ユーザおよびIDストアの管理

ここでは、次の内容について説明します。

概要

ACS は、ACS ネットワーク リソース リポジトリおよび ID ストアを使用して、ネットワーク デバイスおよびその他の ACS クライアントを管理します。特定のネットワーク リソースへのアクセスを要求するホストが ACS を介してネットワークに接続すると、ACS はホストを認証し、ホストがネットワーク リソースと通信できるかどうかを決定します。

ユーザまたはホストを認証および認可するために、ACS は ID ストア内のユーザ定義を使用します。ID ストアには、次の 2 つのタイプがあります。

- 内部：ACS がローカルで保持する ID ストア（ローカル ストアとも呼ばれる）は*内部 ID ストア*と呼ばれます。内部 ID ストアの場合、ACS はユーザがユーザ レコードを設定および保持するためのインターフェイスを提供します。
- 外部：ACS の外部に存在する ID ストアは*外部 ID ストア*と呼ばれます。ACS は、これらの外部 ID ストアに接続し、認証を実行してユーザ情報を取得するために、設定情報を必要とします。

ユーザおよびホストを認証する以外に、ほとんどの ID ストアはユーザおよびホストに関連付けられている属性を返します。要求の処理中にポリシー条件でこれらの属性を使用でき、RADIUS 属性について返された値を認可プロファイルに読み込むこともできます。

内部 ID ストア

ACS では、ユーザ レコードおよびホスト レコードを保持するために、さまざまな内部 ID ストアが保持されます。ID ストアごとに、その特定のストアに関連付けられた ID 属性を定義できます。ユーザ レコードまたはホスト レコードの作成中に、このストアに対して値が定義されます。

これらの ID 属性は、ACS アプリケーションの [System Administration] セクションで ID ディクショナリの一部として定義できます（[System Administration] > [Configuration] > [Dictionaries] > [Identity]）。

各内部ユーザ レコードにはパスワードが含まれており、2 番めのパスワードを TACACS+ イネーブル パスワードとして定義できます。内部ユーザ ID ストアに保存されるパスワードは、特定の期間後に失効してユーザに自分のパスワードを定期的に変更させるように設定できます。

ユーザは、自分のパスワードを RADIUS または TACACS+ プロトコルで変更するか、UCP Web サービスを使用できます。パスワードは、ACS で定義するパスワード複雑度基準に準拠している必要があります。

内部ユーザ レコードは、固定および設定可能という 2 つのコンポーネント タイプで構成されます。

固定コンポーネントは次のとおりです。

- 名前
- 説明
- パスワード
- イネーブルまたはディセーブルのステータス
- 電子メール アドレス
- ユーザが所属する ID グループ

設定可能コンポーネントは次のとおりです。

- TACACS+ 認証のイネーブル パスワード
- ユーザ定義の表示および入力方法を決定する ID 属性のセット
- [Disable Account if Date Exceeds]
- [Disable account after *n* successive failed attempts]
- [Enable Password Hash]
- [Password Never Expired/Disabled]

ユーザを作成する前に ID 属性を設定することを推奨します。ID 属性が設定されると、次のことを実行できます。

- ユーザ定義の一部として、対応する値を入力できます。
- ユーザが認証するときに、ポリシー決定で使用できます。
- RADIUS 属性について返された値を認可プロファイルに読み込むために使用できます。

内部ユーザ ID 属性は、ユーザのセッション継続中にユーザに適用されます。

内部 ID ストアには、内部ユーザを認証するために使用される内部ユーザ属性およびクレデンシャル情報が含まれています。

内部ホスト レコードは内部ユーザ レコードに類似していますが、パスワード情報が含まれていません。ホストは MAC アドレスによって識別されます。内部 ID ストアの管理については、内部 ID ストアの管理（8-5 ページ）を参照してください。

外部 ID ストア

外部 ID ストアは外部データベースであり、ACS はこれに基づいて内部ユーザおよび外部ユーザの認証を実行します。ACS 5.8 では、次の外部 ID ストアがサポートされます。

- LDAP
- Active Directory
- RSA SecurID トークン サーバ
- RADIUS ID サーバ

外部 ID ストアのユーザ レコードには、特定のストアにアクセスするために必要な設定パラメータが含まれています。RSA SecurID トークン サーバを除くすべての外部 ID ストアで、ユーザ レコードの属性を定義できます。外部 ID ストアには、ACS サーバ証明書の証明書情報および証明書認証プロファイルも含まれています。

外部 ID ストアの管理方法の詳細については、外部 ID ストアの管理（8-30 ページ）を参照してください。

2 要素認証の ID ストア

RSA SecurID トークン サーバおよび RADIUS ID サーバを使用すると、2 要素認証を実現できます。これらの外部 ID ストアでは、セキュリティを強化する OTP が使用されます。これらの外部 ID ストアに対して、次の追加設定オプションを使用できます。

- ID キャッシング：ACS の ID キャッシングをイネーブルにすると、認証が実行されない場合に、要求の処理中に ID ストアを使用できます。ユーザ認証なしでユーザ ルックアップを実行できる LDAP や AD とは異なり、RSA SecurID トークン サーバと RADIUS ID サーバではユーザ ルックアップはサポートされません。

  たとえば、認証が実行されないために ID ストアでデータを取得できない場合に備えて、認証要求とは別に TACACS+ 要求を認可するため、ユーザに対して正常に行われた最後の認証から取得した結果と属性をキャッシュするように、ID キャッシングをイネーブルにすることができます。このキャッシュを使用して、要求を認可できます。

- 認証拒否の処理：RSA および RADIUS ID ストアでは、認証試行が拒否された場合、次の結果は区別されません。
  - 認証失敗
  - ユーザが見つからない

  この区別は、フェール オープン操作を決定する場合に重要です。設定オプションが使用可能であり、いずれの結果を使用する必要があるかを定義できます。

ID グループ

ID グループは、階層内に定義される論理エンティティであり、ユーザおよびホストに関連付けられます。これらの ID グループは、ポリシー決定を行うために使用されます。内部ユーザおよびホストの場合、ID グループはユーザまたはホスト定義の一部として定義されます。

外部 ID ストアが使用される場合は、外部 ID ストアから取得された属性およびグループを ACS ID グループにマッピングするために、グループ マッピング ポリシーが使用されます。ID グループは、Active Directory のグループと概念は似ていますが、より基本的な性質を持ちます。

証明書ベースの認証

ユーザおよびホストは、証明書ベースのアクセス要求を使用して自身を識別できます。この要求を処理するには、ID ポリシーに証明書認証プロファイルを定義する必要があります。

証明書認証プロファイルには、ユーザまたはホストの識別に使用される証明書の属性が含まれます。また任意で、要求に存在する証明書の検証に使用できる LDAP ID ストアまたは AD ID ストアを含めることもできます。証明書および証明書ベースの認証の詳細については、次の項を参照してください。

- CA 証明書の設定（8-97 ページ）
- 証明書認証プロファイルの設定（8-102 ページ）

ID 順序

要求の処理に複数の ID ストアおよびプロファイルが使用される複雑な条件を設定できます。これらの ID 方式は、ID 順序オブジェクト内に定義できます。順序内の ID 方式のタイプは任意です。

ID 順序は、認証用と属性取得用の 2 つのコンポーネントで構成されます。

- 証明書に基づく認証の実行を選択した場合は、単一の証明書認証プロファイルが使用されます。
- ID データベースに基づく認証の実行を選択した場合は、認証が成功するまで順番にアクセスされる ID データベースのリストを定義できます。認証が成功すると、データベース内の属性が取得されます。

また、追加属性を取得できる任意のデータベースのリストを設定することもできます。これらの追加データベースは、パスワードベースの認証を使用するか証明書ベースの認証を使用するかに関係なく、設定できます。

証明書ベースの認証を実行する場合、ユーザ名は証明書属性から読み込まれ、このユーザ名がリスト内のすべてのデータベースから属性を取得するために使用されます。証明書属性の詳細については、CA 証明書の設定（8-97 ページ）を参照してください。

ユーザについて一致するレコードが見つかると、対応する属性が取得されます。ACS では、アカウントがディセーブルのユーザやパスワードに変更のマークが付いているユーザについても、属性が取得されます。

（注） ディセーブルの内部ユーザ アカウントは、属性のソースとして使用できますが、認証のソースとしては使用できません。

ID 順序の詳細については、ID ストア順序の設定（8-104 ページ）を参照してください。

この章の内容は、次のとおりです。

- 内部 ID ストアの管理（8-5 ページ）
- 外部 ID ストアの管理（8-30 ページ）
- CA 証明書の設定（8-97 ページ）
- 証明書認証プロファイルの設定（8-102 ページ）
- ID ストア順序の設定（8-104 ページ）

内部 ID ストアの管理

ACS には、ユーザ用の内部 ID ストアとホスト用の内部 ID ストアがあります。

- ユーザ用の内部 ID ストアは、ユーザ、ユーザ属性、およびユーザ認証オプションのリポジトリです。
- ホスト用の内部 ID ストアには、MAC Authentication Bypass（ホスト ルックアップ）のホストに関する情報が含まれています。

各ユーザおよびホストを ID ストア内に定義でき、ユーザおよびホストのファイルをインポートできます。

ユーザ用の内部 ID ストアは、展開内のすべての ACS インスタンスで共有され、各ユーザについて次の内容を含んでいます。

- 標準属性
- ユーザ属性
- 認証情報

(注)　ACS 5.8 では、内部 ID ストアに対してだけ、内部ユーザの認証がサポートされます。

ここでは、次の内容について説明します。

認証情報

ユーザの TACACS+ イネーブル パスワードを定義する内部ユーザ レコードの一部として保存される、追加パスワードを設定できます。このパスワードによって、デバイスへのアクセス レベルが設定されます。このオプションを選択しない場合、標準ユーザ パスワードが TACACS イネーブルにも使用されます。

システムが TACACS+ イネーブル操作に使用されていない場合は、このオプションを選択しないでください。

ID ストア順序機能を使用するには、順番にアクセスされる ID ストアのリストを定義します。同じ ID ストアを認証順序リストと属性取得順序リストに含めることができます。ただし、ID ストアが認証用に使用される場合、追加属性を取得するために ID ストアにアクセスされることはありません。

証明書ベースの認証の場合、ユーザ名は証明書属性から読み込まれ、属性取得用に使用されます。

認証プロセス中に、ユーザまたはホストの複数のインスタンスが内部 ID ストアに存在する場合、認証は失敗します。アカウントがディセーブルのユーザやパスワード変更が必要なユーザについて、属性は取得されます（ただし、認証は拒否されます）。

次のような失敗が ID ポリシーの処理中に発生する場合があります。

- 認証失敗。考えられる原因としては、不正なクレデンシャル、ディセーブルなユーザなどがあります。
- ユーザまたはホストが認証データベースに存在しない。
- 定義されているデータベースへのアクセス中に失敗が発生した。

フェール オープン オプションを定義して、これらの失敗が発生したときに実行するアクションを設定できます。

- 拒否：拒否応答を送信します。
- ドロップ：応答を送信しません。
- 続行：サービス内の次の定義済みポリシーへ処理を続行します。

システム属性 *AuthenticationStatus* に、ID ポリシー処理の結果が保持されます。失敗の発生時にポリシー処理を続行することを選択する場合、後続のポリシー処理の条件でこの属性を使用して、ID ポリシー処理が成功しなかった場合を区別できます。

PAP/ASCII、EAP-TLS、または EAP-MD5 で認証が失敗した場合、処理を続行できます。その他のすべての認証プロトコルでは、要求は拒否され、この結果に対するメッセージがロギングされます。

ID グループ

各内部ユーザを 1 つの ID グループに割り当てることができます。ID グループは、階層構造で定義されます。ユーザに関連付けられる論理エンティティですが、付けられた名前以外のデータや属性は含まれていません。

ポリシー条件で ID グループを使用して、同じポリシー結果が適用されるユーザの論理グループを作成します。内部 ID ストア内の各ユーザを単一の ID グループに関連付けることができます。

