変更すると、単純なポリシーはルールベースのポリシーのデフォルト規則になります。ルールベースのポリシーを保存してから単純なポリシーに変更すると、デフォルト規則以外の規則はすべて失われます。デフォルト規則は、ACS によって自動的に単純なポリシーとして使用されます。

単純なサービスセレクションポリシーの設定

単純なサービスセレクションポリシーでは、すべての要求に同じアクセスサービスを適用します。

単純なサービスセレクションポリシーを設定するには、次の手順を実行します。

- ステップ 1 [Access Policies] > [Service Selection Policy] を選択します。
デフォルトでは、[Simple Service Selection Policy] ページが表示されます。
- ステップ 2 適用するアクセスサービスを選択するか、[Deny Access] を選択します。
- ステップ 3 [Save Changes] を選択して、ポリシーを保存します。

[Service Selection Policy] ページ

このページは、着信要求に適用するサービスを決定する単純なポリシーまたはルールベースのポリシーを設定する場合に使用します。


このページを表示するには、[Access Policies] > [Service Selection] を選択します。

すでにサービスセレクションポリシーが設定されている場合は、対応する単純なポリシーページ (表 10-1 を参照) またはルールベースのポリシーページ (表 10-2 を参照) が開きます。設定されていない場合は、デフォルトで単純なポリシーページが開きます。

表 10-1 [Simple Service Selection Policy] ページ

オプション	説明
Policy type	<p>ポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> • Select one result : 結果はすべての要求に適用されます。 <p>Rule-based result selection : 設定規則により、要求に応じて異なる結果が適用されます。</p>
Service Selection Policy	すべての要求に適用するアクセスサービス。デフォルトは [Deny Access] です。

表 10-2 [Rule-based Service Selection Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> • Select one result : 結果はすべての要求に適用されます。 • Rule-based result selection : 設定規則により、要求に応じて異なる結果が適用されます。
Status	<p>サービスセレクションを実行する規則の現在のステータス。規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor Only : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログエントリには、規則がモニタだけであることを示す情報が含まれます。モニタオプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	<p>サービスの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。</p> <p>ID ベースの条件は、サービスセレクション規則で使用できません。</p>
Results	規則の評価結果として実行されるサービス。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] をクリックします。
Default Rule	<p>次の場合に、ACS によってデフォルト規則が適用されます。</p> <ul style="list-style-type: none"> • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 <p>デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。</p>
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウントの表示 (10-10 ページ) を参照してください。

ルールベースのサービスセレクションポリシーを設定するには、次の項を参照してください。

- [サービスセレクション規則の作成、複製、および編集 \(10-8 ページ\)](#)
- [サービスセレクション規則の削除 \(10-10 ページ\)](#)

サービスセレクションポリシーの設定後、引き続きアクセスサービスポリシーを設定できます。[アクセスサービスポリシーの設定 \(10-23 ページ\)](#) を参照してください。

サービスセレクション規則の作成、複製、および編集

着信要求を処理するアクセス サービスを決定するサービスセレクション規則を作成します。一致する規則がないか、または規則が定義されていない場合は、デフォルト規則によってデフォルトのアクセス サービスが指定されます。

規則を作成するときは、規則の順序が重要であることに注意してください。ACS ネットワークにアクセスしようとするクライアントの要求が ACS によって処理されるときに一致が見つかり、その後の処理はすべて停止され、その一致に関連する結果が検索されます。一致が見つかったあとは、それ以降の規則は考慮されません。

サービスセレクション規則を複製して、既存の規則と同じか、または既存の規則によく似た新規の規則を作成できます。複製された規則名では、元の規則に複製を示すカッコが付けられません。たとえば、Rule-1(1) です。複製の完了後は、各規則（元の規則および複製された規則）に個別にアクセスします。デフォルト規則は複製できません。

サービスセレクション規則のすべての値を編集できます。また、デフォルト規則内の指定したアクセス サービスを編集できます。



(注)

すべての要求に同じアクセス サービスを適用する単純なポリシーを設定するには、[単純なサービスセレクションポリシーの設定 \(10-6 ページ\)](#) を参照してください。

はじめる前に

- サービスセレクションポリシーで使用する条件を設定します。[ポリシー条件の管理 \(9-1 ページ\)](#) を参照してください。



(注)

ID 関連の属性は、サービスセレクションポリシー内の条件としては使用できません。

- サービスセレクションポリシーで使用するアクセス サービスを作成します。[アクセスサービスの作成、複製、および編集 \(10-12 ページ\)](#) を参照してください。サービスセレクションポリシーを設定する前にアクセスサービスのポリシーを設定する必要はありません。
- ポリシー規則で使用する条件のタイプを設定します。詳細については、[ポリシーのカスタマイズ \(10-4 ページ\)](#) を参照してください。

サービスセレクションポリシーを作成、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 [Access Policies] > [Service Selection Policy] を選択します。次の場合があります。

- ルールベースのポリシーを前に作成したことがある場合は、設定されている規則のリストを含む [Rule-Based Service Selection Policy] ページが表示されます。
- ルールベースのポリシーを作成したことがない場合は、[Simple Service Selection Policy] ページが表示されます。[Rule-Based] 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。

- [Create] をクリックします。
- 複製する規則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。
- 変更する規則名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Rule] ページが表示されます。

ステップ 3 値を入力するか変更します。

- ユーザ定義の規則：任意の値を編集できます。少なくとも1つの条件が含まれていることを確認します。規則を複製する場合は、規則名を変更する必要があります。
 - デフォルト規則：アクセス サービスだけを変更できます。
- フィールドの説明については、表 10-3 を参照してください。

表 10-3 [Service Selection Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、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。
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor Only：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。 デフォルトでは、複合条件が表示されます。表示された条件を変更するには、[Policy] ページで [Customize] をクリックします。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。 (注) TACACS+ ユーザ名の複合条件を含むサービス セレクション ポリシーがコンスタントに機能しません。ポリシーは最初の TACACS+ 認証要求にユーザ名が含まれている場合のみ機能します。最初のパケットにユーザ名がない場合に ACS がユーザ名に NAS を要求すると、TACACS+ ユーザ名の状態が一致しません。このため、要求はデフォルトのアクセス拒否条件を満たし、適切なアクセス サービスを満たせません。
Results	
Service	規則の評価結果として実行されるアクセス サービスの名前。

ステップ 4 [OK] をクリックします。

設定した規則を含む [Service Selection Policy] ページが表示されます。

ステップ 5 [Save Changes] をクリックします。

関連項目

- [アクセス サービスの設定 \(10-11 ページ\)](#)
- [サービスセレクション規則の削除 \(10-10 ページ\)](#)

Hit カウントの表示

このページは、ルールベースのポリシーページの [Hit Count] 表示をリセットおよび更新する場合に使用します。

このページを表示するには、ルールベースのポリシーページの [Hit Count] をクリックします。

表 10-4 [Hit Count] ページ

オプション	説明
Hit Counts Reset	
Last time hit counts were reset for this policy	このポリシーで最後にヒットカウントがリセットされた日付と時刻を表示します。
Reset hit counts display for this policy	[Policy] ページのすべての規則について [Hit Count] 表示をゼロ (0) にリセットするには、[Reset] をクリックします。
Hit Counts Collection	
Hit counts are collected every:	ヒットカウント収集の間隔を表示します。
Last time hit counts were collected for this policy:	このポリシーで最後にヒットカウントが更新された日付と時刻を表示します。
Refresh hit counts display for this policy	[Policy] ページのヒットカウント表示をすべての規則の更新されたヒットカウントで更新するには、[Refresh] をクリックします。前回のヒットカウントは削除されます。 TACACS+ 認証要求が成功すると、対応する ID ポリシー規則と認可ポリシー規則の両方のヒットカウントは1ずつ増えます。

サービスセレクション規則の削除



(注) デフォルトのサービスセレクション規則は削除できません。

サービスセレクション規則を削除するには、次の手順を実行します。

- ステップ 1 [Access Policies] > [Service Selection Policy] を選択します。
設定されている規則のリストを含む [Service Selection Policy] ページが表示されます。
- ステップ 2 削除する規則の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。
[Service Selection Rules] ページが表示されます。このとき、削除した規則は表示されません。
- ステップ 4 [Save Changes] をクリックして、新しい設定を保存します。

アクセスサービスの設定

アクセスサービスには、要求の認証および認可ポリシーが含まれています。使用例ごとに異なるアクセスサービスを作成できます。たとえば、デバイス管理、無線ネットワークアクセスなどの使用例があります。

アクセスサービスを作成するときに、サービスに含まれるポリシーのタイプとポリシー構造を定義します。たとえば、デバイス管理やネットワークアクセス用のポリシーがあります。



(注) サービスセレクション規則を定義する前にアクセスサービスを作成する必要がありますが、サービスのポリシーを定義する必要はありません。

ここでは、次の内容について説明します。

- [アクセスサービスの作成、複製、および編集 \(10-12 ページ\)](#)
- [アクセスサービスの削除 \(10-22 ページ\)](#)

アクセスサービスの作成後、そのサービスをサービスセレクションポリシーで使用できます。[サービスセレクションポリシーの設定 \(10-5 ページ\)](#) を参照してください。

アクセスサービスのポリシーはカスタマイズおよび変更できます。[アクセスサービスポリシーの設定 \(10-23 ページ\)](#) を参照してください。

関連項目

- [アクセスサービスの作成、複製、および編集 \(10-12 ページ\)](#)

デフォルトのアクセスサービスの編集

ACS 5.8 には、2つのデフォルトのアクセスサービスが事前設定されています。1つはデバイス管理用、もう1つはネットワークアクセス用です。これらのアクセスサービスは編集可能です。

デフォルトのアクセスサービスを編集するには、次の手順を実行します。

ステップ 1 次のいずれかを選択します。

- [\[Access Policies\] > \[Access Services\] > \[Default Device Admin\]](#)
- [\[Access Policies\] > \[Access Services\] > \[Default Network Access\]](#)

[Default Service Access Service] 編集ページが表示されます。

ステップ 2 [Default Service Access Service] ページのフィールドを編集します。

[General] タブのフィールドについては、[表 10-5](#) を参照してください。

表 10-5 デフォルトのアクセスサービス : [General] ページ

オプション	説明
General	
Name	アクセスサービスの名前。
Description	アクセスサービスの説明。
Service Type	(表示のみ) サービスのタイプ。デバイス管理またはネットワークアクセス。
Policy Structure	

表 10-5 デフォルトのアクセス サービス : [General] ページ

オプション	説明
Identity	アクセス サービスに ID ポリシーを含めて、ACS で認証および属性の取得に使用する ID ストアを定義する場合にオンにします。
Group Mapping	アクセス サービスにグループ マッピング ポリシーを含めて、外部 ID ストアから取得したグループと属性を ACS の ID グループにマッピングする場合にオンにします。
Authorization	アクセス サービスに認可ポリシーを含めて、次を適用する場合にオンにします。 <ul style="list-style-type: none"> ネットワーク アクセス サービスの認可プロファイル。 デバイス管理サービスのシェル プロファイルおよびコマンドセット。

ステップ 3 表 10-7の説明に従って、[Allowed Protocols] タブのフィールドを編集します。

ステップ 4 [Submit] をクリックして、デフォルトのアクセス サービスに対する変更を保存します。

アクセスサービスの作成、複製、および編集

アクセス サービスには、要求の認証および認可ポリシーが含まれています。

アクセス サービスを作成するときに、次を定義します。

- ポリシー構造：サービスに含めるポリシーのタイプ。これらは、サービス テンプレート、既存のサービス、または使用例に従って定義できます。

サービスには次のポリシーを含めることができます。

- ID ポリシー：認証に使用する ID ストアを定義します。
- グループ マッピング ポリシー：マッピング先の ID グループを定義します。
- 認可ポリシー：ネットワーク アクセス の場合、このポリシーでは、適用するセッション認可プロファイルを定義します。デバイス管理の場合、適用するシェル プロファイルまたはコマンドセットを定義します。

- 許可されたプロトコル：このアクセス サービスに許可される認証プロトコルを指定し、ACS がそれらのプロトコルを認証に使用方法に関する詳細情報を指定します。

サービス テンプレートを使用して、特定の条件タイプを使用するようにカスタマイズされたポリシーを含むアクセス サービスを定義します。サービス テンプレートの詳細については、[アクセス サービス テンプレートの設定 \(10-22 ページ\)](#) を参照してください。

既存のアクセス サービスと同じか、または既存のアクセス サービスによく似た規則を含む新規のアクセス サービスを作成するには、アクセス サービスを複製します。複製の完了後は、各サービス（元のサービスおよび複製されたサービス）に個別にアクセスします。

複製元サービスの規則を複製しないでサービス ポリシー構造を複製するには、既存のサービスに基づいて新しいアクセス サービスを作成します。

アクセス サービスを作成、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 [Access Policies] > [Access Services] を選択します。