ACS でユーザの要求が処理されるときに、そのユーザの ID グループが取得され、規則テーブルの条件で使用可能になります。ID グループは、階層構造になっています。

グループ マッピング ポリシーを使用して、外部 ID ストア内の ID グループおよびユーザを ACS の ID グループにマッピングできます。

ID グループの作成

ID グループを作成するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Groups] を選択します。

[Identity Groups] ページが表示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID 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 ID 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。
- [File Operations] をクリックして、次の操作を実行します。
  - Add：ID グループをインポートから ACS に追加します。
  - Update：ACS 内の既存の ID グループを、インポートのリストで上書きします。
  - Delete：インポートにリストされている ID グループを ACS から削除します。
- [Export] をクリックして、ID グループのリストをローカル ハードディスクにエクスポートします。

[File Operations] オプションの詳細については、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（7-8 ページ）を参照してください。

[Create]、[Duplicate]、または [Edit] オプションを選択すると、[Create] ページまたは [Edit] ページが表示されます。

ステップ 3　次のフィールドに情報を入力します。

- Name：ID グループの名前を入力します。ID グループを複製する場合は、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：ID グループの説明を入力します。
- Parent：[Select] をクリックして、ID グループのネットワーク デバイス グループの親を選択します。

ステップ 4　[Submit] をクリックして変更を保存します。

ID グループの設定が保存されます。[Identity Groups] ページが新しい設定で表示されます。新しい ID グループを作成した場合は、このページの階層内で親 ID グループ選択の下に配置されます。

関連項目

- ユーザおよび ID ストアの管理（8-1 ページ）
- 内部 ID ストアの管理（8-5 ページ）
- 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（7-8 ページ）
- ID グループ（8-3 ページ）
- ID グループの作成（8-6 ページ）
- ID グループの削除（8-7 ページ）

ID グループの削除

ID 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　[Users and Identity Stores] > [Identity Groups] を選択します。

[Identity Groups] ページが表示されます。

ステップ 2　削除する ID 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。

```
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。

[Identity Groups] ページが表示されます。このとき、削除した ID グループは表示されません。

関連項目

- ID 属性の管理（8-8 ページ）

ID 属性の管理

管理者は、ポリシー条件の要素となる ID 属性のセットを定義できます。ACS 5.8 ポリシー モデルについては、ACS 5.x ポリシー モデル（3-1 ページ）を参照してください。認証時に、ID 属性がポリシー条件の一部である場合に内部データ ストアから取得されます。

ACS 5.8 は ID 要素と連携動作して、ユーザを認証し、ACS ポリシーへの入力のために属性を取得します。

属性定義には、関連付けられたデータ型および有効な値が含まれています。値のセットは、型によって異なります。たとえば、型が *integer* の場合、定義には有効な範囲が含まれます。ACS 5.8 には、属性値がない場合に使用できるデフォルト値の定義があります。デフォルト値により、すべての属性は少なくとも 1 つの値を持ちます。

関連項目

- 標準属性（8-8 ページ）
- ユーザ属性（8-9 ページ）
- ホスト属性（8-10 ページ）

標準属性

表 8-1 に、内部ユーザ レコードの標準属性を示します。

表 8-1　　標準属性

属性	説明
Username	ACS は、認証要求のユーザ名に対してこのユーザ名を比較します。比較では大文字と小文字は区別されません。
Status	• イネーブル ステータスは、アカウントがアクティブであることを示します。 • ディセーブル ステータスは、ユーザ名の認証が失敗することを示します。
Description	属性のテキスト説明。
Identity Group	ACS は各ユーザを ID グループに関連付けます。詳細については、ID 属性の管理（8-8 ページ）を参照してください。

ユーザ属性

管理者は、ID 属性のセットからユーザ定義の属性を作成および追加できます。内部 ID ストア内のユーザごとにこれらの属性のデフォルト値を割り当て、デフォルト値が必須か任意かを定義できます。

ACS でユーザを定義する必要があります。各内部ユーザと ID グループとの関連付け、説明（任意）、パスワード、イネーブル パスワード（任意）、内部および外部ユーザ属性などです。

内部ユーザは、固定および設定可能という 2 つのコンポーネントで定義されます。固定コンポーネントは、次の属性で構成されます。

- 名前
- 説明
- パスワード
- イネーブルまたはディセーブルのステータス
- 所属する ID グループ

設定可能コンポーネントは、次の属性で構成されます。

- TACACS+ 認証のイネーブル パスワード
- ユーザ定義の表示および入力方法を決定する ID 属性のセット

ユーザを作成する前に ID 属性を設定することを推奨します。ID 属性が設定されると、次のことを実行できます。

- ユーザ定義の一部として、対応する値を入力できます。
- ユーザが認証するときに、ポリシー決定で使用できます。

内部ユーザ ID 属性は、ユーザのセッション継続中にユーザに適用されます。

内部 ID ストアには、（ポリシーで定義したように）内部ユーザを認証するために使用される内部ユーザ属性およびクレデンシャル情報が含まれています。

外部 ID ストアは外部データベースであり、これに基づいて（ポリシーで定義したように）内部ユーザおよび外部ユーザのクレデンシャルおよび認証の確認を実行します。

ACS 5.8 では、自分のポリシー内で使用する ID 属性を次の順序で設定できます。

ステップ 1　（ユーザ ディクショナリを使用して）ID 属性を定義します。

ステップ 2　ポリシーで使用するカスタム条件を定義します。

ステップ 3　内部データベースの各ユーザの値を読み込みます。

ステップ 4　この条件に基づいて規則を定義します。

ACS 5.8 およびユーザの ID 属性について理解が深まると、ポリシー自体はより堅牢で複雑になっていきます。

ユーザ定義の属性値を使用して、ポリシーおよび認可プロファイルを管理できます。ユーザ属性の作成方法については、内部ユーザ ID 属性の作成、複製、および編集（18-13 ページ）を参照してください。

ホスト属性

内部ホスト用の追加属性を設定できます。内部ホストを作成するときに、次のことを実行できます。

- ホスト属性の作成
- ホスト属性へのデフォルト値の割り当て
- デフォルト値が必須か任意かの定義

これらのホスト属性に対して値を入力でき、その値を使用してポリシーおよび認可プロファイルを管理できます。ホスト属性の作成方法については、内部ホスト ID 属性の作成、複製、および編集（18-16 ページ）を参照してください。

ユーザの認証の設定

ACS でユーザ アカウントの認証設定を設定して、ユーザに強力なパスワードの使用を強制できます。[Authentication Settings] ページで行うパスワード ポリシー変更は、すべての内部 ID ストア ユーザ アカウントに適用されます。[User Authentication Settings] ページには、次のタブがあります。

- Password complexity
- Advanced

パスワード 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　[System Administration] > [Users] > [Authentication Settings] を選択します。

[Password Complexity] タブおよび [Advanced] タブがある [User Authentication Settings] ページが表示されます。

ステップ 2　[Password Complexity] タブで、ユーザ パスワードの設定に使用する各チェックボックスをオンにします。

表 8-2 に、[Password Complexity] タブのフィールドを示します。

表 8-2　[Password Complexity] タブ

オプション	説明
Applies to all ACS internal identity store user accounts	
Minimum length	必要な最小長。有効なオプションは 4 ～ 32 です。
Password may not contain the username	パスワードにユーザ名またはユーザ名を逆にしたものを使用できるかどうか。
Password may not contain ‘cisco’	パスワードに *cisco* という単語を使用できないことを指定する場合にオンにします。
Password may not contain	入力した文字列をパスワードに使用しないことを指定する場合にオンにします。
Password may not contain repeated characters four or more times consecutively	パスワードで文字を 4 回以上連続して繰り返すことができないことを指定する場合にオンにします。

表 8-2　[Password Complexity] タブ（続き）

オプション	説明
Change password failed reason message (for TACACS+ only)	現在のパスワードを変更する際に、パスワード ポリシーに一致しないパスワードをユーザが入力したときに表示されるエラー メッセージを入力します。 このオプションは、内部ユーザの TACACS+ 認証にだけ適用されます。このフィールドの最大長は 50 文字です。これらの新しいパスワードが指定した基準に一致しない場合は、このオプションを使用して内部ユーザに適切なエラー メッセージを表示できます。
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	パスワードには、アルファベットの小文字が少なくとも 1 文字含まれている必要があります。
Upper case alphabetic characters	パスワードには、アルファベットの大文字が少なくとも 1 文字含まれている必要があります。
Numeric characters	パスワードには、数字が少なくとも 1 文字含まれている必要があります。
Non-alphanumeric characters	パスワードには、英数字以外の文字が少なくとも 1 文字含まれている必要があります。

ステップ 3　[Advanced] タブで、ユーザ認証プロセスに対して設定する基準の値を入力します。以下の表では、[Advanced] タブのフィールドについて説明します。

表 8-3　[Advanced] タブ

オプション	説明
アカウントの無効化 内部ユーザのアカウントの無効化ポリシーをサポートします。	
Never	アカウントには期限がありません。これがデフォルトのオプションです。このポリシーが理由でディセーブルになっているすべての内部ユーザは、このオプションを選択するとイネーブルになります。
Disable account if Date exceeds	設定した日付を超過すると、内部ユーザがディセーブルになります。たとえば、設定された日付が 2010 年 12 月 28 日である場合、すべての内部ユーザは 2010 年 12 月 28 日の深夜 12 時にディセーブルになります。 日付には、現在のシステム日付または将来の日付を設定できます。現在のシステム日付よりも古い日付は入力できません。 日付超過オプションによってディセーブル化されたすべての内部ユーザは、日付超過オプションの設定を変更するとイネーブルになります。
Disable account if Days exceed	内部ユーザは、設定された日数を超えた場合にディセーブルになります。たとえば、ユーザのアカウントを無効にする日数を 60 日に設定した場合は、その特定のユーザは、アカウントが有効になった時点から 60 日後に無効になります。
Disable account if Failed Attempts Exceed	内部ユーザは、連続した失敗試行の回数が設定された値に達するとディセーブルになります。たとえば、設定された値が 5 の場合、連続した失敗試行回数が 5 に達すると、その内部ユーザはディセーブルになります。

表 8-3　[Advanced] タブ

オプション	説明
Reset current failed attempts count on submit	選択すると、すべての内部ユーザの失敗試行回数が 0 に設定されます。 [Failed Attempts Exceed] オプションによってディセーブルにされたすべての内部ユーザがイネーブルになります。
Disable user account after *n* days of inactivity	ユーザ アカウントはそのユーザがネットワークにログインしていない日数に基づいて無効にする必要があることを指定します。このオプションは内部ユーザにのみ適用できます。日数の範囲は 1 ～ 365 です。
Password History	
Password must be different from the previous *n* versions.	比較対象とするこのユーザの以前のパスワードの数を指定します。以前のパスワードの数にはデフォルトのパスワードも含まれています。このオプションによって、ユーザが以前に使用したパスワードを設定できないようにします。有効なオプションは 1 ～ 99 です。
Password Lifetime	
ユーザに定期的にパスワード変更を求めることができます。	
Disable user account after *n* days if password is not changed for *n* days	パスワードが変更されていない場合、*n* 日後にユーザ アカウントをディセーブルにする必要があることを指定します。有効なオプションは 1 ～ 365 です。このオプションは、MS-CHAPv2 認証の TACACS+ および RADIUS にのみ適用できます。
Expire the password after *n* days if the password is not changed for *n* days	パスワードが変更されていない場合、*n* 日後にユーザ パスワードを期限切れにする必要があることを指定します。有効なオプションは 1 ～ 365 です。このオプションは、MS-CHAPv2 認証の TACACS+ および RADIUS にのみ適用できます。
Display reminder after *n* days	パスワード変更の通知を *n* 日後に表示します。有効なオプションは 1 ～ 365 です。このオプションを設定すると、通知だけが表示されます。新しいパスワードは要求されません。このオプションは、MS-CHAPv2 認証の TACACS+ および RADIUS にのみ適用できます。
Send Email for password expiry before *n* days	内部ユーザのパスワードが期限切れになる前の *n* 番目の日から、ACS でそのユーザに期限日を通知する電子メールの送信が開始されるようにするには、このチェックボックスをオンにし、日数を入力します。このオプションによって、内部ユーザは自分のパスワードが期限切れになるまでに変更できます。 ACS では、[Expire the password after *n* days if the password is not changed for *n* days] オプションまたは [Disable user account after *n* days if password is not changed for *n* days] オプションを設定することなしに、このオプションを設定することはできません。
TACACS Enable Password	
ユーザ レコードに、イネーブル パスワードを保存する別のパスワードを定義する必要があるかどうかを選択します。	
TACACS Enable Password	TACACS+ 認証用の別のパスワードをイネーブルにする場合に、この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。

ユーザ パスワードは、定義した基準を使用して設定されます。これらの基準は、以降のログインだけに適用されます。

(注)　いずれかのユーザがディセーブルになった場合、失敗試行回数の値を複数回再設定する必要があります。このような場合、管理者はそのユーザの現在の失敗試行回数を別個に留意するか、すべてのユーザについて回数を 0 にリセットする必要があります。

非アクティブで *N* 日経過したユーザの無効化

始める前に

- この機能は ACS 内部ユーザにのみ適用できます。
- ACS には、ログ コレクタ サーバから認証成功メッセージが送信されるよう設定する必要があります。
- ログ コレクタ サーバは実行中であり、展開内のすべての ACS ノードから syslog メッセージを受信する必要があります。
- ログ リカバリ機能が有効になっている必要があります。

ACS 5.8 では、管理者により ACS Web インターフェイスから、内部ユーザがネットワークにログインしていなくてもそのユーザのアカウントを有効にしておく最大日数を設定できます。設定された期間を超えると、ユーザがネットワークにログインしていない場合、そのユーザのアカウントは無効化されます。日数の範囲は 1 ～ 365 です。この機能が正しく動作するよう、ログ コレクタ サーバは実行中であり、展開内の ACS ノードから syslog メッセージを受信する必要があります。最終ログイン日はデータベースには格納されていないため、Web インターフェイスでは表示されません。毎日午後 10 時、ACS View によって、アクティブ ユーザのリストをプライマリ管理に提供するジョブが実行されます。アクティブ ユーザとは、設定された期間に認証が 1 回以上成功しているユーザのことです。ユーザが最後にアクティブになった日付は、ACS レポートの Web インターフェイスで、認証成功レポートから確認できます。このリストに基づいて、プライマリ管理は非アクティブなユーザのリストを特定し、そのユーザを無効にして、ログ コレクタ サーバに監査ログ メッセージを送信します。管理者は、無効になったユーザ アカウントを有効にできます。ユーザ アカウントを有効にすると、その後の非アクティブ期間の計算は、最後に有効にされた日付から計算されます。

(注)　ログ コレクタ サーバを変更した場合は、古いログ コレクタ サーバで取ったバックアップを新しいログ コレクタ サーバに復元する必要があります。

(注)　1 つの ACS インスタンスから別の ACS インスタンスに ACS のバックアップを復元する場合は、View のバックアップも、ACS のバックアップに沿って復元する必要があります。

非アクティブで *n* 日経過したユーザ アカウントを無効化するには、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。

[User Authentication Settings] ページが表示されます。

ステップ 2　[Disable user account after n days of inactivity] チェックボックスをオンにします。

ステップ 3　テキスト ボックスに日数を入力します。

ACS では、設定された日数の間アクティブになっていないユーザ アカウントが無効化されます。

内部ユーザの作成

ACS では、セキュリティ上の理由から外部 ID ストアにアクセスしない内部ユーザを作成できます。

一括インポート機能を使用して、数百の内部ユーザを一度に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（7-8 ページ）を参照してください。または、ここで説明する手順に従って、内部ユーザを 1 つずつ作成できます。

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　[Create] をクリックします。次のことも実行できます。

- 複製するユーザ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。
- 変更するユーザ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。
- パスワードを変更するユーザの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。内部ユーザのパスワードは、REST API を使用して変更することもできます。詳細については、「Changing internal user passwords using REST API」を参照してください。

[Change Password] ページが表示されます。

ステップ 3　表 8-4 の説明に従ってフィールドに入力し、内部ユーザのパスワードを変更します。

表 8-4　[Internal User] - [Change Password] ページ

オプション	説明
Password Information	
Password Type	設定されているすべての外部 ID ストア名と、デフォルトのパスワード タイプである [Internal User] が表示されます。リストから 1 個の ID ストアを選択できます。 ユーザ認証の際に、ユーザに外部 ID ストアが設定されている場合、内部 ID ストアは外部 ID ストアに認証要求を転送します。 外部 ID ストアを選択した場合、ユーザのパスワードは設定できません。パスワード編集ボックスはディセーブルです。 パスワード タイプの外部 ID ストアとして ID 順序を使用することはできません。 [Users and Identity Stores] > [Internal Identity Stores] > [Users] ページにある [Change Password] ボタンを使用してパスワード タイプを変更できます。