[Access Services] ページが表示され、設定されているサービス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。
- 複製するアクセスサービ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。
- 変更するアクセスサービス名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。
- 左側のナビゲーションタブでアクセスサービス名をクリックします。

[Access Service Properties] の [General] ページが表示されます。

- 新規のアクセスサービスを作成する場合は、次の手順を実行します。
 - アクセスサービスの名前とポリシー構造を定義します。
 - [Next] をクリックして、[Allowed Protocols] ページに進みます。
 - [Finish] をクリックして、新規のアクセスサービスを保存します。
- アクセスサービスを複製または編集する場合は、次の手順を実行します。
 - [Properties] ページのタブのフィールドを必要に応じて変更します。ポリシーを追加できますが、既存のポリシーは削除できません。
 - [Submit] をクリックして変更を保存します。

有効なフィールドオプションの詳細については、次を参照してください。

- [アクセスサービスの一般プロパティの設定 \(10-13 ページ\)](#)
- [アクセスサービスの許可されたプロトコルの設定 \(10-17 ページ\)](#)
- [アクセスサービステンプレートの設定 \(10-22 ページ\)](#)

アクセスサービスの設定が保存されます。新しい設定を含む [Access Services] ページが表示されます。

関連項目

- [アクセスサービスの削除 \(10-22 ページ\)](#)
- [アクセスサービスポリシーの設定 \(10-23 ページ\)](#)
- [サービスセレクションポリシーの設定 \(10-5 ページ\)](#)

アクセスサービスの一般プロパティの設定

アクセスサービス定義には、一般および許可されたプロトコル情報が含まれています。サービスを複製および編集する場合、[Access Service properties] ページにタブが表示されます。

ステップ 1 [Access Policies] > [Access Services] を選択し、[Create]、[Duplicate]、または [Edit] をクリックします。

ステップ 2 表 10-6 の説明に従って、フィールドに入力します。

表 10-6 Access Service Properties : [General] ページ

オプション	説明
General	
Name	アクセスサービスの名前。サービ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	アクセスサービスの説明。
Access Service Policy Structure	
Based on service template	定義済みのテンプレートに基づいたポリシーを含むアクセスサービスを作成します。このオプションは、サービスの作成だけに使用できます。
Based on existing service	既存のアクセスサービスに基づいたポリシーを含むアクセスサービスを作成します。新しいアクセスサービスには、既存のサービスのポリシー規則は含まれません。このオプションは、サービスの作成だけに使用できます。ポリシー規則を含めてサービスを複製するには、既存のアクセスサービスを複製します。
User selected service type	アクセスサービスタイプを選択するためのオプションがあります。使用できるオプションは、[Network Access]、[Device Administration]、および [External Proxy] です。設定できるポリシーのリストは、選択したアクセスサービスタイプによって異なります。
User Selected Service Type : [Network Access] および [Device Administration]	
Policy Structure	
Identity	アクセスサービスに ID ポリシーを含めて、ACS で認証および属性の取得に使用する ID ストアを定義する場合にオンにします。
Group Mapping	アクセスサービスにグループマッピングポリシーを含めて、外部 ID ストアから取得したグループと属性を ACS の ID グループにマッピングする場合にオンにします。
Authorization	アクセスサービスに認可ポリシーを含めて、次を適用する場合にオンにします。 <ul style="list-style-type: none"> ネットワークアクセスサービスの認可プロファイル。 デバイス管理サービスのシェルプロファイルおよびコマンドセット。
[User Selected Service Type] : [External Proxy]	
[External Proxy Servers] : プロキシに使用する外部サーバのセットを選択します。これらのサーバの使用順序を指定することもできます。	
Available External Proxy Servers	使用可能な外部 RADIUS および TACACS+ サーバのリスト。プロキシに使用する外部サーバを選択し、[Selected External Proxy Servers] リストに移動します。
Selected External Proxy Servers	選択した外部プロキシサーバのリスト。
Advanced Options	
Accounting	
Remote Accounting	リモートアカウントリングをイネーブルにする場合にオンにします。
Local Accounting	ローカルアカウントリングをイネーブルにする場合にオンにします。
Username Prefix\Suffix Stripping	
Strip start of subject name up to the first occurrence of the separator	プレフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が acme\smith、区切り文字が \ の場合、ユーザ名は smith になります。デフォルトの区切り文字は \ です。
Strip end of subject name from the last occurrence of the separator	サフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が smith@acme.com、区切り文字が @ の場合、ユーザ名は smith になります。デフォルトの区切り文字は @ です。

表 10-6 Access Service Properties : [General] ページ (続き)

オプション	説明
RADIUS INBOUND 属性の注入 : RADIUS INBOUND 属性のセクションは、プロキシサーバに送信する前に、入力属性を処理するために使用します。	
Add	RADIUS 入力属性を定義した後で、RADIUS 属性リストに追加するには、[ADD] をクリックします。
Edit	リストされている RADIUS 入力属性を編集するには、リストから属性を選択し、[Edit] をクリックします。属性のプロパティがフィールドに表示されます。プロパティを必要に応じて変更し、[Replace] をクリックします。
Replace	選択した RADIUS 入力属性を、このフィールドに現在定義されている値で置き換えるには、[Replace] をクリックします。
Delete	リストから選択した RADIUS 入力属性を削除するには、[Delete] をクリックします。
Dictionary Type	使用する RADIUS 入力属性が含まれているディクショナリを選択します。
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、指定したディクショナリから RADIUS 属性を選択します。
Attribute Type	選択した RADIUS 属性のタイプ。ACS がアクセス要求を許可する対象となる、属性のクライアントベンダータイプ。これらの属性タイプについては、使用する AAA クライアントで稼働している Cisco IOS ソフトウェアリリースの Cisco IOS マニュアルを参照してください。
Operation	<p>次の3つの操作を実行できます。</p> <ul style="list-style-type: none"> • 選択した RADIUS 属性の新しい属性値を追加するには、[ADD] を選択します。 <ul style="list-style-type: none"> - [Multiple not allowed] の場合：この属性が要求に存在しない場合に限り、選択した属性の新しい値を追加します。 - [Multiple allowed] の場合：新しい値を持つ属性を必ず追加します。 • 選択した RADIUS 属性の既存の値を更新するには、[UPDATE] を選択します。 <ul style="list-style-type: none"> - [Multiple not allowed] の場合：属性が要求に存在する場合に、新しい値で属性値を更新します。 - [Multiple allowed] の場合：この属性の出現をすべて削除し、新しい値を持つ属性を1つ追加します。 - 属性が cisco-avpair (キー = 値のペア) の場合、更新はキーに基づいて行われます。 • 選択した RADIUS 属性の値を削除するには、[DELETE] を選択します。 <p>属性操作ステートメントは順序付けられます。管理者は、設定時にステートメントの順序を変更できます。ACS は、設定された順序に従って属性に動作を実行します。詳細については、RADIUS 属性の書き換え動作 (4-31 ページ) を参照してください。</p>
Attribute New Value	選択した RADIUS 入力属性の新しい値を入力します。このオプションは削除操作を選択した場合は使用できません。
RADIUS OUTBOUND 属性の注入 : RADIUS OUTBOUND 属性のセクションは、プロキシサーバから送信する前に出力属性を処理するために使用します。	
Add	RADIUS 出力属性を定義した後で、RADIUS 属性リストに追加するには、[ADD] をクリックします。
Edit	リストされている RADIUS 出力属性を編集するには、リストから属性を選択し、[Edit] をクリックします。属性のプロパティがフィールドに表示されます。プロパティを必要に応じて変更し、[Replace] をクリックします。

表 10-6 Access Service Properties : [General] ページ (続き)

オプション	説明
Replace	選択した RADIUS 出力属性を、このフィールドに現在定義されている値で置き換えるには、[Replace] をクリックします。
Delete	リストから選択した RADIUS 出力属性を削除するには、[Delete] をクリックします。
Dictionary Type	使用する RADIUS 出力属性が含まれているディクショナリを選択します。
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、指定したディクショナリから RADIUS 属性を選択します。
Attribute Type	選択した RADIUS 属性のタイプ。ACS がアクセス要求を許可する対象となる、属性のクライアントベンダータイプ。これらの属性タイプについては、使用する AAA クライアントで稼働している Cisco IOS ソフトウェアリリースの Cisco IOS マニュアルを参照してください。
Operation	<p>次の 3 つの操作を実行できます。</p> <ul style="list-style-type: none"> • 選択した RADIUS 属性の新しい属性値を追加するには、[ADD] を選択します。 <ul style="list-style-type: none"> - [Multiple not allowed] の場合：この属性が要求に存在しない場合に限り、選択した属性の新しい値を追加します。 - [Multiple allowed] の場合：新しい値を持つ属性を必ず追加します。 • 選択した RADIUS 属性の既存の値を更新するには、[UPDATE] を選択します。 <ul style="list-style-type: none"> - [Multiple not allowed] の場合：属性が要求に存在する場合に、新しい値で属性値を更新します。 - [Multiple allowed] の場合：この属性の出現をすべて削除し、新しい値を持つ属性を 1 つ追加します。 - 属性が cisco-avpair (キー = 値のペア) の場合、更新はキーに基づいて行われます。 • 選択した RADIUS 属性の値を削除するには、[DELETE] を選択します。 <p>属性操作ステートメントは順序付けられます。管理者は、設定時にステートメントの順序を変更できます。ACS は、設定された順序に従って属性に動作を実行します。詳細については、RADIUS 属性の書き換え動作 (4-31 ページ) を参照してください。</p>
Attribute New Value	選択した RADIUS 出力属性の新しい値を入力します。このオプションは削除操作を選択した場合は使用できません。

ステップ 3 [Next] をクリックして、許可されたプロトコルを設定します。[アクセスサービスの許可されたプロトコルの設定 \(10-17 ページ\)](#) を参照してください。

関連項目

- [アクセスサービスの許可されたプロトコルの設定 \(10-17 ページ\)](#)
- [アクセスサービス テンプレートの設定 \(10-22 ページ\)](#)

アクセスサービスの許可されたプロトコルの設定

アクセス サービス作成の第2部は、許可されたプロトコルです。アクセス サービス定義には、一般および許可されたプロトコル情報が含まれています。サービスを複製および編集する場合、[Access Service properties] ページにタブが表示されます。

ステップ 1 [Access Policies] > [Access Services] を選択し、次の操作を実行します。

- [Create] をクリックして新規のアクセス サービスを作成してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。
- [Duplicate] をクリックしてアクセス サービスを複製してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。
- [Edit] をクリックしてアクセス サービスを編集してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。

ステップ 2 表 10-7に示すように、フィールドに入力します。

表 10-7 Access Service Properties : [Allowed Protocols] ページ

オプション	説明
Process Host Lookup	たとえば RADIUS Service-Type が 10 の場合に [Host Lookup] フィールドを処理し、RADIUS Calling-Station-ID 属性の System UserName 属性を使用するように ACS を設定する場合にオンにします。 ACS でホスト ルックアップ要求を無視し、認証と認可に system UserName 属性の元の値を使用する場合はオフにします。オフにすると、メッセージ処理はプロトコル (たとえば PAP) に従って行われます。
Authentication Protocols	
Allow PAP/ASCII	PAP/ASCII をイネーブルにします。PAP は、平文パスワード (つまり暗号化されていないパスワード) を使用する最もセキュリティ レベルの低い認証プロトコルです。 [Allow PAP/ASCII] をオンにすると、[Detect PAP as Host Lookup] をオンにして、ネットワーク アクセス サービスでこのタイプの要求を PAP ではなくホスト ルックアップ要求として検出するように ACS を設定できます。
Allow CHAP	CHAP 認証をイネーブルにします。CHAP は、パスワードの暗号化とともにチャレンジレスポンス方式を使用します。CHAP は、Windows Active Directory では使用できません。
Allow MS-CHAPv1	MS-CHAPv1 をイネーブルにします。
Allow MSCHAPv2	MSCHAPv2 をイネーブルにします。
Allow EAP-MD5	EAP ベースの Message Digest 5 ハッシュ認証をイネーブルにします。 [Allow EAP-MD5] をオンにすると、[Detect EAP-MD5 as Host Lookup] をオンにして、ネットワーク アクセス サービスでこのタイプの要求を EAP-MD5 ではなくホスト ルックアップ要求として検出するように ACS を設定できます。

表 10-7 Access Service Properties : [Allowed Protocols] ページ (続き)