Password	ユーザの現在のパスワード。[System Administration] > [Users] > [Authentication Settings] で定義したパスワード ポリシーに準拠する必要があります。有効範囲は 4 ～ 32 文字です。
Confirm Password	ユーザのパスワード。[Password] のエントリと正確に一致する必要があります。
Change Password on Next Login	次回のユーザ ログインで、古いパスワードによる認証のあとに、ユーザのパスワードを変更するプロセスを開始する場合に、このボックスをオンにします。

表 8-4　[Internal User] - [Change Password] ページ

オプション	説明
Enable Password Information	
Enable Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。4 ～ 128 文字です。このオプションはディセーブルにすることができます。詳細については、「認証情報（8-5 ページ）」を参照してください。
Confirm Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。[Enable Password] のエントリと正確に一致する必要があります。

- [File Operations] をクリックして、次の操作を実行します。
  - Add：内部ユーザをインポートから ACS に追加します。
  - Update：ACS 内の既存の内部ユーザをインポートのユーザのリストで上書きします。
  - Delete：インポートにリストされている内部ユーザを ACS から削除します。
- [Export] をクリックして、内部ユーザのリストをローカル ハードディスクにエクスポートします。

[File Operations] オプションの詳細については、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（7-8 ページ）を参照してください。

[Create]、[Duplicate]、または [Edit] オプションを選択すると、[User Properties] ページが表示されます。[Edit] ビューで、ユーザの最初の作成および最終変更の情報を参照できます。この情報は編集できません。

ステップ 4　表 8-5 の説明に従って、フィールドに入力します。

表 8-5　[Users and Identity Stores] > [Internal Identity Store] > [User Properties] ページ

オプション	説明
General	
Name	ユーザ名。
Status	ドロップダウン リスト ボックスを使用して、ユーザのステータスを選択します。 • Enabled：このユーザの認証要求は許可されます。 • Disabled：このユーザの認証要求は失敗します。
Description	（任意）ユーザの説明。
Identity Group	[Select] をクリックして、[Identity Groups] ウィンドウを表示します。ID グループを選択して [OK] をクリックし、特定の ID グループを使用してユーザを設定します。
Email Address	内部ユーザの電子メール アドレスを入力します。ACS View によって、この電子メール アドレスに警告が送信されます。ACS はこの電子メール アドレスを使用して、内部ユーザのパスワードが期限切れになる *n* 日前に、パスワード有効期限をそのユーザに通知します。
アカウントの無効化	
Disable Account if Date Exceeds	各ユーザに対してアカウントの無効化ポリシーを使用する場合、このチェックボックスをオンにします。このオプションによって、設定した日付が超過したときに、ユーザ アカウントをディセーブルにすることができます。このオプションは、グローバルなユーザ アカウントの無効化ポリシーを上書きします。すなわち、管理者が必要に応じてユーザごとに異なる有効期限を設定できます。このオプションのデフォルト値は、アカウント作成日から 60 日後です。ユーザ アカウントは、設定された日付の深夜 12 時にディセーブルになります。

表 8-5　[Users and Identity Stores] > [Internal Identity Store] > [User Properties] ページ（続き）

オプション	説明
Disable account after *n* successive failed attempts	各ユーザの試行失敗の回数を設定するには、このチェックボックスをオンにします。失敗の回数を、表示されるテキスト ボックスに入力します。値の範囲は 1 ～ 99 です。ユーザが誤ったログイン クレデンシャルを入力した場合、ACS はこの試行失敗の回数を使用して、そのユーザ アカウントを無効化するか、そのユーザが再試行することを許可するかを決定します。試行失敗が *n* 回に達したら、ACS はそのユーザ アカウントを無効化します。試行失敗の回数をここで設定しない場合、ACS は、試行失敗の回数の設定について、ID グループ レベルでのチェックを試行します。ユーザ レベルでの試行失敗の回数が優先されます。
Password Hash	
Enable Password Hash	Cisco SSL ハッシュ アルゴリズムの PBKDF2 を使用してパスワードのハッシュを有効にし、ユーザ パスワードのセキュリティを強化するには、このチェックボックスをオンにします。このオプションは内部ユーザにのみ適用できます。このオプションを有効にすると、CHAP や MSCHAP などの認証タイプは機能しません。このオプションは、デフォルトで無効です。このオプションを中途で無効にした場合、このオプションを無効にした直後に、パスワード変更オプションを使用して、パスワードを再設定する必要があります。詳細については、内部ユーザに対するパスワード ハッシュの有効化および無効化（8-18 ページ）を参照してください。
Password Lifetime	
Password Never Expired/Disabled	パスワードが期限切れになっているユーザ アカウントをアクティブにするには、[Password Never Expired/Disabled] チェックボックスをオンにします。このオプションは、[System Administration] > [Users] > [Authentication Settings] > [Advanced] ページで設定されているパスワードの有効期間の設定よりも優先されます。
Password Information このページのこのセクションは、内部ユーザを作成した場合にだけ表示されます。 パスワードは最低 4 文字です。	
Password Type	設定されているすべての外部 ID ストア名と、デフォルトのパスワード タイプである [Internal User] が表示されます。リストから 1 個の ID ストアを選択できます。 ユーザ認証の際に、ユーザに外部 ID ストアが設定されている場合、内部 ID ストアは外部 ID ストアに認証要求を転送します。 外部 ID ストアを選択した場合、ユーザのパスワードは設定できません。パスワード編集ボックスはディセーブルです。 パスワード タイプの外部 ID ストアとして ID 順序を使用することはできません。 [Users and Identity Stores] > [Internal Identity Stores] > [Users] ページにある [Change Password] ボタンを使用してパスワード タイプを変更できます。
Password	ユーザのパスワード。[System Administration] > [Users] > [Authentication Settings] で定義したパスワード ポリシーに準拠する必要があります。
Confirm Password	ユーザのパスワード。[Password] のエントリと正確に一致する必要があります。
Change Password on next login	ユーザが次回ログインするときに、古いパスワードの認証後にユーザのパスワードを変更するプロセスを開始する場合に、このボックスをオンにします。
Enable Password Information このページのこのセクションは、内部ユーザを作成した場合にだけ表示されます。 パスワードは 4 ～ 128 文字です。	

表 8-5　[Users and Identity Stores] > [Internal Identity Store] > [User Properties] ページ（続き）

オプション	説明
Enable Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。4 ～ 128 文字です。このオプションはディセーブルにすることができます。詳細については、「認証情報（8-5 ページ）」を参照してください。
Confirm Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。[Enable Password] のエントリと正確に一致する必要があります。
ユーザ情報 定義されている場合、このセクションにはユーザ レコードに対して定義された追加 ID 属性が表示されます。	
ManagementHierarchy	ユーザの階層に割り当てられたアクセス レベル。ユーザがアクセス可能なネットワーク デバイスの階層レベルを入力します。 例： • Location:All:US:NY:MyMgmtCenter1 • Location:All:US:NY:MyMgmtCenter1|US:NY:MyMgmtCenter2 属性タイプは文字列で、最大文字長は 256 です。
Creation/Modification Information このページのこのセクションは、内部ユーザを作成または変更したあとにだけ表示されます。	
Date Created	*表示のみ。*ユーザのアカウントが作成された日付と時刻。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。
Date Modified	*表示のみ。*ユーザのアカウントが最後に変更（更新）された日付と時刻。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。

ステップ 5　[Submit] をクリックします。

ユーザ設定が保存されます。[Internal Users] ページが新しい設定で表示されます。

（注）　[Creating Internal Users] ページの [Password Never Expired/Disabled] オプションは、[System Administration] > [Users] > [Authentication Settings] > [Advanced] ページで設定されているパスワードの有効期間の設定のみを上書きします。このオプションが、日付を超過、日数を超過、試行失敗の回数を超過、またはアカウントが非アクティブで n 日経過したことによるアカウントの無効化設定より優先されることはありません。

関連項目

- ユーザの認証の設定（8-10 ページ）
- 内部 ID ストア ユーザの一括操作の表示および実行（8-21 ページ）
- 内部 ID ストアからのユーザの削除（8-18 ページ）

内部 ID ストアからのユーザの削除

内部 ID ストアからユーザを削除するには、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　削除するユーザ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。

選択した内部ユーザが削除されます。

関連項目

- 内部 ID ストア ユーザの一括操作の表示および実行（8-21 ページ）
- 内部ユーザの作成（8-14 ページ）

内部ユーザに対するパスワード ハッシュの有効化および無効化

ACS 5.8 では、ACS Web インターフェイスの [Creating Internal Users] ページに [Enable Password Hash] オプションを導入することにより、内部ユーザのパスワードのセキュリティを強化します。リリース 5.8 より前の ACS では、ACS の内部ユーザ データベースで、内部ユーザのパスワードをクリア テキストとして保存していました。ACS 管理者は、内部ユーザのパスワードを内部ユーザ データベースで確認できます。それで、内部ユーザのパスワードのセキュリティを強化するために、ACS 5.8 では新機能「Enable Password Hash」を導入しました。このオプションを有効にすると、ユーザのパスワードは、Cisco SSL ハッシュ アルゴリズムの PBKDF2 を使用してハッシュに変換され、内部ユーザ データベースにハッシュで保存されます。この機能は、パスワード ベースの認証にのみ適用できます。そのため、このオプションを有効にすると、MSCHAP 認証と CHAP 認証は使用できません。内部ユーザの作成中にこのオプションを有効にすると、ACS ではこのパスワードをハッシュに変換し、それと同じものを内部ユーザ データベースに保存します。ユーザがそのログイン パスワードを使用してネットワークへのア

クセスを試行すると、ACS ではそのパスワードを、PBKDF2 ハッシュ アルゴリズムを使用してハッシュに変換し、このハッシュ エントリと ACS 内部ユーザのデータベースに格納されているエントリとを比較します。パスワード ハッシュ値がデータベースのハッシュ値に一致すると、ユーザは ACS からネットワークへのログインを許可されます。パスワード ハッシュ値がデータベースのハッシュ値に一致しないと、ACS による認証は失敗し、ユーザはネットワークにログインできません。このオプションを無効にするには、[Enable Password Hash] チェックボックスをオフにします。セキュリティを強化するための PDKDF2 アルゴリズムで使用される反復により、サーバにかかる負荷が高くなると、ACS からの認証応答に遅延が発生することがあります。

ACS で内部ユーザのパスワードのハッシュを有効にするには、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] ページに、使用可能な内部ユーザのリストが表示されます。

ステップ 2　次のいずれかの操作を行います。

- [Create] をクリックします。
- パスワードのハッシュを有効化するユーザ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。

ステップ 3　[Enable Password Hash] 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。

パスワード ハッシュのオプションが、選択した内部ユーザに対して有効化されます。

ACS の内部ユーザのパスワード ハッシュを無効にするには、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] ページに、使用可能な内部ユーザのリストが表示されます。

ステップ 2　パスワードのハッシュを無効化するユーザ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。

ステップ 3　[Enable Password Hash] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックします。

パスワード ハッシュのオプションが、選択した内部ユーザに対して無効化されます。

（注）　[Enable Password Hash] オプションを無効化したら、直ちにユーザ パスワードを変更する必要があります。

ステップ 5　パスワード ハッシュのオプションを無効化したユーザの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。

ステップ 6　[Password] フィールドに新しいパスワードを入力します。

ステップ 7　[Confirm Password] フィールドに新しいパスワードを入力します。

ステップ 8　[Submit] をクリックします。

ユーザおよび管理者へのパスワード期限切れ通知電子メールの設定

はじめる前に

- 電子メールの設定は [Monitoring Configuration] の下で設定する必要があります。電子メールの設定については、電子メール設定の指定（15-17 ページ）を参照してください。

ACS 5.8 では、内部ユーザと管理者に向けて、パスワード期限切れ通知電子メールを設定することができます。内部ユーザと管理者に向けたパスワード期限切れ通知電子メールの送信が必要になるまでの日数は、ACS Web インターフェイスの [Creating Internal Users] ページで設定できます。この機能を設定すると、ACS 5.8 は内部ユーザと管理者に、パスワードが期限切れになる *n* 日前から、電子メールで期限日を通知します。ACS では、管理プロセス再開直後から 5 分経過したら、ユーザおよび管理者のパスワードの期限切れを検証します。続いて、最後に検証された時刻から 24 時間ごとに検証が実行されます。この機能が正しく動作するには、[Email Settings] オプションを [Monitoring Configuration] の下で設定する必要があります。

ユーザに対するパスワード期限切れリマインダの設定

内部ユーザにパスワード期限切れリマインダ メールを送信するには、ACS Web インターフェイスで次のように設定する必要があります。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

[Internal Users] ページに、使用可能な内部ユーザのリストが表示されます。

ステップ 2　次のいずれかの操作を行います。

- [Create] をクリックします。
- パスワード期限切れリマインダを設定するユーザ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。

ステップ 3　[Email Address] テキスト ボックスに、ユーザのメール アドレスを入力します。

ステップ 4　[Submit] をクリックします。

ステップ 5　[System Administration] > [Users] > [Authentication Settings] > [Advanced] を選択します。

ユーザ向けの [Advanced Authentication Settings] ページが表示されます。

ステップ 6　[Send Email for password expiry before n days] チェックボックスをオンにし、日数を入力します。

(注)　パスワードの有効期間が設定されていない場合、[Send Email for password expiry before n days] チェックボックスは無効になっています。

ステップ 7　[Submit] をクリックします。

パスワード期限切れリマインダが設定されました。ユーザは、パスワードが期限切れになる *n* 日前から、電子メールで期限日を受信します。電子メールには次のようなメッセージが記載されています。