オプション	説明
Allow EAP-TLS	<p>EAP-TLS 認証プロトコルをイネーブルにし、EAP-TLS 設定を行います。エンドユーザクライアントからの EAP Identity 応答で提示されたユーザ ID を ACS が確認する方法を指定できます。ユーザ ID は、エンドユーザクライアントによって提示された証明書の情報に照らして確認されます。この比較は、ACS とエンドユーザクライアントとの間に EAP-TLS トンネルが確立されたあとに行われます。[Allow EAP-TLS] を選択した場合は、次を設定できます。</p> <ul style="list-style-type: none"> • [Enable Stateless Session resume] : アクセスサービスごとにステートレスセッション再開機能をイネーブルにするには、このチェックボックスをオンにします。この機能では、次のオプションを設定することが可能です。 <ul style="list-style-type: none"> - [Proactive Session Ticket update] : セッションチケットが更新される前に経過する必要がある持続可能時間の量を示すパーセント値を入力します。たとえば、値 10 を入力した場合、セッションチケットの更新は持続可能時間の 10 パーセントが過ぎた後に実行されます。 - [Session ticket Time to Live] : 正の整数を使用して日、週、月、および年に対応する最大値を入力します。 <p>EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS 認証が行われるのは、証明書の設定に必要な手順を完了した場合にかぎられます。詳細については、ローカルサーバ証明書の設定 (18-17 ページ) を参照してください。</p>
Allow LEAP	LEAP 認証をイネーブルにします。
Allow PEAP	<p>PEAP 認証プロトコルと PEAP 設定をイネーブルにします。デフォルトの内部方式は、MSCHAPv2 です。</p> <p>[Allow PEAP] をオンにすると、次の PEAP 内部方式を設定できます。</p> <ul style="list-style-type: none"> • [Allow EAP-TLS] : 内部方式として EAP-TLS を使用する場合にオンにします。 • Allow EAP-MSCHAPv2 : 内部方式として EAP-MSCHAPv2 を使用する場合にオンにします。 <ul style="list-style-type: none"> - Allow Password Change : ACS でパスワード変更をサポートする場合にオンにします。 - Retry Attempts : ACS でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効な値は 1 ~ 3 です。 • Allow EAP-GTC : 内部方式として EAP-GTC を使用する場合にオンにします。 <ul style="list-style-type: none"> - Allow Password Change : ACS でパスワード変更をサポートする場合にオンにします。 - Retry Attempts : ACS でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効な値は 1 ~ 3 です。 • [Allow PEAP Cryptobinding TLV] : PEAP 暗号化バインド TLV のサポートを使用する場合にオンにします。 • [Allow PEAPv0 only for legacy clients] : PEAP サプリカントが PEAPv0 にかぎりネゴシエーションできるようにするには、このオプションをオンにします。 <p>(注) 少数のレガシークライアントは PEAPv1 プロトコル規格を確認しません。その結果、EAP カンバセーションは [Invalid EAP payload] エラーメッセージでドロップされます。</p>

表 10-7 Access Service Properties : [Allowed Protocols] ページ (続き)

オプション	説明
Allow EAP-FAST	<p>EAP-FAST 認証プロトコルと EAP-FAST 設定をイネーブルにします。EAP-FAST プロトコルは、同じサーバ上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MSCHAPv2 です。</p> <p>[Allow EAP-FAST] をオンにすると、EAP-FAST 内部方式を設定できます。</p> <ul style="list-style-type: none"> • Allow EAP-MSCHAPv2 <ul style="list-style-type: none"> - Allow Password Change : ACS で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合にオンにします。 - Retry Attempts : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ~ 3 です。 • Allow EAP-GTC <ul style="list-style-type: none"> - Allow Password Change : ACS で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合にオンにします。 - Retry Attempts : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ~ 3 です。 • [Allow TLS-Renegotiation] : ACS で TLS 再ネゴシエーションをサポートする場合にオンにします。このオプションでは、エンドユーザクライアントと ACS の間で匿名の TLS ハンドシェイクが可能になります。EAP-MS-CHAP は、フェーズ 0 の内部方式としてのみ使用されます。 • Use PACs : EAP-FAST クライアントに認可 PAC をプロビジョニングするように ACS を設定する場合に選択します。追加の PAC オプション (10-20 ページ) が表示されます。 • Don't use PACs : トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように ACS を設定する場合に選択します。PAC のすべての要求は無視され、ACS は PAC を含まない Success-TLV で応答します。 <ul style="list-style-type: none"> - Allow Machine Authentication : マシン認証を実行するよう ACS を設定する場合、このオプションをオンにします。 - Accept Client Certificate : Cisco IP Phone を使用する時、クライアント証明書を受け入れるよう ACS を設定する場合、このオプションをオンにします。

表 10-7 Access Service Properties : [Allowed Protocols] ページ (続き)

オプション	説明
Allow EAP-FAST (続き)	<p>PAC オプション</p> <ul style="list-style-type: none"> • Tunnel PAC Time To Live : 存続可能時間 (TTL) の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 1 日です。 • Proactive PAC Update When: < [n%] > of PAC TTL is Left : Update 値により、クライアントに有効な PAC が保持されます。ACS は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。Update 値は、TTL の残り時間のパーセンテージです (デフォルト : 10%)。 • Allow Anonymous In-band PAC Provisioning : ACS でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントにいわゆる PAC をプロビジョニングする場合にオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。 <p>(注) 匿名 PAC プロビジョニングをイネーブルにするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。</p> <ul style="list-style-type: none"> • Allow Authenticated In-band PAC Provisioning : ACS は Secure Socket Layer (SSL) サーバ側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバ証明書および信頼できるルート CA が ACS にインストールされている必要があります。 <ul style="list-style-type: none"> - Server Returns Access Accept After Authenticated Provisioning : 認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すよう ACS を設定する場合、このオプションをオンにします。 - Accept Client Certificate For Provisioning : Cisco IP Phone を使用する時、PAC をプロビジョニングするためのクライアント証明書を受け入れるよう ACS を設定する場合、このオプションをオンにします。 • Allow Machine Authentication : ACS でエンドユーザクライアントにマシン PAC をプロビジョニングし、(マシンクレデンシャルを持たないエンドユーザクライアントに対して) マシン認証を実行する場合にオンにします。 マシン PAC は、要求 (インバンド) によって、または管理者 (アウトオブバンド) によって、クライアントにプロビジョニングできます。ACS がエンドユーザクライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、ACS 外部 ID ストアで確認されます。その詳細が正しいことが確認されると、その後の認証は実行されません。 <p>(注) ACS 5.8 では、マシン認証の外部 ID ストアとして Active Directory だけがサポートされます。</p> <p>このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。ACS は、期限切れのマシン PAC を受け取ると、(エンドユーザクライアントからの新規マシン PAC 要求を待たずに) エンドユーザクライアントに新規マシン PAC を自動的に再プロビジョニングします。</p> <ul style="list-style-type: none"> • Enable Stateless Session Resume : ACS で EAP-FAST クライアントに認可 PAC をプロビジョニングし、常に EAP-FAST のフェーズ 2 を実行する場合にオンにします (デフォルトはオン)。 次の場合は、このオプションをオフにします。 <ul style="list-style-type: none"> - ACS が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 - EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザ認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。ACS は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。

表 10-7 Access Service Properties : [Allowed Protocols] ページ (続き)

オプション	説明
Preferred EAP protocol	<p>使用可能な次のオプションから、優先させる EAP プロトコルを選択します。</p> <ul style="list-style-type: none"> • EAP-FAST • PEAP • LEAP • EAP-TLS • EAP-MD5 <p>このオプションでは、特定のプロトコルが実装されていない場合に、No-Acknowledgment を送信する機能を持たない古いサブリカント(エンド デバイス)と連携するよう、ACS に柔軟性を持たせることができます。このオプションを使用して、デバイスとネゴシエーションしているプロトコルのリストの先頭に特定のプロトコルを配置し、ネゴシエーションを成功させることができます。</p>
EAP-TLS L-bit	<p>アクセス ポリシーで、L (長さを含む) フラグを有効にします。ACS 5.x においてターミナル ワイヤレス LAN ユニット (TWLU) クライアントに対する EAP-TLS 認証を実行する際、TWLU は暗号変更仕様と暗号化ハンドシェイク メッセージに L フラグ (長さを含むフラグ) が設定されていることを想定しています。Honeywell TWLU ユニットが使用されている場合、すべての TWLU ユニットのグループと L フラグが含まれているアクセス ポリシーを作成し、すべての TWLU ユニットでそのアクセス ポリシーを使用して、他のクライアントを妨げないようにすることを推奨します。EAP-TLS L ビットは、ACS Web インターフェイスの [Access Policies] > [Access Services] > [Default Network Access] > [Edit: "Default Network Access"] ページ内にあります。</p>
Allow weak ciphers for EAP	<p>(注) このオプションは、ACS 5.8 パッチ 4 以降で利用可能です。</p> <p>EAP プロトコルで弱い暗号方式を有効にします。このオプションを有効にすると、レガシークライアントが弱い暗号方式を使用してネゴシエートすることを許可します。このオプションを有効にするのは、レガシークライアントが弱い暗号方式しかサポートしていない場合に限ることを推奨します。このオプションは、デフォルトで無効です。</p> <p>(注) FIPS を有効にすると、ACS はこのオプションを有効にできないようにします。また、その逆も同様です。</p>
RADIUS Access-Accept の User-Name として送信	
RADIUS Access-Request User-Name	RADIUS アクセス許可応答の RADIUS アクセス要求で受け取ったユーザ名を ACS に送信させる場合にこのオプションを選択します。
Principal User Name	RADIUS アクセス許可応答でユーザの認証に使用される証明書のプリンシパル名を ACS に送信させる場合にこのオプションを選択します。

ステップ 3 [Finish] をクリックして、アクセス サービスの変更を保存します。

アクセス サービスをイネーブルにするには、サービス セレクション ポリシーに追加する必要があります。

アクセスサービステンプレートの設定

サービステンプレートを使用して、特定の条件タイプを使用するようにカスタマイズされたポリシーを含むアクセスサービスを定義します。

ステップ 1 [アクセスサービスの一般プロパティの設定 \(10-13 ページ\)](#) で、[Based on service template] を選択し、[Select] をクリックします。

ステップ 2 [表 10-8](#)の説明に従って、フィールドに入力します。

表 10-8 アクセスサービステンプレート

テンプレート名	アクセスサービスタイプ	プロトコル	ポリシー	条件	結果
Device Admin - Simple	デバイス管理	PAP/ASCII	Identity	なし - 単純	内部ユーザ
			許可	Identity group、NDG:Location、NDG:Device Type、Time and Date	シェルプロファイル
Device Admin - Command Auth	デバイス管理	PAP/ASCII	Identity	なし - 単純	内部ユーザ
			許可	Identity group、NDG:Location、NDG: Time and Date	コマンドセット
Network Access - Simple	ネットワークアクセス	PEAP、EAP-FAST	Identity	なし - 単純	内部ユーザ
			許可	NDG:Location、Time and date	認可プロファイル
Network Access - MAC Authentication Bypass	ネットワークアクセス	Process Host Lookup、PAP/ASCII (Detect PAP as Host Lookup)、EAP-MD5 (Detect EAP-MD5 as Host Lookup)	Identity	なし - 単純	内部ユーザ
			許可	Use case	認可プロファイル

アクセスサービスの削除

アクセスサービスを削除するには、次の手順を実行します。

ステップ 1 [Access Policies] > [Access Services] を選択します。

[Access Services] ページが表示され、設定されているサービスのリストが表示されます。

ステップ 2 削除するアクセスサービスの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、確認メッセージの[OK] をクリックします。

[Access Policies] ページが表示されます。このとき、削除したアクセスサービスは表示されません。

関連項目

- [アクセス サービスの作成、複製、および編集 \(10-12 ページ\)](#)

アクセス サービス ポリシーの設定

アクセス サービスの作成後、アクセス サービス ポリシーを設定します。

- [ID ポリシーの表示 \(10-23 ページ\)](#)
- [ID ポリシー規則のプロパティ設定 \(10-26 ページ\)](#)
- [グループマッピングポリシーの設定 \(10-28 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [デバイス管理のシェル/コマンド認可ポリシーの設定 \(10-36 ページ\)](#)

すべての着信要求に同じアクセス サービスを適用する単純なポリシーを設定するか、またはルールベースのポリシーを作成できます。



(注)

単純なポリシーを作成および保存してからルールベースのポリシーに変更すると、単純なポリシーはルールベースのポリシーのデフォルト規則になります。ルールベースのポリシーを保存してから単純なポリシーに変更すると、デフォルト規則以外の規則はすべて失われます。デフォルト規則は、ACS によって自動的に単純なポリシーとして使用されます。

ポリシー規則の設定を開始する前に、次の操作を行う必要があります。

- ポリシー条件および結果を設定します。[ポリシー条件の管理 \(9-1 ページ\)](#) を参照してください。
- ポリシー規則によって適用される条件および結果のタイプを選択します。[ポリシーのカスタマイズ \(10-4 ページ\)](#) を参照してください。

ポリシー規則の設定の詳細については、次を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

ID ポリシーの表示

アクセス サービスの ID ポリシーでは、ACS で認証と属性の取得に使用する ID ソースを定義します。ACS は、取得した属性をその後のポリシーで使用できます。

次の ID ソースがあります。

- パスワードベースの認証の ID ソースは、単一の ID ストアまたは ID ストア順序にすることができます。
- 証明書ベースの認証の ID ソースは、証明書認証プロファイルまたは ID ストア順序にすることができます。

ID ストア順序は、認証に使用される順序および属性を取得する任意の追加順序を定義します。[ID ストア順序の設定 \(8-104 ページ\)](#) を参照してください。

ID ポリシーを含むアクセス サービスを作成した場合は、このポリシーを設定および変更できます。すべての要求の認証に同じ ID ソースを適用する単純なポリシー、またはルールベースの ID ポリシーを設定できます。

ルールベースのポリシーでは、各規則に 1 つ以上の条件、および認証に使用される ID ソースである結果が含まれます。ID ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。



注意

単純なポリシー ページとルールベースのポリシー ページを切り替えると、以前に保存したポリシーは失われます。

単純な ID ポリシーを設定するには、次の手順を実行します。

- ステップ 1** [Access Policies] > [Access Services] > *service* > [Identity] を選択します。*service* は、アクセスサービスの名前です。
- デフォルトでは、[表 10-9](#)で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。

表 10-9 [Simple Identity Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> Simple : 結果がすべての要求に適用されることを指定します。 Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。 <p>ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Identity Source	<p>すべての要求に適用する ID ソース。デフォルトは [Deny Access] です。手順は次のとおりです。</p> <ul style="list-style-type: none"> パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。 証明書ベースの認証の場合、証明書認証プロファイルまたは ID ストア順序を選択します。 <p>ID ストア順序は、認証に使用される順序および属性を取得する任意の追加順序を定義します。ID ストア順序の設定 (8-104 ページ) を参照してください。</p>
Advanced options	<p>次のオプションについて、要求を拒否またはドロップするか、認証を続行するかを指定します。</p> <ul style="list-style-type: none"> If authentication failed : デフォルトは拒否です。 If user not found : デフォルトは拒否です。 If process failed : デフォルトはドロップです。 <p>基になるプロトコルの制限により、ACS では、[Continue] オプションが選択された場合でも処理を続行できない場合があります。PAP/ASCII、EAP-TLS、または Host Lookup の場合、認証に失敗しても ACS は処理を続行できます。</p> <p>その他のすべての認証プロトコルの場合、[Continue] オプションを選択しても要求はドロップされます。</p>

ステップ 2 認証用の ID ソースを選択するか、または [Deny Access] を選択します。

その他の高度なオプションを設定できます。ID ポリシー規則のプロパティ設定 (10-26 ページ) を参照してください。

ステップ 3 [Save Changes] を選択して、ポリシーを保存します。

ルールベースの ID ポリシーの表示

[Access Policies] > [Access Services] > *service* > [Identity] を選択します。<service> は、アクセス サービスの名前です。

デフォルトでは、表 10-9 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。設定されている場合は、表 10-10 で説明されているフィールドを含む [Rules-Based Identity Policy] ページが表示されます。

表 10-10 [Rule-based Identity Policy] ページ



オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> Simple : 結果がすべての要求に適用されることを指定します。 Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。 <p> 注意 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Status	<p>規則の現在のステータス。規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> Enabled : 規則はアクティブです。 Disabled : ACS によって規則の結果は適用されません。 Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として認証に使用される ID ソース。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	<p>次の場合に、ACS によってデフォルト規則が適用されます。</p> <ul style="list-style-type: none"> イネーブルな規則が一致しない。 他の規則が定義されていない。 <p>デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。</p>

表 10-10 [Rule-based Identity Policy] ページ (続き)

オプション	説明
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウントの表示 (10-10 ページ) を参照してください。

ルールベースのポリシーを設定するには、次の項を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

ホストルックアップ要求用の ID ポリシー設定の詳細については、[ホストルックアップ要求用の認可ポリシーの設定 \(4-20 ページ\)](#) を参照してください。

関連項目

- [グループマッピングポリシーの設定 \(10-28 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [デバイス管理のシェル/コマンド認可ポリシーの設定 \(10-36 ページ\)](#)

ID ポリシー規則のプロパティ設定

ID ポリシー規則を作成、複製、または編集して、クライアントの認証に使用する ID データベースを決定したり、クライアントの属性を取得したりできます。

このページを表示するには、次の手順を実行します。

-
- ステップ 1** [Access Policies] > [Access Services] > *service* > [Identity] を選択し、次のいずれかを実行します。
- [Create] をクリックします。
 - 規則チェックボックスをオンにし、[Duplicate] をクリックします。
 - 規則名をクリックするか規則チェックボックスをオンにし、[Edit] をクリックします。
- ステップ 2** [表 10-11](#)の説明に従って、[Identity Rule Properties] ページのフィールドに入力します。

表 10-11 [Identity Rule Properties] ページ

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、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。
Rule Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。
Results	
Identity Source	要求に適用する ID ソース。デフォルトは [Deny Access] です。手順は次のとおりです。 <ul style="list-style-type: none"> • パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。 • 証明書ベースの認証の場合、証明書認証プロファイルまたは ID ストア順序を選択します。 ID ストア順序は、認証に使用される順序および追加属性を取得する任意の順序を定義します。 ID ストア順序の設定 (8-104 ページ) を参照してください。
Advanced options	次のオプションについて、要求を拒否またはドロップするか、認証を続行するかを指定します。 <ul style="list-style-type: none"> • If authentication failed : デフォルトは拒否です。 • If user not found : デフォルトは拒否です。 • If process failed : デフォルトはドロップです。 基になるプロトコルの制限により、ACS では、[Continue] オプションが選択された場合でも処理を続行できない場合があります。PAP/ASCII、EAP-TLS、または Host Lookup の場合、認証に失敗しても ACS は処理を続行できます。 その他のすべての認証プロトコルの場合、[Continue] オプションを選択しても、要求はドロップされます。

グループマッピングポリシーの設定

外部 ID ストアから取得したグループと属性を ACS ID グループにマッピングするグループマッピングポリシーを設定します。ACS によってユーザまたはホストの要求が処理される時に、このポリシーによって認可ポリシー規則で使用できる関連 ID グループが取得されます。

グループマッピングポリシーを含むアクセスサービスを作成した場合は、このポリシーを設定および変更できます。すべての要求に同じ ID グループを適用する単純なポリシー、またはルールベースのポリシーを設定できます。

ルールベースのポリシーでは、各規則に 1 つ以上の条件と結果が含まれます。条件は、外部属性ストアから取得された属性またはグループだけに基づくことができます。結果は、ID グループ階層内の ID グループです。ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。



注意

単純なポリシー ページとルールベースのポリシー ページを切り替えると、以前に保存したポリシーは失われます。

単純なグループマッピングポリシーを設定するには、次の手順を実行します。

- ステップ 1** [Access Policies] > [Access Services] > *service* > [Group Mapping] を選択します。 *service* は、アクセスサービスの名前です。
- デフォルトでは、[Simple Group Mapping Policy] ページが表示されます。フィールドの説明については、表 10-12 を参照してください。
- [Rule-Based Group Mapping Policy] ページのフィールドの説明については、表 10-13 を参照してください。

表 10-12 [Simple Group Mapping Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 <ul style="list-style-type: none"> Simple : 結果がすべての要求に適用されることを指定します。 Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。
	<p>注意 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Identity Group	すべての要求の属性とグループをマッピングする ID グループ。

表 10-13 [Rule-based Group Mapping Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> Simple : 結果がすべての要求に適用されることを指定します。 Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。 <p> 注意 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Status	<p>規則の現在のステータス。規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> Enabled : 規則はアクティブです。 Disabled : ACS によって規則の結果は適用されません。 Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として使用される ID グループ。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	<p>次の場合に、ACS によってデフォルト規則が適用されます。</p> <ul style="list-style-type: none"> イネーブルな規則が一致しない。 他の規則が定義されていない。 <p>デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。</p>
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。Hit カウントの表示 (10-10 ページ) を参照してください。

ステップ 2 ID グループを選択します。

ステップ 3 [Save Changes] を選択して、ポリシーを保存します。

ルール ベースのポリシーを設定するには、次の項を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)

- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

関連項目

- [ID ポリシーの表示 \(10-23 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [デバイス管理のシェル/コマンド認可ポリシーの設定 \(10-36 ページ\)](#)

グループマッピングポリシー規則のプロパティの設定

このページは、外部データベースから取得された属性とグループの ACS ID グループへのマッピングを定義するグループマッピングポリシー規則を作成、複製、または編集するために使用します。

ステップ 1 [Access Policies] > [Access Services] > *service* > [Group Mapping] を選択し、次のいずれかを実行します。

- [Create] をクリックします。
- 規則チェックボックスをオンにし、[Duplicate] をクリックします。
- 規則名をクリックするか規則チェックボックスをオンにし、[Edit] をクリックします。

ステップ 2 [表 10-14](#) の説明に従って、フィールドに入力します。

表 10-14 [\[Group Mapping Rule Properties\] ページ](#)

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、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。
Rule Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログエントリには、規則がモニタだけであることを示す情報が含まれます。モニタオプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。

表 10-14 [Group Mapping Rule Properties] ページ (続き)

オプション	説明
Results	
Identity Group	要求の属性とグループをマッピングする ID グループ。

ネットワーク アクセスのセッション認可ポリシーの設定

ネットワーク アクセス認可のアクセス サービスを作成すると、セッション認可ポリシーが作成されます。その後、このポリシーに規則を追加し、変更してクライアントセッションのアクセス権を決定できます。

標準の最初に一致する規則テーブルであるスタンドアロン認可ポリシーをアクセス サービスに作成できます。例外ポリシーを含む認可ポリシーを作成することもできます。[認可例外ポリシーの設定 \(10-37 ページ\)](#) を参照してください。要求が例外規則に一致すると、ポリシー例外規則の結果が常に適用されます。

規則には、任意の条件と複数の結果を含めることができます。

- 認可プロファイル：ユーザ定義属性を定義し、任意で、Access-Accept メッセージによって返されるダウンロード可能 ACL を定義します。
- セキュリティグループタグ (SGT)：Cisco Security Group Access をインストールした場合、要求に適用する SGT を認可規則で定義できます。

ACS が複数の認可プロファイルを含む規則を処理する方法の詳細については、[複数の認可プロファイルを含む規則の処理 \(3-17 ページ\)](#) を参照してください。

認可ポリシーを設定するには、次の項を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)


認可ポリシーの作成については、次を参照してください。

- ホストルックアップ要求については、[ACS とシスコセキュリティグループアクセス \(4-24 ページ\)](#) を参照してください。
- Security Group Access のサポートについては、[エンドポイントアドミッションコントロールポリシーの作成 \(4-27 ページ\)](#) を参照してください。

ステップ 1 [Access Policies] > [Access Services] > *service* > [Authorization] を選択します。

ステップ 2 表 10-15 の説明に従って、フィールドに入力します。

表 10-15 [Network Access Authorization Policy] ページ

オプション	説明
Status	<p>規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。
NDG:name	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。
conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	
Authorization Profile	<p>対応する規則が一致したときに適用される認可プロファイルを表示します。</p> <p>Security Group Access 機能をイネーブルにすると、規則の結果をカスタマイズできます。規則では、エンドポイントのアクセス権限、そのエンドポイントのセキュリティグループ、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。</p>
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	<p>次の場合に、ACS によってデフォルト規則が適用されます。</p> <ul style="list-style-type: none"> • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 <p>デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。</p>
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。</p> <p>Security Group Access 機能をイネーブルにすると、規則の結果セットを選択することもできます (セッション認可プロファイルのみ、セキュリティグループのみ、または両方)。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。Hit カウントの表示 (10-10 ページ) を参照してください。

ネットワーク アクセス認可規則のプロパティの設定

このページは、ネットワーク アクセス サービスのアクセス権を決定する規則を作成、複製、および編集する場合に使用します。

ステップ 1 [Access Policies] > [Access Services] > <service> > [Authorization] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。

ステップ 2 表 10-16 の説明に従って、フィールドに入力します。

表 10-16 [Network Access Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、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。
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。
Results	
Authorization Profiles	使用可能なプロファイルと選択されたプロファイルのリスト。要求に適用する複数の認可ポリシーを選択できます。矛盾を解決する場合の認可ポリシー順序の重要性については、 複数の認可プロファイルを含む規則の処理 (3-17 ページ) を参照してください。
Security Group	(Security Group Access のみ) 適用するセキュリティグループ。 Security Group Access をイネーブルにすると、セッション認可プロファイルのみ、セキュリティグループのみ、または両方を表示するように結果オプションをカスタマイズできます。

デバイス管理認可ポリシーの設定

デバイス管理認可ポリシーは、ネットワーク管理者の認可と権限を決定します。

認可ポリシーは、アクセスサービスの作成中に作成します。[Access Service Create] ページの詳細については、[アクセスサービスの一般プロパティの設定 \(10-13 ページ\)](#) を参照してください。


このページを使用して、次のことを行います。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズできるページを開きます。