```
Dear User,
Your password is going to expire on day, date month year at time UTC.We recommend that
you reset your password immediately to avoid being locked out.
Regards,
CiscoSecureACS Administrator.
```

管理者に対するパスワード期限切れリマインダの設定

内部管理者にパスワード期限切れリマインダ メールを送信するには、ACS Web インターフェイスで次のように設定する必要があります。

ステップ 1　[System Administration] > [Administrators] > [Accounts] を選択します。

[Administrators accounts] ページに、使用可能な内部管理者のリストが表示されます。

ステップ 2　次のいずれかの操作を行います。

- [Create] をクリックします。
- パスワード期限切れリマインダを設定する管理者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。

ステップ 3　[Email Address] テキスト ボックスに、管理者のメール アドレスを入力します。

ステップ 4　[Submit] をクリックします。

ステップ 5　[System Administration] > [Administrators] > [Settings] > [Authentication] > [Advanced] を選択します。

管理者向けの [Advanced Authentication Settings] ページが表示されます。

ステップ 6　[Send Email for password expiry before n days] チェックボックスをオンにし、日数を入力します。

（注）　[Disable administrator account after n days if password was not changed] オプションが設定されていない場合、[Send Email for password expiry before n days] チェックボックスは無効になっています。

ステップ 7　[Submit] をクリックします。

パスワード期限切れリマインダが設定されました。管理者は、パスワードが期限切れになる *n* 日前から、電子メールで期限日を受信します。電子メールには次のようなメッセージが記載されています。