[Access Policies] > [Access Services] > *service* > [Authorization] を選択します。

表 10-17 で説明されている [Device Administration Authorization Policy] ページが表示されます。

表 10-17 [Device Administration Authorization Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用されるシェル プロファイルとコマンドセットを表示します。規則の結果をカスタマイズできます。規則によって、シェル プロファイル、コマンドセット、またはその両方を適用できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 <ul style="list-style-type: none"> • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件および結果のタイプを選択する [Customize] ページを開きます。[Conditions] および [Results] カラムには、カスタマイゼーション設定が反映されます。  注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウンタの表示 (10-10 ページ) を参照してください。

デバイス管理認可規則のプロパティの設定

このページは、デバイス管理アクセスサービスの認可および権限を決定する規則を作成、複製、および編集する場合に使用します。

[Access Policies] > [Access Services] > **service** > [Authorization] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。

表 10-18 で説明されている [Device Administration Authorization Rule Properties] ページが表示されます。

表 10-18 [Device Administration Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、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。
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。
Results	
Shell Profiles	ルールに適用するシェルプロファイル。
Command Sets	使用可能なコマンドセットと選択されたコマンドセットのリスト。適用する複数のコマンドセットを選択できます。

デバイス管理認可例外ポリシーの設定

定義済み認可ポリシーのデバイス管理認可例外ポリシーを作成できます。例外規則の結果は、常に認可ポリシー規則よりも優先されます。


このページを使用して、次のことを行います。

- 例外規則を表示します。
- 例外規則を削除します。
- 例外規則を作成、複製、編集、およびカスタマイズするページを開きます。

[Access Policies] > [Access Services] > **service** > [Authorization] を選択し、[Device Administration Authorization Exception Policy] をクリックします。

表 10-19で説明されている [Device Administration Authorization Exception Policy] ページが表示されます。

表 10-19 [Device Administration Authorization Exception Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。
NDG:name	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。
Condition	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用されるシェルプロファイルとコマンドセットを表示します。規則の結果をカスタマイズできます。規則によって、シェルプロファイル、コマンドセット、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。対応する認可ポリシーと同じ条件および結果のセットを使用する必要はありません。  注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。Hit カウントの表示 (10-10 ページ) を参照してください。

デバイス管理のシェル/コマンド認可ポリシーの設定

アクセスサービスを作成してデバイス管理のサービスポリシー構造を選択すると、ACS によって自動的にシェル/コマンド認可ポリシーが作成されます。その後、ポリシー規則を作成および変更できます。

Web インターフェイスでは、デバイス管理の複数のコマンドセットを作成する機能がサポートされています。この機能を使用すると、保持する基本コマンドセットの数を少なくすることができます。すべての組み合わせを個々のコマンドセットで保持するのではなく、規則の結果としてコマンドセットを組み合わせて選択できます。

例外ポリシーを含む認可ポリシーを作成して、標準のポリシー結果よりも優先させることもできます。認可例外ポリシーの設定 (10-37 ページ) を参照してください。

ACS が複数のコマンドセットを含む規則を処理する方法の詳細については、複数のコマンドセットを持つ規則の処理 (3-11 ページ) を参照してください。

規則を設定するには、次の項を参照してください。

- ポリシー規則の作成 (10-38 ページ)
- 規則の複製 (10-40 ページ)
- ポリシー規則の編集 (10-40 ページ)
- ポリシー規則の削除 (10-41 ページ)

認可例外ポリシーの設定

認可ポリシーには例外ポリシーを含めることができます。一般に、例外は一時ポリシーです。たとえば、ビジターに一時的なアクセス権を付与したり、特定のユーザに対してアクセスレベルを上げたりします。例外ポリシーは、変化する状況やイベントに効率的に対応するために使用します。

例外規則の結果は、常に標準の認可ポリシー規則よりも優先されます。

例外ポリシーは、メインの認可ポリシーテーブルとは別の規則テーブルに作成します。対応する標準の認可ポリシーで使用されているのと同じポリシー条件を例外ポリシーで使用する必要はありません。


例外ポリシー規則のページにアクセスするには、次の手順を実行します。

- ステップ 1** [Access Policies] > [Service Selection Policy] > *service* > [authorization policy] を選択します。*service* はアクセス サービスの名前、*authorization policy* はセッション認可またはシェル/コマンドセット認可ポリシーです。
- ステップ 2** ルールベースのポリシー ページで、規則テーブルの上にある [Exception Policy] リンクをクリックします。
- 表 10-20 で説明されているフィールドを含む [Exception Policy] テーブルが表示されます。

表 10-20 [Network Access Authorization Exception Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。

表 10-20 [Network Access Authorization Exception Policy] ページ (続き)

オプション	説明
NDG:name	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。
Condition Name	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用される認可プロファイルを表示します。 Security Group Access 機能をイネーブルにすると、規則の結果をカスタマイズできます。規則では、エンドポイントのアクセス権限、そのエンドポイントのセキュリティグループ、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。対応する認可ポリシーと同じ条件のセットを使用する必要はありません。 Security Group Access 機能をイネーブルにすると、規則の結果セットを選択することもできます (セッション認可プロファイルのみ、セキュリティグループのみ、または両方)。  注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウントの表示 (10-10 ページ) を参照してください。

規則を設定するには、次の項を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

関連項目

- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [デバイス管理のシェル/コマンド認可ポリシーの設定 \(10-36 ページ\)](#)

ポリシー規則の作成

規則を作成するときは、規則の順序が重要であることに注意してください。ACS ネットワークにアクセスしようとするクライアントの要求が ACS によって処理されるときに一致が見つかったら、その後の処理はすべて停止され、その一致に関連する結果が検索されます。一致が見つかったあとは、それ以降の規則は考慮されません。

一致する規則がないか、または規則が定義されていない場合は、デフォルト規則によってデフォルトのポリシーが指定されます。デフォルト規則の結果は編集できます。

はじめる前に

- ポリシー条件および結果を設定します。[ポリシー条件の管理 \(9-1 ページ\)](#) を参照してください。
- ポリシー規則によって適用される条件および結果のタイプを選択します。[ポリシーのカスタマイズ \(10-4 ページ\)](#) を参照してください。

新規のポリシー規則を作成するには、次の手順を実行します。

-
- ステップ 1** [Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセスサービスの名前、*policy* はポリシーのタイプです。次の場合があります。
- ルールベースのポリシーを前に作成したことがある場合は、設定されている規則のリストを含むルールベースのポリシー ページが表示されます。
 - ルールベースのポリシーを作成したことがない場合は、単純なポリシー ページが表示されます。[Rule-Based] をクリックします。
- ステップ 2** [Rule-Based Policy] ページで、[Create] をクリックします。
[Rule] ページが表示されます。
- ステップ 3** 規則を定義します。
- ステップ 4** [OK] をクリックします。
新しい規則を示す [Policy] ページが表示されます。
- ステップ 5** [Save Changes] をクリックして、新規の規則を保存します。
-

アクセス サービスによって処理されるすべての要求に同じ結果を使用する単純なポリシーを設定するには、次を参照してください。

- [ID ポリシーの表示 \(10-23 ページ\)](#)
- [グループマッピングポリシーの設定 \(10-28 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [ネットワーク アクセスのセッション認可ポリシーの設定 \(10-31 ページ\)](#)
- [デバイス管理のシェル/コマンド認可ポリシーの設定 \(10-36 ページ\)](#)

関連項目

- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)



(注)

ACS 5.8 では、ACS Web インターフェイスからアクセス サービス ポリシーを作成、編集、または並べ替えるために ACS 設定監査レポートの詳細な監査レポートが表示されます。

規則の複製

既存の規則と同じか、または既存の規則によく似た新規の規則を作成する場合は、規則を複製できます。複製された規則名では、元の規則に複製を示すカッコが付けられます。たとえば、Rule-1(1)です。

複製の完了後は、各規則（元の規則および複製された規則）に個別にアクセスします。



(注) デフォルト規則は複製できません。

規則を複製するには、次の手順を実行します。

-
- ステップ 1** [Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセスサービスの名前、*policy* はポリシーのタイプです。
- 設定されている規則のリストを含む [Policy] ページが表示されます。
- ステップ 2** 複製する規則のチェックボックスにチェックを入れます。デフォルト規則は複製できません。
- ステップ 3** [Duplicate] をクリックします。
- [Rule] ページが表示されます。
- ステップ 4** 規則の名前を変更し、他の該当するフィールド オプションに入力します。
- ステップ 5** [OK] をクリックします。
- 新しい規則を示す [Policy] ページが表示されます。
- ステップ 6** [Save Changes] をクリックして、新規の規則を保存します。
- ステップ 7** 重複する規則をキャンセルするには、[Discard Changes] をクリックします。
-

関連項目

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

ポリシー規則の編集

ポリシー規則のすべての値を編集できます。また、デフォルト規則の結果を編集することもできます。

規則を編集するには、次の手順を実行します。

-
- ステップ 1** [Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセスサービスの名前、*policy* はポリシーのタイプです。
- 設定されている規則のリストを含む [Policy] ページが表示されます。
- ステップ 2** 変更する規則名をクリックします。または、名前前のチェックボックスをオンにして [Edit] をクリックします。
- [Rule] ページが表示されます。

- ステップ 3 適切な値を編集します。
- ステップ 4 [OK] をクリックします。
編集された規則を示す [Policy] ページが表示されます。
- ステップ 5 [Save Changes] をクリックして、新しい設定を保存します。
- ステップ 6 編集した情報をキャンセルするには、[Discard Changes] をクリックします。

関連項目

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

ポリシー規則の削除



(注) デフォルト規則は削除できません。

ポリシー規則を削除するには、次の手順を実行します。

- ステップ 1 [Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。 *service* はアクセスサービスの名前、*policy* はポリシーのタイプです。
設定されている規則のリストを含む [Policy] ページが表示されます。
- ステップ 2 削除する規則のチェックボックスに 1 つ以上のチェックを入れます。
- ステップ 3 [Delete] をクリックします。
[Policy] ページが表示されます。このとき、削除した規則は表示されません。
- ステップ 4 [Save Changes] をクリックして、新しい設定を保存します。
- ステップ 5 削除された情報を保持するには、[Discard Changes] をクリックします。

関連項目

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)

複合条件の設定

複合条件は、単純なポリシー条件で許可された属性に基づく条件のセットを定義する場合に使用します。複合条件はポリシー規則ページで定義します。個別の条件オブジェクトとして定義することはできません。

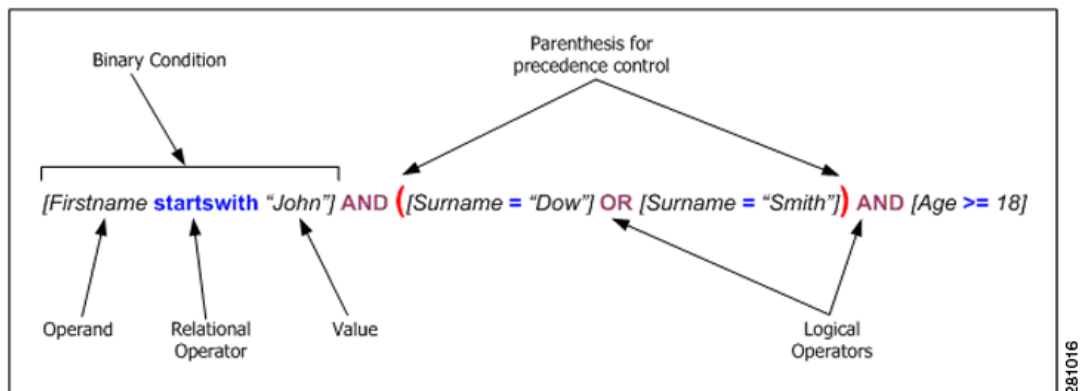
ここでは、次の内容について説明します。

- 複合条件の構築ブロック (10-42 ページ)
- 複合条件のタイプ (10-43 ページ)
- 複合式ビルダーの使用方法 (10-46 ページ)

複合条件の構築ブロック

図 10-1 に、複合条件の構築ブロックを示します。

図 10-1 複合条件の構築ブロック



- オペランド：属性または条件のタイプ。プロトコル/要求属性、ID 属性、ID グループ、ネットワーク デバイス グループ (NDG)、日付/時刻、カスタムまたは標準条件など。
- 関係演算子：オペランドと値の関係を指定する演算子。等号 (=)、一致しない、など。条件で使用できる演算子は、オペランドのタイプによって異なります。
- バイナリ条件：指定されたオペランドと値の関係を定義します。[username = "Smith"] など。
- 論理演算子：バイナリ条件、またはバイナリ条件の間に適用されます。サポートされている論理演算子は、AND と OR です。
- 優先制御：カッコを使用して、論理演算子の優先順位を変更できます。管理者はカッコを入れ子にして優先順位を制御できます。論理演算子の通常の優先順位、つまりカッコを使用しない場合の優先順位は、NOT、AND、OR の順です。NOT の優先順位が最も高く、OR の優先順位が最も低くなります。