```
Dear Administrator,
Your password is going to expire on day, date month year at time UTC.We recommend that
you reset your password immediately to avoid being locked out.
Regards,
CiscoSecureACS Administrator.
```

関連項目

- 内部 ID ストア ユーザの一括操作の表示および実行（8-21 ページ）
- 内部ユーザの作成（8-14 ページ）

内部 ID ストア ユーザの一括操作の表示および実行

内部 ID ストア ユーザに対する一括操作を表示および実行するには、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、設定されているすべてのユーザについて次の情報が示されます。

- Status：ユーザのステータス

- User Name：ユーザのユーザ名
- Identity Group：ユーザが所属している ID グループ
- Description：（任意）ユーザの説明

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。内部ユーザの作成の詳細については、内部ユーザの作成（8-14 ページ）を参照してください。
- 情報を編集する内部ユーザ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。内部ユーザ編集ページのさまざまなフィールドの詳細については、内部ユーザの作成（8-14 ページ）を参照してください。
- 情報を複製する内部ユーザ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。内部ユーザ複製ページのさまざまなフィールドの詳細については、内部ユーザの作成（8-14 ページ）を参照してください。
- [File Operations] をクリックして、次の一括操作を実行します。
  - Add：内部ユーザをインポート ファイルから ACS に追加するには、このオプションを選択します。
  - Update：ACS の内部ユーザのリストをインポート ファイルの内部ユーザのリストで置換するには、このオプションを選択します。
  - Delete：インポート ファイルにリストされている内部ユーザを ACS から削除するには、このオプションを選択します。

一括操作の詳細については、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（7-8 ページ）を参照してください。

関連項目

- 内部ユーザの作成（8-14 ページ）
- 内部 ID ストア ユーザの一括操作の表示および実行（8-21 ページ）
- 内部 ID ストアからのユーザの削除（8-18 ページ）

ホストの認証の設定

ACS 5.8 では、ホストの認証を設定するため、[System Administration] の下に新しいセクション [Authentication Settings] を導入してします。このセクションを使用すると、ホストの非アクティブ時間に基づいて、ホスト アカウントを無効化したり削除したりできます。

ここでは、次の内容について説明します。

- 非アクティブで N 日および N + x 日経過したホスト アカウントの無効化および削除（8-22 ページ）

非アクティブで *N* 日および *N+x* 日経過したホスト アカウントの無効化および削除

始める前に

- この機能は、MAB 認証要求を送信する内部ホストにのみ適用できます。
- ACS には、ログ コレクタ サーバから認証成功メッセージが送信されるよう設定する必要があります。

- ログ コレクタ サーバは実行中であり、展開内のすべての ACS ノードから syslog メッセージを受信する必要があります。
- ログ リカバリ機能が有効になっている必要があります。

ACS 5.8 では、内部ホストのアカウントが有効である間、そのホストがネットワークにログインしていなくても、管理者により ACS Web インターフェイスから最大日数を設定することができます。設定された期間を超えると、ホストがネットワークにログインしていない場合、そのホストのアカウントは無効化されます。また、管理者は、ホスト アカウントが無効化されてからホストがネットワークにログインしていない場合に ACS がそのホスト アカウントをデータベースから削除するまでの日数も設定できます。

ホスト アカウントを無効にするためのデフォルト値は、30 日の非アクティブ期間です。ホスト アカウントを削除するためのデフォルト値は、そのホスト アカウントが無効化されてから 60 日の非アクティブ期間です。この機能が正しく動作するよう、ログ コレクタ サーバは実行中であり、展開内のすべての ACS ノードから syslog メッセージを受信する必要があります。

ACS は、MAB エントリの最後のログイン日付に基づいて、非アクティブ期間を計算します。毎日午後 10 時、ACS View によって、アクティブな MAB エントリのリストをプライマリ管理に提供するジョブが実行されます。アクティブなホストとは、設定された期間に認証が 1 回以上成功しているホストのことです。ホストが最後にアクティブになった時刻は、ACS レポートの Web インターフェイスで、認証成功レポートから確認できます。このリストに基づいて、プライマリ管理は非アクティブな MAB エントリのリストを特定し、その MAB エントリを無効にして、ログ コレクタ サーバに監査ログ メッセージを送信します。管理者は、無効になったホスト アカウントを有効にできます。ホスト アカウントを有効にすると、その後の非アクティブ期間の計算は、最後に有効にされた日付から計算されます。

(注) ログ コレクタ サーバを変更した場合は、古いログ コレクタ サーバで取ったバックアップを新しいログ コレクタ サーバに復元する必要があります。

(注) 1 つの ACS インスタンスから別の ACS インスタンスに ACS のバックアップを復元する場合は、View のバックアップも、ACS のバックアップに沿って復元する必要があります。

非アクティブで *n* 日経過したホスト アカウントを無効化するには、次の手順を実行します。

ステップ 1　[System Administration] > [Hosts] > [Authentication Settings] を選択します。

[Host Authentication Settings] ページが表示されます。

ステップ 2　[Disable host account after n days of inactivity] チェックボックスをオンにします。

ステップ 3　テキスト ボックスに日数を入力します。

ACS では、設定された日数の間アクティブになっていないホスト アカウントが無効化されます。

無効化されて *n* 日経過したホスト アカウントを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Hosts] > [Authentication Settings] を選択します。

[Host Authentication Settings] ページが表示されます。

ステップ 2　[Delete host account after *n* days of disablement/inactivity] チェックボックスをオンにします。

ステップ 3　テキスト ボックスに日数を入力します。

ACS では、アカウントが無効化されてから設定された日数の間アクティブになっていないホスト アカウントが削除されます。

ID ストアでのホストの作成

MAC アドレスを作成、複製、または編集し、ID グループを内部ホストに割り当てるには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal Hosts] ページが表示され、設定されている内部ホストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する MAC アドレ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 MAC アドレスをクリックします。または、MAC アドレス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。
- [File Operations] をクリックして、一括操作を実行します。インポート プロセスの詳細については、内部 ID ストア ホストの一括操作の表示および実行（8-26 ページ）を参照してください。
- [Export] をクリックして、ホストのリストをローカル ハード ドライブにエクスポートします。

[Create]、[Duplicate]、または [Edit] オプションをクリックすると、[Internal Hosts General] ページが表示されます。

ステップ 3　表 8-6 の説明に従って、[Internal MAC Address Properties] ページのフィールドに入力します。

表 8-6　[Internal Hosts Properties] ページ

オプション	説明
General	
MAC Address	新しいホストを内部 ID ストアに追加するとき、ACS 5.8 ではワイルドカードがサポートされます。有効な MAC アドレスを入力します。次の形式のいずれかを使用します。 • 01-23-45-67-89-AB/01-23-45-* • 01:23:45:67:89:AB/01:23:45:* • 0123.4567.89AB/0123.45* • 0123456789AB/012345* ACS は、上記のいずれかの形式の MAC アドレスを受け入れ、ハイフンで区切られた 6 個の 16 進数に変換して保存します。たとえば、01-23-45-67-89-AB のように変換します。
Status	ドロップダウン リスト ボックスを使用して、MAC アドレスをイネーブルまたはディセーブルにします。
Description	（任意）MAC アドレスの説明を入力します。
Identity Group	MAC アドレスを関連付ける ID グループを入力するか、[Select] をクリックして [Identity Groups] ウィンドウを表示します。MAC アドレスを関連付ける ID グループを選択し、[OK] をクリックします。

表 8-6　[Internal Hosts Properties] ページ（続き）

オプション	説明
MAC Host Information	*表示のみ*。MAC ホストの ID 属性情報が表示されます。
Creation/Modification Information	
このページのこのセクションは、MAC アドレスを作成または変更したあとにだけ表示されます。	
Date Created	*表示のみ*。ホスト アカウントが作成された日付。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。
Date Modified	*表示のみ*。ホスト アカウントが最後に変更（更新）された日付。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。

ステップ 4　[Submit] をクリックして変更を保存します。

MAC アドレスの設定が保存されます。[Internal MAC list] ページが新しい設定で表示されます。

（注） MAC アドレスのワイルドカード（サポートされるフォーマット）を持つホストは 4.x から 5.x. に移行されます。

（注） 組織固有識別子（OUI）クライアントの全範囲を許可する MAC アドレスのワイルドカードを追加できます。
例：シスコの MAC アドレス 00-00-0C-* を追加すると、シスコ デバイスの範囲全体がホストに追加されます。

関連項目

- ホスト ルックアップ（4-14 ページ）
- 内部ホストの削除（8-26 ページ）
- 内部 ID ストア ホストの一括操作の表示および実行（8-26 ページ）
- ポリシーおよび ID 属性（3-17 ページ）
- ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-19 ページ）

内部ホストの削除

MAC アドレスを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal MAC List] ページが表示され、設定されている MAC アドレスが示されます。

ステップ 2　削除する内部ホスト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。

[Internal MAC List] ページが、削除された MAC アドレスなしで表示されます。

関連項目

- ホスト ルックアップ（4-14 ページ）
- 内部 ID ストア ホストの一括操作の表示および実行（8-26 ページ）
- ID ストアでのホストの作成（8-24 ページ）
- ポリシーおよび ID 属性（3-17 ページ）
- ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-19 ページ）

内部 ID ストア ホストの一括操作の表示および実行

内部 ID ストアに対する一括操作を表示および実行するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal Hosts] ページが表示され、設定されている内部ホストが示されます。

ステップ 2　[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：内部ホストをインポート ファイルから ACS に追加するには、このオプションを選択します。
- Update：ACS の内部ホストのリストをインポート ファイルの内部ホストで置換するには、このオプションを選択します。
- Delete：インポート ファイルにリストされている内部ホストを ACS から削除するには、このオプションを選択します。

一括操作の詳細については、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（7-8 ページ）を参照してください。

関連項目

- ホスト ルックアップ（4-14 ページ）
- ID ストアでのホストの作成（8-24 ページ）

- 内部ホストの削除（8-26 ページ）
- ポリシーおよび ID 属性（3-17 ページ）
- ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-19 ページ）

管理階層

管理階層は、組織の管理階層内の下位層のレベルに応じて、内部のユーザまたは内部のホストに管理者がアクセス権を付与できるようにします。組織の管理階層内の特定のデバイスを管理する位置を表す階層ラベルが各デバイスに割り当てられます。

たとえば、階層ラベル *All:US:NY:MyMgmtCenter* は、デバイスが米国のニューヨーク市の MyMgmtcenter にあることを示します。管理者はユーザに、割り当てられている階層のレベルに基づいてアクセス権を付与できます。たとえば、ユーザは *All:US:NY* というレベルが割り当てられている場合は、*All:US:NY* で始まる階層のデバイスを通じてユーザがネットワークにアクセスすると、そのユーザにアクセス権が付与されます。内部ホストについても同様です。

管理階層の属性

管理階層機能を使用するには、管理者が内部ユーザ ディクショナリに次の属性を作成する必要があります:

- ManagementHierarchy 属性：管理者が内部ユーザまたは内部ホストごとに 1 つ以上の階層を定義できるようにします。この属性は文字列で、最大文字長は 256 です。内部ユーザ ID 属性の作成、複製、および編集（18-13 ページ）および内部ホスト ID 属性の作成、複製、および編集（18-16 ページ）を参照してください。
- UserIsInManagementHierarchy 属性または HostIsInManagementHierarchy 属性：ユーザまたはホストに定義されている階層が等しいか、ネットワーク デバイスおよび AAA クライアントに定義されている階層に含まれている場合は、この属性の値を true に設定します。この属性のタイプはブールで、デフォルト値は false です。ACS Web インターフェイスのユーザまたはホストのページには表示されません。この属性は、ID 属性ディクショナリ リストのみで表示できます。内部ユーザ ID 属性の作成、複製、および編集（18-13 ページ）および内部ホスト ID 属性の作成、複製、および編集（18-16 ページ）を参照してください。

管理階層 AAA デバイスの設定

管理センターおよび関連するカスタマー名は、AAA クライアントごとの管理階層内で設定する必要があります。ネットワーク デバイス グループは AAA クライアントの管理階層として使用できます。これに使用されるネットワーク デバイス グループが管理階層属性と呼ばれます。管理者は、管理階層として使用される新しいネットワーク デバイス グループを作成できます。*Location* 階層は管理階層属性の例です。

例：

Location:All Locations:ManagementCenter1:Customer1

管理階層のユーザまたはホストの設定

特定のレベルのアクセスは、各ユーザまたはホストに割り当てられた管理階層の最上位ノードを表すように定義されます。このレベルは、ユーザの「ManagementHierarchy」属性に定義されています。合計値の長さは 256 文字までに制限されています。

管理者は、管理センターまたは AAA クライアントのロケーションを定義するときに階層レベルを設定できます。ManagementHierarchy 属性の構文は次のとおりです。

<HierarchyName>: <HierarchyRoot>:<Value>

例：

- *Location:All Locations:ManagementCenter1*
- *Location:All Locations:ManagementCenter1:Customer 1*

管理者は、管理階層に複数の値を設定できます。複数値属性の構文は次のとおりです。

<HierarchyName>: <HierarchyRoot>:<Value>|<Value>|...

例：

Location:All Locations:ManagementCenter1:Customer1|ManagementCenter1:Customer2

UserIsInManagement 階層属性の設定と使用

UserIsInManagementHierarchy 属性を設定して使用するには、次の手順を実行してます。

ステップ 1　内部ユーザの ManagementHierarchy 属性および UserIsInManagementHierarchy 属性を作成します。内部 ID 属性の設定（18-14 ページ）を参照してください。

ステップ 2　必須階層を持つネットワーク デバイスおよび AAA クライアントのネットワーク デバイス グループを作成します。ネットワーク デバイス グループの作成、複製、および編集（7-2 ページ）を参照してください。

ステップ 3　ネットワーク デバイスおよび AAA クライアントを作成し、ネットワーク デバイス グループに関連付けます。ネットワーク デバイスの作成、複製、および編集（7-11 ページ）を参照してください。

ステップ 4　内部ユーザを作成し、ManagementHierarchy 属性を設定します。内部ユーザの作成（8-14 ページ）を参照してください。

ステップ 5　Choose **Access Policies > Access Services > Default Network Access > Authorization**.

[Authorization] ページが表示されます。

ステップ 6　**[Customize]** をクリックし、複合条件をポリシー条件に追加して **[OK]** をクリックします。

ステップ 7　**[Create]** をクリックして新しいポリシーを作成し、次の手順を実行します。

a. ポリシーの適切な名前を入力し、ステータスを設定します。
b. [Conditions] セクションで、**[Compound Condition]** チェックボックスをオンにします。
c. ディクショナリ ドロップダウン リストから **[Internal users]** を選択します。
d. 使用可能な属性リストから **[UserIsInManagementHierarchy]** 属性を選択します。
e. **[Static value]** を選択し、一致させるルールの条件として **[True]** を入力します。
f. **[Add]** をクリックし、この複合条件をポリシーに追加します。
g. ルールのポリシー結果を選択し、**[OK]** をクリックします。

ネットワーク アクセスの認可ポリシーの作成についての詳細は、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）を参照してください。

ステップ 8　正常に作成されたポリシーは、作成されたポリシーを使用してユーザを認証しようとします。ユーザは、ユーザに定義された階層が等しいか、または AAA クライアント階層に含まれている場合にのみ、認証されます。認証結果を分析するためにログを参照できます。

関連項目

HostIsInManagement 階層属性の設定と使用（8-29 ページ）。

HostIsInManagement 階層属性の設定と使用

HostIsInManagementHierarchy 属性を設定して使用するには、次の手順を実行します。

ステップ 1　内部ホストの ManagementHierarchy および HostIsInManagementHierarchy 属性を作成します。内部 ID 属性の設定（18-14 ページ）を参照してください。

ステップ 2　必須階層を持つネットワーク デバイスおよび AAA クライアントのネットワーク デバイス グループを作成します。ネットワーク デバイス グループの作成、複製、および編集（7-2 ページ）を参照してください。

ステップ 3　ネットワーク デバイスおよび AAA クライアントを作成し、ネットワーク デバイス グループに関連付けます。ネットワーク デバイスの作成、複製、および編集（7-11 ページ）を参照してください。

ステップ 4　内部ホストを作成し、ManagementHierarchy 属性を設定します。内部ユーザの作成（8-14 ページ）を参照してください。

ステップ 5　Choose **Access Policies > Access Services > Default Network Access > Authorization**.

[Authorization] ページが表示されます。

ステップ 6　**[Customize]** をクリックし、複合条件をポリシー条件に追加して **[OK]** をクリックします。

ステップ 7　**[Create]** をクリックして新しいポリシーを作成し、次の手順を実行します。

a. ポリシーの適切な名前を入力し、ステータスを設定します。

b. [Conditions] セクションで、**[Compound Condition]** チェックボックスをオンにします。

c. ディクショナリ ドロップダウン リストから **[Internal hosts]** を選択します。

d. 使用可能な属性のリストから **[HostIsInManagementHierarchy]** 属性を選択します。

e. **[Static value]** を選択し、一致させるルールの条件として **[True]** を入力します。

f. **[Add]** をクリックし、この複合条件をポリシーに追加します。

g. ルールのポリシー結果を選択し、**[OK]** をクリックします。

ネットワーク アクセスの認可ポリシーの作成についての詳細は、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）を参照してください。

ステップ 8　正常に作成されたポリシーは、作成されたポリシーを使用してユーザを認証しようとします。ユーザは、ユーザに定義された階層が等しいか、または AAA クライアント階層に含まれている場合にのみ、認証されます。認証結果を分析するためにログを参照できます。

関連項目

- UserIsInManagement 階層属性の設定と使用（8-28 ページ）。

外部 ID ストアの管理

ACS 5.8 は、数多くの方法で外部 ID システムと統合します。外部認証サービスを利用するか、または外部システムを使用して、必要な属性を取得してプリンシパルを認証することにより、属性を ACS ポリシーに統合できます。

たとえば、ACS は Microsoft AD を利用してプリンシパルを認証できます。また、LDAP バインド操作を使用して、データベース内のプリンシパルを検索して認証することもできます。ACS は、AD グループ所属などの ID 属性を取得して、ACS ポリシー決定を行うことができます。

(注)　ACS 5.8 には、Windows ユーザのダイヤルイン アクセス権属性の組み込みチェックはありません。LDAP または Windows AD を使用して msNPAllowDialin 属性を設定する必要があります。この属性の設定方法については、次の URL で Microsoft 社のマニュアルを参照してください。
http://msdn.microsoft.com/en-us/library/ms678093%28VS.85%29.aspx

ここでは、ACS 5.8 でサポートされている外部 ID ストアの概要と、それらの設定方法について説明します。

ここでは、次の内容について説明します。

LDAP の概要

Lightweight Directory Access Protocol（LDAP）は、TCP/IP および UDP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、x.500 ベースのディレクトリ サーバにアクセスするためのライトウェイト メカニズムです。LDAP は RFC 2251 で定義されています。

ACS 5.8 は、LDAP プロトコルを使用して LDAP 外部データベース（ID ストアとも呼ばれる）と統合します。LDAP ID ストアの設定については、外部 LDAP ID ストアの作成（8-35 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。

- 外部 LDAP ID ストアの作成（8-35 ページ）
- LDAP グループの設定（8-43 ページ）
- LDAP 属性の表示（8-44 ページ）

ディレクトリ サービス

ディレクトリ サービスは、コンピュータ ネットワークのユーザおよびネットワーク リソースに関する情報を保存および編成するためのソフトウェア アプリケーション（アプリケーションのセット）です。ディレクトリ サービスを使用すると、これらのリソースへのユーザ アクセスを管理できます。

LDAP ディレクトリ サービスは、クライアント/サーバ モデルに基づきます。クライアントは、LDAP サーバに接続することで LDAP セッションを開始し、操作要求をサーバに送信します。サーバは、応答を送信します。1 台以上の LDAP サーバに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、ディレクトリを管理します。ディレクトリは、情報を保有するデータベースです。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバ間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバ間で分散できます。各サーバには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり Distinguished Name（DN; 認定者名）があります。この名前には、エントリ内の属性で構成されている Relative Distinguished Name（RDN; 相対識別名）と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

LDAP を使用した認証

ACS 5.8 は、ディレクトリ サーバでバインド操作を実行し、プリンシパルを検索および認証することによって、LDAP ID ストアに対してプリンシパルを認証できます。認証が成功した場合、ACS はプリンシパルに所属するグループおよび属性を取得できます。取得する属性は、ACS Web インターフェイス（LDAP ページ）で設定できます。ACS は、これらのグループおよび属性を使用してプリンシパルを認可できます。

ユーザの認証または LDAP ID ストアの問い合わせを行うために、ACS は LDAP サーバに接続し、接続プールを保持します。LDAP 接続管理（8-32 ページ）を参照してください。

複数の LDAP インスタンス

ACS 5.8 に複数の LDAP インスタンスを作成できます。IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバを使用するか、または同じ LDAP サーバ上の異なるデータベースを使用して認証を行うように、ACS を設定できます。

プライマリ サーバの各 IP アドレスおよびポートの設定は、セカンダリ サーバの IP アドレスおよびポートの設定とともに、ACS LDAP ID ストア インスタンスに対応する LDAP インスタンスを形成します。

ACS 5.8 では、個々の LDAP インスタンスが固有の LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。

この方法は、LDAP データベースにユーザまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザとグループに対してそれぞれ単一のサブツリー ディレクトリだけをサポートするため、ACS が認証要求を送信する必要があるユーザ ディレクトリ サブツリーとグループ ディレクトリ サブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

フェールオーバー

ACS 5.8 では、プライマリ LDAP サーバとセカンダリ LDAP サーバ間でのフェールオーバーがサポートされています。ACS による LDAP 認証のコンテキストでは、ACS が LDAP サーバに接続できないために認証要求が失敗した場合に、フェールオーバーが適用されます。

たとえば、サーバがダウンした場合や ACS がサーバに到達できない場合などです。この機能を使用するには、プライマリとセカンダリの LDAP サーバを定義する必要があり、フェールオーバー設定を行う必要があります。

フェールオーバー設定を行い、ACS が接続しようとする最初の LDAP サーバに到達できない場合には、常に ACS は他の LDAP サーバへの接続を試みます。

ACS が接続を試みる最初のサーバは、プライマリ LDAP サーバであるとはかぎりません。ACS が接続を試みる最初の LDAP サーバは、その前に試みた LDAP 認証と、[Failback Retry Delay] ボックスに入力する値によって決まります。

LDAP 接続管理

ACS 5.8 では、複数の同時 LDAP 接続がサポートされています。接続は、最初の LDAP 認証時にオン デマンドで開かれます。最大接続数は、LDAP サーバごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。

同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバ（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバごとに設定される最大管理接続数によって決まります。

ACS は、ACS で設定されている LDAP サーバごとに、開いている LDAP 接続（バインド情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。

認証プロセスが完了したあと、Connection Manager は Connection Manager への接続を解放します。

バインド接続を使用したユーザの認証

ACS は、バインド要求を送信して、LDAP サーバに対してユーザを認証します。バインド要求には、ユーザの DN およびユーザ パスワードがクリア テキストで含まれています。ユーザの DN およびパスワードが LDAP ディレクトリ内のユーザ名およびパスワードと一致した場合に、ユーザは認証されます。

- 認証エラー：ACS は認証エラーを ACS ログ ファイルにロギングします。
- 初期化エラー：LDAP サーバのタイムアウト設定を使用して、LDAP サーバでの接続または認証が失敗したと判断する前に ACS が LDAP サーバからの応答を待つ秒数を設定します。

  LDAP サーバが初期化エラーを返す理由で考えられるのは、次のとおりです。

  - LDAP がサポートされていない。
  - サーバがダウンしている。

  - サーバがメモリ不足である。
  - ユーザに特権がない。
  - 間違った管理者クレデンシャルが設定されている。
- バインド エラー

  LDAP サーバがバインド（認証）エラーを返す理由で考えられるのは、次のとおりです。
  - フィルタリング エラー：フィルタ基準を使用した検索が失敗する。
  - パラメータ エラー：無効なパラメータが入力された。
  - ユーザ アカウントが制限されている（ディセーブル、ロックアウト、期限切れ、パスワード期限切れなど）。

外部リソース エラーとして次のエラーがロギングされ、LDAP サーバで考えられる問題が示されます。

- 接続エラーが発生した。
- タイムアウトが期限切れになった。
- サーバがダウンしている。
- サーバがメモリ不足である。

未知ユーザ エラーとして次のエラーがロギングされます。

データベースにユーザが存在しない。

無効パスワード エラーとして次のエラーがロギングされます。ユーザは存在しますが、送信されたパスワードが無効です。

無効なパスワードが入力された。

グループ メンバーシップ情報の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の 2 つの方法のいずれかで表します。

- グループがサブジェクトを参照：グループ オブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のようなグループに保存できます。
  - 認定者名（DN）
  - プレーン ユーザ名
- サブジェクトがグループを参照：サブジェクト オブジェクトには、所属するグループを指定する属性が含まれています。

  LDAP ID ストアには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。
- Reference Direction：グループ メンバーシップを決定するときに使用する方法を指定します（Groups to Subjects または Subjects to Groups）。
- Group Map Attribute：グループ メンバーシップ情報を含む属性を示します。
- Group Name Attribute：グループ名情報を含む属性を示します。
- Group Object Class：特定のオブジェクトをグループとして認識することを決定します。
- Group Search Subtree：グループ検索の検索ベースを示します。
- Member Type Option：グループ メンバー属性にメンバーが保存される方法を指定します（DN として、またはプレーン ユーザ名として）。

属性取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ストアのインスタンスごとに、ID ストア ディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 整数 64
- IP アドレス（IP バージョン 4（IPv4）または IP バージョン 6（IPv6）アドレスのいずれかです。）
- Unsigned Integer 32
- ブール

符号なし整数および IP アドレス属性の場合、ACS は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性に対して値が取得されなかった場合、ACS ではデバッグ メッセージをロギングしますが、認証およびルックアップ プロセスは失敗しません。

変換が失敗した場合、または ACS で属性に対して値が取得されなかった場合、ACS が使用できる属性のデフォルト値を任意で設定できます。

証明書取得

ユーザ ルックアップの一部として証明書取得を設定した場合、ACS は証明書属性の値を LDAP から取得する必要があります。これを実行するには、LDAP ID ストアの設定時に、取得する属性のリストに証明書属性を設定しておく必要があります。

LDAP サーバ ID チェック

バックグラウンド

この機能は、Cisco ACS が LDAP サーバに対するユーザ認証または認可を実行した場合にスプーフィング攻撃を防止できます（IPv4）。

LDAP サーバは、攻撃者が本来の LDAP サーバ IP アドレスを使用して不適切な LDAP サーバを確立した場合に（ネットワーク上の別の攻撃者によって行われる可能性もあります）スプーフィングされるおそれがあり、同じ CA によって発行された有効な LDAP サーバ証明書を取得する可能性があります。

ACS は、LDAP サーバの証明書の特定検証を、次に従って実行する必要があります。
RFC 4513—*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*

機能の概要

ACS は、LDAP サーバの証明書から取得したデータ（通常は X.509 SAN セクションにありますが、CN セクションにある場合もあります）と、そのサーバについて ACS 管理者が設定したデータを照合します。この認証チェックが成功すると、LDAP 接続は確立されます。失敗した場合は接続が切断されます。

LDAP サーバの証明書のホスト名データは、次の形式のいずれかです。

- IP アドレス
- DNS
- ワイルドカード文字「*」を使用した DNS

最初の 2 つの形式の場合は、一致は単純です。ワイルドカード文字が検出された場合、ACS は次を確認するため、2 種類の健全性チェックを実行します。

- 再構築されたアドレスが正しい長さであるかどうか。
- 再構築されたアドレスのワイルドカード文字の直後に「.」があるかどうか。

外部 LDAP ID ストアの作成

（注）　ACS 用の LDAP ID ストアを設定しても、LDAP データベースの設定には影響を与えません。ACS は LDAP データベースを認識し、データベースを認証の対象とすることができます。使用している LDAP データベースを管理するには、そのデータベースのマニュアルを参照してください。

LDAP ID ストアを作成すると、ACS によって次のものも作成されます。

- そのストア用の新しいディクショナリ。2 つの属性 ExternalGroups および IdentityDn があります。
- ExternalGroup 属性からのグループ マッピングのカスタム条件。条件名の形式は LDAP:*ID-store-name* ExternalGroups です。

事前定義済みの条件名を編集でき、[Custom condition] ページで IdentityDn 属性からカスタム条件を作成できます。カスタム セッション条件の作成、複製、および編集（9-5 ページ）を参照してください。

外部 LDAP ID ストアを作成、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　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

[LDAP Identity Stores] ページが表示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID ストア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 ID ストア名をクリックします。または、名前の隣にあるボックスをオンにして [Edit] をクリックします。

ID ストアを作成している場合は、ウィザードの最初のページである [General] が表示されます。

ID ストアを複製している場合は、[External Identity Stores] > [Duplicate: "<*idstore*>"] ページの [General] タブが表示されます。*idstore* は、選択した外部 ID ストアの名前です

ID ストアを複製している場合は、[External Identity Stores] > [Edit: "<*idstore*>"] ページの [General] タブが表示されます。*idstore* は、選択した外部 ID ストアの名前です

ステップ 3　必要に応じて、[Name] フィールドおよび [Description] フィールドに入力します。

ステップ 4　パスワードの変更、パスワードの有効期限の検出、およびパスワードのリセットを行うには、[Enable Password Change] チェックボックスをオンにします。

ステップ 5　[Next] をクリックします。

ステップ 6　外部 LDAP サーバ接続の設定（8-36 ページ）に進みます。

（注）　外部 LDAP サーバとして、NAC ゲスト サーバも使用できます。外部 LDAP サーバとして NAC ゲスト サーバを使用する手順については、以下の URL を参照してください。
http://www.cisco.com/c/en/us/td/docs/security/nac/guestserver/configuration_guide/20/nacguestserver/g_guestpol.html

関連項目

- 外部 LDAP ID ストアの削除（8-43 ページ）

外部 LDAP サーバ接続の設定

[LDAP] ページは、外部 LDAP ID ストアを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。ウィザードに従います。
- [Duplicate] をクリックしてから、[Next] をクリックします。[Server Connection] ページが表示されます。
- [**Edit**] をクリックしてから、[**Next**] をクリックします。[Server Connection] ページが表示されます。

表 8-7　[LDAP: Server Connection] ページ

オプション	説明
Server Connection	
Enable Secondary Server	セカンダリ LDAP サーバをイネーブルにする場合にオンにし、プライマリ LDAP サーバに障害が発生した場合のバックアップとして使用します。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。
Always Access Primary Server First	セカンダリ LDAP サーバにアクセスする前にプライマリ LDAP サーバにアクセスする場合にクリックします。
Failback to Primary Server After *min.*Minutes	プライマリ サーバに到達できない場合に ACS がセカンダリ LDAP サーバを使用して認証する時間（分単位）を設定する場合にクリックします。***min.*** は時間（分単位）です。この時間のあと、ACS はプライマリ LDAP サーバを使用した認証を再試行します（デフォルトは 5 です）。
Enable Deployment Configuration	展開設定用のタブをイネーブルにする場合はオンにします。サーバ接続ページのプライマリおよびセカンダリ ホスト名フィールドは展開設定をイネーブルにすると読み取り専用フィールドになります。展開設定ページのプライマリおよびセカンダリ LDAP サーバのホスト名の詳細を設定する必要があります。現在の ACS のホスト名の詳細は、保存後にサーバ接続のページに表示されます。 展開設定ページでプライマリ LDAP サーバのホスト名を設定した後で [Enable Secondary Server] チェックボックスをオンにすると、ポート番号、サーバ タイムアウトおよび最大管理者接続などの必須フィールドがゼロに設定されます。これらのフィールドに適切な値を入力する必要があります。

表 8-7　[LDAP: Server Connection] ページ（続き）

オプション	説明
Primary Server	
Hostname	プライマリ LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
Port	プライマリ LDAP サーバが受信している TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者に問い合わせることによって、ポート番号を取得できます。
Anonymous Access	LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバによって、クライアントが誰かは区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへのクライアント読み取りアクセスが許可されます。 認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。
Authenticated Access	LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。
Admin DN	管理者の認定者名を入力します。つまり、User Directory Subtree 内の必要なすべてのユーザの検索が許可され、グループの検索が許可されている LDAP アカウントです。 指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、LDAP が認証したユーザのグループ マッピングは失敗します。
Password	LDAP 管理者アカウントのパスワードを入力します。
Use Secure Authentication	Secure Sockets Layer（SSL）を使用して ACS とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[Port] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションをイネーブルにした場合は、ルート CA を選択する必要があります。
Check Server Identity	LDAP サーバとの接続を確立している間に ACS がサーバ ID のチェックを実行できるようにする場合は、このチェックボックスをオンします。
Root CA	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証をイネーブルにします。
Server Timeout <*sec.*> Seconds	プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に ACS がプライマリ LDAP サーバからの応答を待つ秒数を入力します。<*sec.*> は秒数です。有効値の範囲は 1 ～ 300 です。（デフォルト = 10）。
Max Admin Connections	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、User Directory Subtree および Group Directory Subtree の下にあるユーザおよびグループのディレクトリの検索に使用されます。有効値の範囲は 1 ～ 99 です。（デフォルト = 8）。
Test Bind To Server	プライマリ LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。

表 8-7　[LDAP: Server Connection] ページ（続き）

オプション	説明
Secondary Server	
Hostname	セカンダリ LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
Port	セカンダリ LDAP サーバが受信している TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP マシン上に DS プロパティを表示することによって、ポート番号を取得できます。
Anonymous Access	LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバによって、クライアントが誰かは区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへのクライアント アクセス（読み取りおよび更新）が許可されます。 認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。
Authenticated Access	LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。
Admin DN	管理者のドメイン名を入力します。つまり、User Directory Subtree 内の必要なすべてのユーザの検索が許可され、グループの検索が許可されている LDAP アカウントです。 指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、LDAP が認証したユーザのグループ マッピングは失敗します。
Password	LDAP 管理者アカウントのパスワードを入力します。