表 10-21 に、複合条件の構築中にサポートされる動的属性マッピングの概要を示します。

表 10-21 ポリシーの複合条件でサポートされる動的属性マッピング

オペランド1	オペランド2	例
文字列属性	文字列属性	—
整数属性	整数属性	—
列挙型属性	列挙型属性	—
ブール属性	ブール属性	—
IP アドレス属性	IP アドレス属性	—

表 10-21 ポリシーの複合条件でサポートされる動的属性マッピング

オペランド 1	オペランド 2	例
特別な場合		
階層型属性	文字列属性	NDG : Customer と 「内部ユーザ」 の文字列属性
文字列属性	階層型属性	—



(注)

動的属性マッピングは、「String Enum」タイプの ExternalGroups 属性および「Date Time Period」タイプの「Time And Date」属性には適用できません。

階層型属性の場合、階層型属性と比較する文字列属性を設定する際に、文字列属性の値は階層型属性名で始まる必要があるため、値には属性名が付きます。

次に例を示します。

- NDG の下で作成された *DeviceGroup* 属性と比較する *UrsAttr* という新しい文字列属性を定義する場合、*UrsAttr* の値は次のように設定する必要があります。

DeviceGroup: Value

- 各内部ユーザ内の階層型属性である *UserIdentityGroup* と文字列属性を比較する場合は、文字列属性を次のように設定する必要があります。

IdentityGroup:All Groups:"Identity Group Name"

関連項目

- [複合条件のタイプ \(10-43 ページ\)](#)
- [複合式ビルダーの使用方法 \(10-46 ページ\)](#)

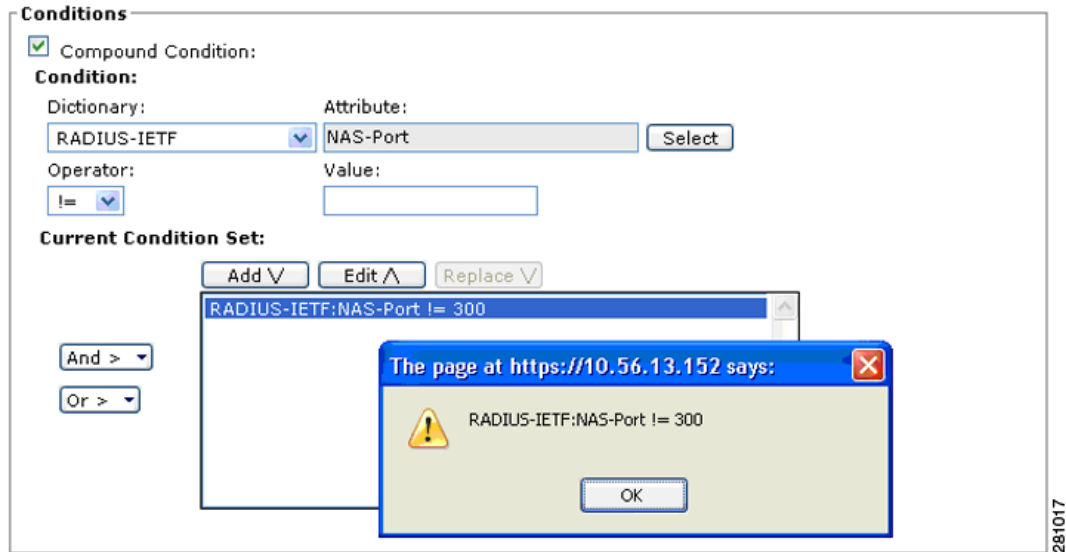
複合条件のタイプ

3つのタイプの複合条件を作成できます。

アトミック条件

1つの述語で構成され、リスト内の唯一のエントリです。NDGを除いて、規則テーブル内のすべての単純な条件では、属性と値の間で等号 (=) 演算が行われると想定されるため、アトミック条件は等号 (=) 以外の演算子の選択に使用されます。例については、[図 10-2](#)を参照してください。

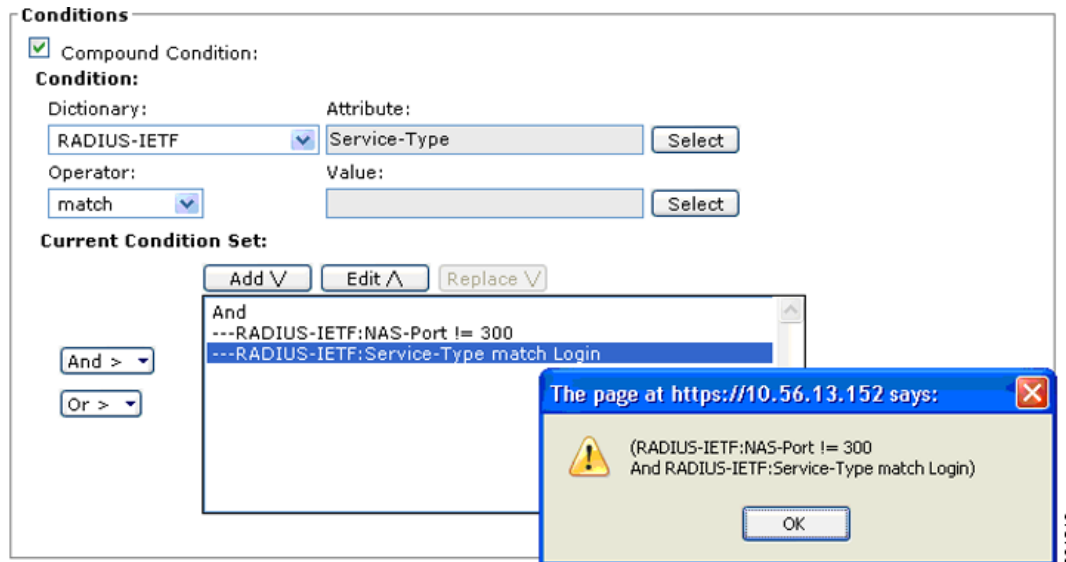
図 10-2 複合式: アトミック条件



単一の入れ子になった複合条件

単一の演算子とそのあとに続く述語のセット（2つ以上）で構成されます。演算子は、それぞれの述語の間に適用されます。例については、図 10-3を参照してください。プレビュー ウィンドウには、論理演算子の優先を示すカッコ [()] が表示されます。

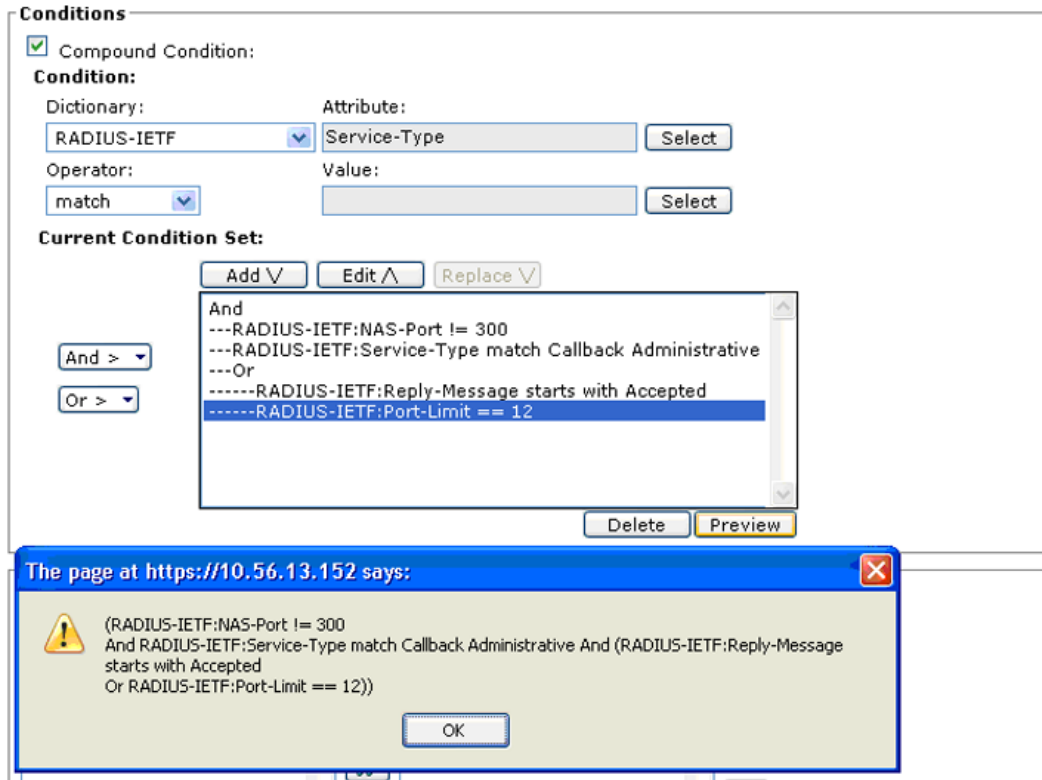
図 10-3 単一の入れ子になった複合式



複数の入れ子になった複合条件

条件の任意の述語を別の単純な入れ子になった複合条件に置き換えることによって、単一の入れ子になった複合条件を拡張できます。例については、図 10-4を参照してください。プレビュー ウィンドウには、論理演算子の優先を示すカッコ [()] が表示されます。

図 10-4 複数の入れ子になった複合式

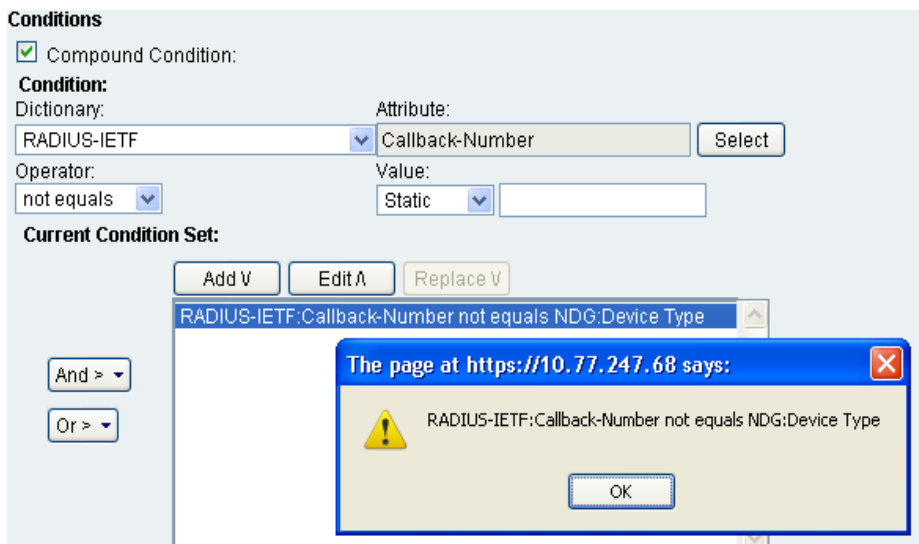


281019

動的な値を持つ複合式

オペランドとして選択されたディクショナリ属性と比較する、別のディクショナリ属性を選択するために動的な値を選択できます。例については、図 10-5を参照してください。

図 10-5 動的な値を持つ複合式ビルダー



282674

関連項目

- 複合条件の構築ブロック (10-42 ページ)
- 複合式ビルダーの使用法 (10-46 ページ)

複合式ビルダーの使用法

複合条件を作成するには、規則のプロパティ ページで式ビルダーを使用します。式ビルダーには2つのセクションがあります。プライマリ条件を作成する述語ビルダーと、式を管理するためのコントロールです。

最初のセクションでは、プライマリ条件を定義します。オペランドを定義するディクショナリと属性を選択し、演算子を選択し、条件の値を指定します。2番目のセクションでは、条件の順序を整理し、バイナリ条件またはバイナリ条件の間に適用される論理演算子を指定します。

表 10-22 に、条件式ビルダーのフィールドを示します。

表 10-22 式ビルダーのフィールド

フィールド	説明
Condition	このセクションでは、プライマリ条件を定義します。
Dictionary	オペランドを取得するディクショナリを指定します。使用できるオプションは、定義するポリシーによって異なります。たとえば、サービス セレクション ポリシーを定義する場合、ID ディクショナリは使用できません。
Attribute	条件のオペランドである属性を指定します。使用できる属性は、選択したディクショナリによって異なります。
Operator	関係演算子の内容は、上記のオペランド フィールドの選択内容に従って動的に決定されます。
Value	条件の値。このフィールドのタイプは、条件または属性のタイプによって異なります。次の2つのオプションのいずれかを選択します。 <ul style="list-style-type: none"> • [Static] : 選択した場合、属性タイプに応じて、静的な値を入力または選択する必要があります。 • [Dynamic] : 選択した場合、オペランドとして選択されたディクショナリ属性と比較する、別のディクショナリ属性を選択できます。
Current Condition Set	このセクションでは、条件の順序を整理し、バイナリ条件またはバイナリ条件の間に適用する論理演算子を指定します。
Condition list	複合条件の定義済みバイナリ条件および関連付けられている論理演算子のリストが表示されます。
Add	バイナリ条件の定義後、[Add] をクリックして条件を条件リストに追加します。
Edit	バイナリ条件を編集するには、条件リストで条件を選択し、[Edit] をクリックします。[Condition] フィールドに条件のプロパティが表示されます。条件を必要に応じて変更し、[Replace] をクリックします。
Replace	選択した条件を [Condition] フィールドで現在定義されている条件に置き換える場合にクリックします。
And Or	選択した条件に適用する論理演算子、または選択した条件とその上の条件間に適用する論理演算子を指定します。適切な演算子をクリックし、[Insert] をクリックして演算子を別の行として追加します。または、演算子をクリックし、[Replace] をクリックして選択した行を置き換えます。
Delete	選択したバイナリ条件または演算子を条件リストから削除する場合にクリックします。
Preview	現在の式に対応するカッコ表現で表示する場合にクリックします。複合式の作成後、規則テーブルにカッコ表現が表示されます。

関連項目

- [複合条件の構築ブロック \(10-42 ページ\)](#)
- [複合条件のタイプ \(10-43 ページ\)](#)

[Security Group Access Control] ページ

ここでは、次の内容について説明します。

- [\[Egress Policy Matrix\] ページ \(10-47 ページ\)](#)
- [出力ポリシー マトリクスのセルの編集 \(10-48 ページ\)](#)
- [出力ポリシーのデフォルト ポリシーを定義ページ \(10-48 ページ\)](#)
- [NDAC ポリシー ページ \(10-49 ページ\)](#)
- [\[NDAC Policy Properties\] ページ \(10-51 ページ\)](#)
- [\[Network Device Access EAP-FAST Settings\] ページ \(10-52 ページ\)](#)

[Egress Policy Matrix] ページ

出力ポリシーは SGACL ポリシーとも呼ばれ、送信元および宛先 SGT に基づいてネットワークの出力ポイントで適用する SGACL を決定します。ACS は、出力ポリシーをマトリクスとして表します。送信元および宛先の軸にすべてのセキュリティ グループを表示します。マトリクス内の各セルには、対応する送信元および宛先 SGT に適用する ACL のセットを含めることができます。

ネットワーク デバイスによって、セルに定義した特定のポリシーにデフォルト ポリシーが追加されます。空のセルの場合、デフォルト ポリシーだけが適用されます。

出力ポリシーのマトリクスを使用して、対応する送信元および宛先 SGT に適用する ACL のセットを表示、定義、および編集します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択します。

表 10-23 [Egress Policy Matrix] ページ

オプション	説明
Destination Security Group	すべての宛先セキュリティ グループが表示されるカラムの見出し。
Source Security Group	すべての送信元セキュリティ グループが表示される行の見出し。
Cells	対応する送信元および宛先セキュリティ グループに適用する SGACL を含めます。
Edit	セルをクリックしてから [Edit] をクリックして、そのセルの [Edit] ダイアログボックスを開きます。 出力ポリシー マトリクスのセルの編集 (10-48 ページ) を参照してください。

表 10-23 [Egress Policy Matrix] ページ (続き)

オプション	説明
Default Policy	デフォルトの出力ポリシーを定義するためのダイアログボックスを開く場合にクリックします。出力ポリシーのデフォルトポリシーを定義ページ (10-48 ページ) を参照してください。
Set Matrix View	出力ポリシーのマトリクス表示を変更するには、オプションを選択し、[Go] をクリックします。 <ul style="list-style-type: none"> All : 出力ポリシー マトリクスのすべての行とカラムを消去します。 Customize View : 選択したセルに対応する送信元および宛先セキュリティ グループをカスタマイズできるウィンドウを開きます。

関連項目

- 出力ポリシーの作成 (4-28 ページ)

出力ポリシー マトリクスのセルの編集

このページは、選択したセルのポリシーを設定する場合に使用します。対応する送信元および宛先セキュリティ グループに適用する SGACL を設定できます。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、セルを選択してから [Edit] をクリックします。

表 10-24 [Edit Cell] ページ

オプション	説明
Configure Security Groups	表示のみ。選択したセルの送信元および宛先セキュリティ グループ名が表示されます。
General	セルのポリシーの説明。
ACL	対応する送信元および宛先セキュリティ グループに適用する SGACL を、[Available] リストから [Selected] リストに移動します。SGACL のリストの順序を指定するには、上向き (^) および下向き (v) 矢印を使用します。

関連項目

- 出力ポリシーの作成 (4-28 ページ)

出力ポリシーのデフォルト ポリシーを定義ページ

このページは、デフォルトの出力ポリシーを定義する場合に使用します。ネットワーク デバイスによって、セルに定義されている特定のポリシーにデフォルト ポリシーが追加されます。空のセルの場合、デフォルト ポリシーだけが適用されます。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、[Default Policy] をクリックします。

表 10-25 [Default Policy] ページ

オプション	説明
ACL	対応する送信元および宛先セキュリティグループに適用する SGACL を、[Available] リストから [Selected] リストに移動します。SGACL のリストの順序を指定するには、上向き (^) および下向き (v) 矢印を使用します。 最終的な catch-all 規則として [Permit All] または [Deny All] を選択します。

関連項目

- [出力ポリシーの作成 \(4-28 ページ\)](#)
- [デフォルト ポリシーの作成 \(4-29 ページ\)](#)

NDAC ポリシー ページ

ネットワーク デバイス アドミッション コントロール (NDAC) ポリシーは Security Group Access 環境のネットワーク デバイスの SGT を決定します。NDAC ポリシーは次の要求を処理します。

- あるデバイスからのネイバーに関するピア認可要求。
- 環境要求 (デバイスはそのデバイス自体に関する情報を収集します)。

要求のタイプにかかわらず、特定のデバイスについては同じ SGT がポリシーによって返されます。



(注)

NDAC ポリシーはデフォルトで実装されるため、アクセス サービスに追加しないでください。ただし、エンドポイント アドミッション コントロールの場合、アクセス サービスとセッション認可ポリシーを定義する必要があります。セッション認可ポリシーの作成については、[ネットワーク アクセス認可規則のプロパティの設定 \(10-33 ページ\)](#) を参照してください。

このページは、すべてのデバイスに同じセキュリティグループを割り当てる単純なポリシーを設定するか、またはルールベースのポリシーを設定する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] > [Authentication Policy] を選択します。

すでに NDAC ポリシーが設定されている場合は、対応する単純なポリシー ページまたはルールベースのポリシー ページが開きます。設定されていない場合は、デフォルトで単純なポリシー ページが開きます。

単純なポリシー ページ

このページは、単純な NDAC ポリシーを定義する場合に使用します。

表 10-26 [Simple NDAC Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> • Simple : 結果がすべての要求に適用されることを指定します。 • Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。 <p>ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Security Group	<p>デバイスに割り当てるセキュリティグループを選択します。デフォルトは [Unknown] です。</p>

ルールベースのポリシー ページ


ルールベースのポリシーに関するこのページを使用して、次のことを行います。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズするページを開きます。

表 10-27 [Rule-Based NDAC Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> • Simple : 結果がすべての要求に適用されることを指定します。 • Rule-based : 要求に応じて異なる結果が適用されるように規則を設定します。 <p>ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Status	<p>規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	<p>ルールの名前。デフォルト規則は次の場合に条件に使用できます。</p> <ul style="list-style-type: none"> • イネーブルな規則が一致しない。 • 規則が定義されていない。 <p>規則を編集または複製するには、リンクをクリックします。</p> <p>デフォルト規則は編集できますが、削除、ディセーブル、または複製することはできません。</p>
Conditions	<p>ポリシー規則の定義に使用できる条件。規則の条件の表示を変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。</p>
Results	<p>対応する条件に一致した場合にデバイスに割り当てられるセキュリティグループが表示されます。</p>
Hit Count	<p>規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。</p>

表 10-27 [Rule-Based NDAC Policy] ページ (続き)

オプション	説明
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。ポリシーページでは、各追加条件に対して新規の条件欄が表示されます。認証ポリシーに対応した同様の条件を使用する必要はありません。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。Hit カウントの表示 (10-10 ページ) を参照してください。

関連トピック：

- [NDAC ポリシーの設定 \(4-26 ページ\)](#)
- [\[NDAC Policy Properties\] ページ \(10-51 ページ\)](#)

[NDAC Policy Properties] ページ

このページは、デバイスの SGT を決定する規則を作成、複製、および編集する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] > [Authentication Policy] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。



(注) エンドポイントアドミッションコントロールの場合、アクセスサービスとセッション認可ポリシーを定義する必要があります。セッション認可ポリシーの作成については、[ネットワークアクセス認可規則のプロパティの設定 \(10-33 ページ\)](#) を参照してください。

表 10-28 [NDAC Policy Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、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。
Status	<p>規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログエントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。

表 10-28 [NDAC Policy Properties] ページ (続き)

オプション	説明
Conditions	
conditions	規則に対して設定できる条件。各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を入力します。 複合式の条件が使用できる場合は、[Compound Expression] をオンにすると、式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。 ポリシーの条件のリストを変更するには、 NDAC ポリシー ページ (10-49 ページ) の [Customize] ボタンをクリックします。
Results	
Security Group	対応する条件に一致した場合にデバイスに割り当てるセキュリティグループを選択します。

関連トピック：

- [NDAC ポリシーの設定 \(4-26 ページ\)](#)
- [NDAC ポリシー ページ \(10-49 ページ\)](#)

[Network Device Access EAP-FAST Settings] ページ

このページは、NDAC ポリシーで使用する EAP-FAST プロトコルのパラメータを設定する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] を選択します。

表 10-29 [Network Device Access EAP-FAST Settings] ページ

オプション	説明
EAP-FAST の設定	
Tunnel PAC Time To Live	PAC が期限切れになり置換する必要があるまでの PAC の存続可能時間 (TTL) または期間。
Proactive PAC Update When % of PAC TTL is Left	PAC の更新が必要になる時点における PAC TTL の残り時間のパーセンテージ。

関連トピック：

- [NDAC ポリシーの設定 \(4-26 ページ\)](#)
- [Security Group Access 用の EAP-FAST 設定の構成 \(4-27 ページ\)](#)
- [NDAC ポリシー ページ \(10-49 ページ\)](#)

最大ユーザセッション数

最適なパフォーマンスを得るには、ネットワーク リソースにアクセスする同時ユーザ数を制限できます。ACS 5.8 は、ユーザ 1 人あたりの同時サービスセッションの数に制限を課します。

制限はいくつかの方法で設定されます。ユーザ レベルまたはグループ レベルで制限を設定できます。最大ユーザセッションの設定に応じて、セッション カウントはユーザに適用されます。



(注) 最大セッション数をユーザに有効にするには、管理者は RADIUS アカウンティングを設定する必要があります。



(注) 最大セッション数をデバイス管理に有効にするには、管理者は TACACS+ セッション認可およびアカウンティングを設定する必要があります。

ここでは、次の内容について説明します。

- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッション グループ設定 \(10-54 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)
- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

最大セッションユーザの設定

各ユーザの最大ユーザセッションをグローバルに設定できます。

最大ユーザセッション数を設定するには、次の手順を実行します。

- ステップ 1 [Access Policies] > [Max User Session Policy]> [Max Session User Settings]を選択します。
- ステップ 2 [Max User Session Value] を、許可される同時セッションの最大数に指定します。
- ステップ 3 ユーザのセッション数を無制限にするには、[Unlimited Sessions] 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。



(注) セッションの最大数がユーザ レベルとグループ レベルの両方で設定されている場合、小さい方の値が優先されます。

次に例を示します。

グループ America:US:West のユーザ Bob のグループの最大セッション値は 5 セッション、そのユーザの最大セッション値は 5 であるとしてします。この場合、ユーザ Bob に可能な最大セッションは 5 だけになります。

関連項目

- [最大セッション グループ設定 \(10-54 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)

- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

最大セッショングループ設定

ID グループの最大セッション数を設定できます。グループ内の少人数のユーザによってすべてのセッションが使用される場合があります。他のユーザからの新しいセッションの作成要求は、セッション数がすでに最大設定値に達しているため、拒否されます。

ACS 5.8 では、グループ内のユーザに最大セッション制限を設定できます。たとえば、特定の ID グループに所属する各ユーザは、同じグループの他のユーザが開いているセッション数に関係なく、制限以上はセッションを開くことができません。特定のユーザにセッション制限を設定するオプションはありません。

ACS Web インターフェイスから ID グループに所属するユーザの最大セッション制限を設定できます。

ACS 4.x 移行ユーティリティには、最大セッション設定の移行が含まれています。

特定のユーザのセッション制限を計算する場合は、ユーザ 1 人あたりのグローバルセッション制限、ユーザが所属する ID グループあたりのセッション制限、グループ内のユーザ 1 人あたりのセッション制限のいずれか最小設定値が優先されます。

グループの最大セッション数を設定するには、次の手順を実行します。

-
- ステップ 1 [Access Policies] > [Max User Session Policy] > [Max Session Group Settings] を選択します。設定した ID グループがすべて一覧表示されます。
- ステップ 2 最大セッション数を設定するグループのチェックボックスをオンにします。
- ステップ 3 [Edit] をクリックします。
- ステップ 4 [表 10-30](#)の説明に従って、フィールドに入力します。

表 10-30 [Max User Session Global Settings] ページ

オプション	説明
General	
Name	ID グループの名前。
Description	ID グループの説明。
Max Session Group Settings	
Unlimited Session	グループに無制限セッションを提供する場合に、このチェックボックスをオンにします。
Max Session for Group	グループに許可する同時セッションの最大数の値を指定します。
Unlimited Sessions for Users in Group	グループの各ユーザに無制限のセッションを提供する場合は、このチェックボックスをチェックします。
Max Session for User in Group	グループ内の各ユーザに許可する同時セッションの最大数の値を指定します。このオプションは、グループの最大セッション数を上書きします。

- ステップ 5 [Submit] をクリックします。
-

[Unlimited] がデフォルトで選択されています。階層に基づいてグループレベルのセッションが適用されます。次に例を示します。

グループ階層は、[America:US:West:CA] で最大セッションは次のとおりです。

- America: 最大 100 セッション
- US: 最大 80 セッション
- West: 最大 75 セッション
- CA: 最大 50 セッション

「グループ X のユーザの最大セッション数」が N に設定されている場合、グループ X に属する各ユーザは N セッションより多くを開くことはできません。

ユーザが *America/US/West* に属している場合、ACS は、セッション数がグループ *America/US/West*、*America/US*、*America* に指定された制限を超えていないことを確認します。ユーザグループの最大セッション数を 100 に設定した場合、グループのすべてのメンバーによって確立されたすべてのセッションの総数は 100 を超えることはできません。セッションが許可されると、3 つのノードの [Number of Active Sessions Available] カウンタが 1 増加します。ACS ランタイムコンポーネントは、認証中にこの検証を処理します。



(注)

セッションの最大数がグループレベル、グループレベル内のユーザレベル、およびユーザレベルでグローバルに設定されている場合、ACS はそれらのうちの最小値を考慮します。

関連項目

- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)
- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

最大セッションのグローバル設定

RADIUS および TACACS+ 要求にセッションキーを割り当てることができます。セッションキーには、RADIUS および TACACS+ の一連の属性が提供されます。環境に従ってセッションキーの属性をカスタマイズできます。セッションキーを割り当てない場合、ACS はデフォルトのセッションキー値を使用します。

セッションキーは、ユーザセッションを追跡するために使用される固有のキーです。セッションキーは、同じセッションに再認証するユーザと新しいセッションを開始するユーザとを ACS が区別できるようにします。単一のセッションのセッションキー属性はアクセス要求とアカウンティング開始パケットで同じなる必要があります。セッションキーは、ACS がセッションを適切に特定する役に立ちます。ACS が同じセッションを再認証する場合は、同じキーが保持されます。

最大ユーザセッションのグローバル設定を設定するには、[System Administration] > [Users] > [Max User Session Global Settings] を選択します。

表 10-31 [Max User Session Global Settings] ページ

オプション	説明
RADIUS Session Key Assignment	
Available Session Keys	割り当てに使用可能な RADIUS セッション キー。 (注) RADIUS セッション キーで RADIUS Acct-Session-Id (属性 #44) を使用するには、アクセス要求 Router(config)# radius-server attribute 44 include-in-access-req で送信される Acct-Session-Id を設定する必要があります。
Assigned Session Keys	割り当てられた RADIUS セッション キー。RADIUS のデフォルトのセッション キーは、UserName:NAS-Identifier:NAS-Port:Calling-Station-ID です。
TACACS+ Session Key Assignment	
Available Session Keys	割り当てに使用可能な TACACS+ セッション キー。
Assigned Session Keys	割り当てられている TACACS+ セッション キー。TACACS+ のデフォルトのセッション キーは、User:NAS-Address:Port:Remote-Address です。
Max User Session Timeout Settings	
Unlimited Session Timeout	タイムアウトなし。
Max User Session Timeout	セッション タイムアウトに到達した場合、ACS は各セッションを閉じて、セッション カウントを更新するために疑似停止パケットを送信します。 (注) ユーザはデバイスからのログアウトは強制されません。

関連項目

- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッショングループ設定 \(10-54 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)
- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

ユーザセッションの削除

ユーザが [Logged-in] として示されていますが、AAA クライアントへの接続は失われて、ユーザは実際にはログインしていない場合にのみ、[Purge] オプションを使用できます。

削除しても AAA クライアントからユーザはログオフされませんが、セッション カウントは 1 減ります。カウントがゼロの間、デバイスから届く停止パケットまたは中間アップデートは廃棄されます。別の AAA クライアントに同じユーザ名とパスワードでユーザがログインしている場合に、この削除により、このセッションが影響を受けることはありません。



(注) 疑似アカウンティング停止は、セッション カウント値に関係なく送信されます。

ユーザセッションを削除するには、次の手順を実行します。

- ステップ 1 [System Administration] > [Users] > [Purge User Sessions] に移動します。
[Purge User Session] ページにすべての AAA クライアントのリストが表示されます。

- ステップ 2 ユーザセッションを削除する AAA クライアントを選択します。
- ステップ 3 [Get Logged-in User List] をクリックします。
すべてのログインユーザのリストが表示されます。
- ステップ 4 特定の AAA クライアントにログインしているすべてのユーザセッションを削除するには、[Purge All Sessions] をクリックします。

関連項目

- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッショングループ設定 \(10-54 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

分散環境の最大ユーザセッション

分散環境では、ランタイムによって保持される最大ユーザセッションに関するセッションキャッシュ関連情報を除くすべてのユーザおよび ID グループの設定がセカンダリに複製されます。このため、各サーバのランタイムには独自のセッションによって確立された詳細があります。また、最大セッションカウントは、認証/アカウンティング要求が受信される ACS サーバに基づいて適用されます。

関連項目

- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッショングループ設定 \(10-54 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)
- [プロキシシナリオの最大ユーザセッション \(10-57 ページ\)](#)

プロキシシナリオの最大ユーザセッション

認証要求とアカウンティング要求は同じ ACS サーバに送信する必要があります。そうしないと、最大セッション機能は希望どおりに働きません。

関連項目

- [最大ユーザセッション数 \(10-52 ページ\)](#)
- [最大セッションユーザの設定 \(10-53 ページ\)](#)
- [最大セッショングループ設定 \(10-54 ページ\)](#)
- [最大セッションのグローバル設定 \(10-55 ページ\)](#)
- [ユーザセッションの削除 \(10-56 ページ\)](#)
- [分散環境の最大ユーザセッション \(10-57 ページ\)](#)

ログイン試行失敗の最大回数のポリシー

ACS 5.8 では、n 回連続して試行を失敗した後、管理者はユーザアカウントを無効にできます。ACS の Web インターフェイスからログイン試行失敗の最大回数を設定できます。この機能は内部ユーザにのみ適用されます。この機能はユーザ レベル、ID グループレベル、グローバル レベルで設定できます。ACS 5.8 では、ユーザ レベルと ID グループ レベルで、ログイン試行失敗の最大回数の設定を導入します。グローバル レベルでのログイン試行失敗の最大回数の設定は、すでに ACS で利用できます。



(注) ACS は試行失敗の最大回数に達するまで、もしくはログイン試行が成功するまでカウントを行います。ACS では、ログイン試行失敗回数をカウントする特定の時間範囲（15 分、30 分、1 時間など）は設定されていません。



(注) グループ レベルの試行失敗の最大回数より少ない回数がユーザに設定されている場合、回数が少ないとしても ACS はユーザ レベルの設定を考慮します。

ユーザが誤ったログイン情報を入力すると、ACS は次のログイン試行失敗の最大回数のポリシー アルゴリズムを実行します。

ステップ 1 ログイン試行失敗の最大回数がユーザ レベルで設定されている場合：

- ログイン試行失敗の最大回数に達すると、ACS はユーザ アカウントを無効にします。
- ログイン試行失敗の最大回数に達していない場合、ACS はユーザがクレデンシャルを入力して再度ログインを試行できるようにします。

ログイン試行失敗の最大回数がユーザ レベルで設定されていない場合、ACS は ID グループ レベルでチェックを行います。

ステップ 2 ログイン試行失敗の最大回数がユーザの ID グループ レベルで設定されている場合：

- ログイン試行失敗の最大回数に達すると、ACS はユーザ アカウントを無効にします。
- ログイン試行失敗の最大回数に達していない場合、ACS はユーザがクレデンシャルを入力して再度ログインを試行できるようにします。

ログイン試行失敗の最大回数がユーザが直接関連しているグループ レベルで設定されていない場合、ACS は親 ID グループ レベルでチェックを行います。

ステップ 3 ログイン試行失敗の最大回数が親 ID グループで設定されている場合：

- ログイン試行失敗の最大回数に達すると、ACS はユーザ アカウントを無効にします。
- ログイン試行失敗の最大回数に達していない場合、ACS はユーザがクレデンシャルを入力して再度ログインを試行できるようにします。

ログイン試行失敗の最大回数が親グループで設定されていない場合、ACS は階層グループの root に達するまで順次その階層の次のレベルでチェックを行います。ログイン試行失敗の最大回数が root を含めどのグループにも設定されていない場合、ACS はグローバルレベルのログイン試行失敗の最大回数チェックを行います。

ステップ 4 ログイン試行失敗の最大回数がグローバル レベルで設定されている場合：

- ログイン試行失敗の最大回数に達すると、ACS はユーザ アカウントを無効にします。
- ログイン試行失敗の最大回数に達していない場合、ACS はユーザがクレデンシャルを入力して再度ログインを試行できるようにします。

ログイン試行失敗の最大回数が設定されていない場合、ACS はユーザアカウントを無効にすることがなく、ユーザは何度もログイン クレデンシャルを入力できます。

ここでは、次の内容について説明します。

- ユーザのログイン試行失敗の最大回数を設定する (10-59 ページ)。
- ID グループのログイン試行失敗の最大回数を設定する (10-59 ページ)。
- グローバルにユーザのログイン試行失敗の最大回数を設定する (10-60 ページ)

ユーザのログイン試行失敗の最大回数を設定する

内部ユーザのログイン試行失敗の最大回数を設定するには、次の手順を実行します。

- ステップ 1** [Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。
[Internal Users] ページが表示されます。
- ステップ 2** 次のいずれかの操作を実行します。
 - [Create] をクリックします。
 - ログイン試行失敗の最大回数を設定したいユーザ名をクリックするか、名前の横にあるチェックボックスにチェックを入れて、[Edit] をクリックします。
- ステップ 3** [Disable account after n successive failed attempts] チェックボックスをオンにし、用意されているテキストボックスにログイン試行失敗の最大回数を入力します。
- ステップ 4** [Submit] をクリックします。
選択したユーザのログイン試行失敗の最大回数が設定されます。[Internal Users] ページが新しい設定で表示されます。

ID グループのログイン試行失敗の最大回数を設定する

ID グループのログイン試行失敗の最大回数を設定するには、次の手順を実行します。

- ステップ 1** [Access Policies] > [Max Login Failed Attempts Policy] > [Max Login Failed Attempts Group Settings] を選択します。
設定した ID グループがすべて一覧表示されます。
- ステップ 2** ログイン試行失敗の最大回数を設定したいグループ名の横にあるチェックボックスをオンにします。
- ステップ 3** [Edit] をクリックします。
[Edit Identity Groups] ページが表示され、ID グループ名と説明が示されます。
- ステップ 4** [Disable account after n successive failed attempts] チェックボックスをオンにし、[Max Login Failed Attempts Group Settings] 領域に用意されているテキストボックスに試行失敗の回数を入力します。
- ステップ 5** [Submit] をクリックします。
選択した ID グループのログイン試行失敗の最大回数が設定されます。

グローバルにユーザのログイン試行失敗の最大回数を設定する

グローバルにユーザのログイン試行失敗の最大回数を設定するには、次の手順を実行します。

-
- ステップ 1 [System Administration] > [Users] > [Authentication Settings] を選択します。
[Advanced] タブがある [User Authentication Settings] ページが表示されます。
 - ステップ 2 [Disable account if] チェックボックスをオンにします。
 - ステップ 3 [Failed Attempts Exceed] チェックボックスをオンにして、用意されているテキストボックスにログイン試行失敗の最大回数を入力します。
 - ステップ 4 [Submit] をクリックします。
内部ユーザのログイン試行失敗の最大回数がグローバルに設定されます。
-



(注)

一次と二次のインスタンスの認証ポイントが地理的に異なっている場合、ワイドエリア ネットワークによる分散導入更新は遅くなる可能性があり、その結果として、二次インスタンスから一次インスタンスまで更新の遅れが発生します。この場合で、一次インスタンスと異なる地理的場所に導入されている二次インスタンスに対してあるユーザを認証した場合、「n 回試行を失敗したのちユーザを無効にする」機能は正しく作動しません。