Use Secure Authentication	Secure Sockets Layer（SSL）を使用して ACS とセカンダリ LDAP サーバ間の通信を暗号化する場合にクリックします。[Port] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションをイネーブルにした場合は、ルート CA を選択する必要があります。
Check Server Identity	LDAP サーバとの接続を確立している間に ACS がサーバ ID のチェックを実行できるようにする場合は、このチェックボックスをオンします。
Root CA	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証をイネーブルにします。
Server Timeout <*sec.*> Seconds	セカンダリ LDAP サーバでの接続または認証が失敗したと判断する前に ACS がセカンダリ LDAP サーバからの応答を待つ秒数を入力します。<*sec.*> は秒数です。有効値の範囲は 1 ～ 300 です。（デフォルト = 10）。
Max Admin Connections	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、User Directory Subtree および Group Directory Subtree の下にあるユーザおよびグループのディレクトリの検索に使用されます。有効値の範囲は 1 ～ 99 です。（デフォルト = 8）。
Test Bind To Server	セカンダリ LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。

ステップ 2　[Next] をクリックします。

ステップ 3　外部 LDAP ディレクトリ構成の設定（8-39 ページ）に進みます。

外部 LDAP ディレクトリ構成の設定

このページは、外部 LDAP ID ストアを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。[Directory Organization] ページに到達するまでウィザードに従います。
- [Duplicate]。[Directory Organization] ページが表示されるまで [Next] をクリックします。
- [Edit]。[Directory Organization] ページが表示されるまで [Next] をクリックします。

表 8-8　[LDAP: Directory Organization] ページ

オプション	説明
スキーマ	
Subject Object class	サブジェクトを識別する LDAP *objectClass* 属性の値。多くの場合、サブジェクト レコードの *objectClass* 属性には複数の値があり、サブジェクトに固有のものや、他のオブジェクト タイプと共有されているものがあります。 このボックスには、共有されていない値を入力する必要があります。有効な値は 1 ～ 20 文字であり、有効な LDAP オブジェクト タイプである必要があります。このパラメータには、任意の UTF-8 文字を含めることができます。（デフォルト = Person）。
Group Object class	オブジェクトをグループとして識別する検索で使用するグループ オブジェクト クラスを入力します（デフォルト = GroupOfUniqueNames）。
Subject Name Attribute	サブジェクト名を含むサブジェクト レコード内の属性名。この属性名は、ディレクトリ サーバから取得できます。この属性によって、LDAP スキーマ内のサブジェクト名が指定されます。この属性を使用して、サブジェクト オブジェクトを検索するクエリーを作成します。 詳細については、LDAP データベースに関するドキュメントを参照してください。有効な値は 1 ～ 20 文字であり、有効な LDAP 属性である必要があります。このパラメータには、任意の UTF-8 文字を含めることができます。一般的な値は、*uid* および *CN* です（デフォルト = uid）。
Group Map Attribute	ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の 2 つの方法のいずれかで表します。 • グループがサブジェクトを参照 • サブジェクトがグループを参照 [Group Map Attribute] には、マッピング情報を入力します。 マッピング情報を含む属性（次の条件に従って、サブジェクトまたはグループの属性）を入力する必要があります。 • [Subject Objects Contain Reference To Groups] オプション ボタンを選択した場合は、サブジェクト属性を入力します。 • [Group Objects Contain Reference To Subjects] オプション ボタンを選択した場合は、グループ属性を入力します。

表 8-8　[LDAP: Directory Organization] ページ（続き）

オプション	説明
Group Name Attribute	グループ名を含むグループ レコード内の属性名。この属性名は、ディレクトリ サーバから取得できます。この属性によって、LDAP スキーマ内のグループ名が指定されます。この属性を使用して、グループ オブジェクトを検索するクエリーを作成します。 詳細については、LDAP データベースに関するドキュメントを参照してください。一般的な値は DN および *CN* です。（デフォルト = DN）。
Certificate Attribute	証明書定義を含む属性を入力します。証明書認証プロファイルの一部として定義されたときに、これらの定義を任意で使用して、クライアントによって提示された証明書を確認できます。その場合、クライアント証明書と LDAP ID ストアから取得された証明書の間でバイナリ比較が実行されます。
Subject Objects Contain Reference To Groups	サブジェクト オブジェクトにグループの参照が含まれる場合にクリックします。
Group Objects Contain Reference To Subjects	グループ オブジェクトにサブジェクトの参照が含まれる場合にクリックします。
Subjects In Groups Are Stored In Member Attribute As	ドロップダウン リスト ボックスを使用して、グループ内のサブジェクトがメンバー属性に次のうちのいずれとして保存されるかを指定します。 • Username • Distinguished name
ディレクトリ構造	

Subject Search Base	すべてのサブジェクトを含むサブツリーの認定者名（DN）を入力します。次に例を示します。
	`o=corporation.com`
	サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて
	`o=corporation.com`
	または
	`dc=corporation,dc=com`
	と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

Group Search Base	すべてのグループを含むサブツリーの認定者名（DN）を入力します。次に例を示します。
	`ou=organizational unit[,ou=next organizational unit]o=corporation.com`
	グループを含むツリーがベース DN である場合は、LDAP 設定に応じて
	`o=corporation.com`
	または
	`dc=corporation,dc=com`
	と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

Test Configuration	設定の結果として生ずる可能性があるユーザおよびグループの数をカウントすることによって、予期される接続およびスキーマの結果を取得する場合にクリックします。
Username Prefix\Suffix Stripping	

表 8-8　[LDAP: Directory Organization] ページ（続き）

オプション	説明
Strip start of subject name up to the last occurrence of the separator	ユーザ名からドメイン プレフィックスを削除するために適切なテキストを入力します。 ユーザ名の中で、[*start_string*] ボックスに指定した区切り文字が検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。 ユーザ名に、[*start_string*] ボックスに指定した文字が複数含まれている場合は、最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\echamberlain である場合、echamberlain が LDAP サーバに送信されます。 [*start_string*] ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。ACS では、ユーザ名にこれらの文字を使用できません。X ボックスにこれらの文字のいずれかを入力すると、ストリッピングが失敗します。
Strip end of subject name from the first occurrence of the separator	ユーザ名からドメイン サフィックスを削除するために適切なテキストを入力します。 ユーザ名の中で、Y ボックスに指定した区切り文字が検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。 ユーザ名に、Y ボックスに指定した文字が複数含まれる場合は、最初の区切り文字から文字が削除されます。たとえば、区切り文字がアットマーク（@）で、ユーザ名が *jwiedman@domain* である場合、*jwiedman* が LDAP サーバに送信されます。 [*end_string*] ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。ACS では、ユーザ名にこれらの文字を使用できません。[*end_string*] ボックスにこれらの文字のいずれかを入力すると、ストリッピングが失敗します。
MAC Address Format	
Search for MAC Address in Format <*format*>	内部 ID ストアの MAC アドレスは、xx-xx-xx-xx-xx-xx 形式で保存されます。LDAP データベースの MAC アドレスは、別の形式で保存できます。ただし、ACS でホストルックアップ要求が受信されると、MAC アドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リスト ボックスを使用して、特定の形式での MAC アドレスの検索をイネーブルにします。<*format*> は次のいずれかです。 • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx • xxxx.xxxx.xxxx 選択する形式は、LDAP サーバに保存されている MAC アドレスの形式と一致している必要があります。

ステップ 2　[Next] をクリックします。

展開設定での LDAP ホスト名の設定（8-42 ページ）に進みます。

関連項目

- LDAP グループの設定（8-43 ページ）
- 外部 LDAP ID ストアの削除（8-43 ページ）

展開設定での LDAP ホスト名の設定

ACS 5.8 は、展開時のさまざまな ACS インスタンスに対する異なる LDAP ホスト名の設定をサポートします。展開時にすべての ACS インスタンスを単一の LDAP サーバに通信するように設定すると、その LDAP サーバのパフォーマンスに影響が及ぶ可能性があります。また、LDAP サーバをさまざまな場所に配置している場合、地理的に近い場所に配置された LDAP サーバで ACS インスタンスを設定できます。このタイプの設定を行うと、応答時間が向上します。したがって、負荷を管理し、パフォーマンス レベルを向上させるには、さまざまなインスタンスがさまざまな LDAP サーバと通信するような方法で（できれば、LDAP サーバを地理的にローカルな場所に配置して）設定します。

ACS は、それぞれの ACS インスタンスに異なる LDAP サーバのホスト名を設定する [Deployment Configuration] という新しいタブを導入します。[Deployment Configuration] ページの設定を保存すると、LDAP サーバのホスト名が [Server Connection] ページに自動的に入力されます。この設定は、展開時にプライマリ ACS インスタンスのみから実行できます。セカンダリ ACS インスタンスからは LDAP 設定の情報のみを表示できます。

展開時に [LDAP Deployment Configurations] をイネーブルにした場合、要求が ACS インスタンスのいずれかに着信すると、その ACS インスタンスが設定されたプライマリ LDAP サーバを検索します。設定済みの LDAP サーバを検出した後、その LDAP サーバと通信して必要な詳細を取得します。

はじめる前に

[Server Connection] ページの **[Enable Deployment Configuration]** チェックボックスをオンにします。[Deployment Configuration] チェックボックスをオンにすると、プライマリおよびセカンダリ LDAP サーバのホスト名フィールドが読み取り専用フィールドになります。

展開時にこのページを使用して、さまざまな ACS インスタンスのプライマリおよびセカンダリ LDAP ホスト名を設定します。

ステップ 1　**[Users and Identity Stores] > [External Identity Stores] > [LDAP]** を選択し、次のいずれかをクリックします。

- [Create]。[Directory Configuration] ページに到達するまでウィザードに従います。
- **[Duplicate]** をクリックし、[Deployment Configuration] ページが表示されるまで **[Next]** をクリックします。
- **[Edit]** をクリックし、[Deployment Configuration] ページが表示されるまで **[Next]** をクリックします。

（注）　[Enable Deployment Configuration] チェックボックスをオンにして、[Deployment Configuration] タブでの操作ができるようにします。[Deployment Configuration] チェックボックスがオンになっていない場合でも、[Deployment Configuration] タブを表示できます。この[Enable Deployment Configuration] チェックボックスをオンにしていない場合、展開時に ACS インスタンスにプライマリおよびセカンダリ LDAP サーバに異なるホスト名を設定できません。

[Deployment Configuration] ページが表示され、展開でアクティブな ACS インスタンスの現在のリストが表示されます。

ステップ 2　ACS インスタンス名の近く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。

LDAP ホスト名の設定ダイアログボックスが表示されます。

このダイアログ ボックスには以下の 2 つのフィールドが含まれています。

- **Primary Hostname**：選択した ACS インスタンスが指定したプライマリ LDAP サーバと通信するように、プライマリ LDAP サーバのホスト名を入力します。
- **Secondary Hostname**：プライマリ LDAP サーバがダウンした場合に選択した ACS インスタンスが指定した LDAP サーバと通信するように、セカンダリ サーバのホスト名を入力します。

ステップ 3　[OK] をクリックします。

LDAP サーバ名の設定が保存されます。

ステップ 4　[Finish] をクリックします。

作成した外部 ID ストアが保存されます。

関連項目

- 外部 LDAP ID ストアの作成（8-35 ページ）
- 外部 LDAP ID ストアの削除（8-43 ページ）

外部 LDAP ID ストアの削除

1 つ以上の外部 LDAP ID ストアを同時に削除できます。

外部 LDAP ID ストアを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

[LDAP Identity Stores] ページが表示され、設定されている外部 ID ストアのリストが示されます。

ステップ 2　削除する外部 ID ストア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。

次のエラー 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。

[External Identity Stores] ページが表示されます。このとき、削除した ID ストアはリストに含まれません。

関連項目

- 外部 LDAP ID ストアの作成（8-35 ページ）

LDAP グループの設定

このページは、外部 LDAP グループを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。ウィザードに従います。
- [Duplicate]。次に [Directory Groups] タブをクリックします。

- [Edit]。次に [Directory Groups] タブをクリックします。

[Selected Directory Groups] フィールドに、規則テーブル グループ マッピング条件でオプションとして使用できるグループのリストが表示されます。

ステップ 2　次のいずれかを実行します。

- [Select] をクリックして、[Groups] セカンダリ ウィンドウを開きます。このウィンドウからグループを選択して [Selected Directory Groups] リストに追加できます。
- または、[Group Name] フィールドに LDAP グループを入力して [Add] をクリックすることもできます。

選択したグループを [Selected Directory Groups] リストから削除するには、そのグループを [Selected Directory Groups] リストで選択して [Deselect] をクリックします。

ステップ 3　[Submit] をクリックして変更を保存します。

LDAP 属性の表示

このページは、外部 LDAP 属性を表示する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

ステップ 2　属性を表示する LDAP ID ストアの隣にあるチェックボックスをオンにし、[Edit] をクリックして、[Directory Attributes] タブをクリックします。

ステップ 3　[Name of example Subject to Select Attributes] フィールドに、属性を取得するオブジェクト例の名前を入力し、[Select] をクリックします。

たとえば、オブジェクトをユーザにして、オブジェクト名をユーザ名またはユーザの DN にすることができます。

ステップ 4　表 8-9 の説明に従って、フィールドに入力します。

表 8-9　[LDAP: Attributes] ページ

オプション	説明
Attribute Name	ポリシー条件で使用可能な属性のリストに含める属性名を入力します。
Type	[Attribute Name] フィールドに入力した属性名に関連付けるタイプを選択します。
Default	[Attribute Name] フィールドに入力した属性名に関連付けるデフォルト値を指定します。デフォルト値を指定しない場合、デフォルトは使用されません。 [Select] ボタンによって [Attribute Name/Type/Default] ボックスに属性がインポートされた場合は、これらのデフォルト値が使用されます。 • String：属性名 • 整数 64 • IP アドレス：IP バージョン 4（IPv4）または IP バージョン 6（IPv6）アドレスを指定できます。 • Unsigned Integer 32 • ブール
Policy Condition Name	（*任意*）この属性のカスタム条件の名前を指定します。この条件は、ポリシーの条件をカスタマイズするときに選択できます。

ステップ 5　[Add] をクリックすると、入力した情報が画面上のフィールドに追加されます。

ここに表示される属性をポリシー条件で使用できます。

ステップ 6　[Submit] をクリックして変更を保存します。

LDAP 展開の設定

このページは、外部 LDAP 属性を表示する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

ステップ 2　属性を表示する LDAP ID ストアの隣にあるチェックボックスをオンにし、[Edit] をクリックして、[Directory Attributes] タブをクリックします。

ステップ 3　[Name of example Subject to Select Attributes] フィールドに、属性を取得するオブジェクト例の名前を入力し、[Select] をクリックします。

たとえば、オブジェクトをユーザにして、オブジェクト名をユーザ名またはユーザの DN にすることができます。

ステップ 4　表 8-9 の説明に従って、フィールドに入力します。

表 8-10　　LDAP : [Attributes] ページ

オプション	説明
Attribute Name	ポリシー条件で使用可能な属性のリストに含める属性名を入力します。
Type	[Attribute Name] フィールドに入力した属性名に関連付けるタイプを選択します。
Default	[Attribute Name] フィールドに入力した属性名に関連付けるデフォルト値を指定します。デフォルト値を指定しない場合、デフォルトは使用されません。 [Select] ボタンによって [Attribute Name/Type/Default] ボックスに属性がインポートされた場合は、これらのデフォルト値が使用されます。 • String：属性名 • 整数 64 • IP アドレス：IP バージョン 4（IPv4）または IP バージョン 6（IPv6）アドレスを指定できます。 • Unsigned Integer 32 • ブール
Policy Condition Name	（*任意*）この属性のカスタム条件の名前を指定します。この条件は、ポリシーの条件をカスタマイズするときに選択できます。

ステップ 5　[Add] をクリックすると、入力した情報が画面上のフィールドに追加されます。

ここに表示される属性をポリシー条件で使用できます。

ステップ 6　[Submit] をクリックして変更を保存します。

外部 MAB データベースとしての Cisco NAC Profiler の利用

ACS は、Cisco NAC Profiler と通信して、802.1X 非対応デバイスが 802.1X 対応ネットワークで認証できるようにします。802.1X を使用して認証できないエンドポイントは、スイッチで MAC 認証バイパス（MAB）機能を使用して、802.1X 対応ネットワークに接続します。

一般的に、プリンタ、ファクス装置、IP 電話、無停電電源（UPS）などの非ユーザ接続デバイスには、802.1x サプリカントは装備されていません。

つまり、これらのデバイスが接続するスイッチ ポートは、デバイスまたはユーザ クレデンシャルの 802.1X 交換を使用してデバイスを認証できず、デバイスがネットワークに接続するには、スイッチ ポートはポートベースの認証以外の認証メカニズム（一般的に、エンドポイント MAC アドレスベース）に戻る必要があります。

Cisco NAC Profiler は、これらのシステムの認証コンポーネントと連携動作できないエンドポイントを識別して特定するためのソリューションを提供します。その結果、これらのエンドポイントにネットワークへのアドミッションのための代替メカニズムを提供できます。

NAC Profiler は、LDAP 対応ディレクトリで構成されます。このディレクトリは、MAC 認証バイパス（MAB）に使用できます。したがって、NAC Profiler は ACS の外部 LDAP データベースとして機能して、802.1X 非対応デバイスを認証します。

（注）　ACS 内部ホスト データベースを使用すると、802.1X 非対応デバイスの MAC アドレスを定義できます。ただし、NAC Profiler がすでにネットワーク内にある場合は、それを外部 MAB データベースとして使用できます。

Cisco NAC Profiler を外部 MAB データベースとして利用するには、次のことを実行する必要があります。

- Cisco NAC Profiler で LDAP インターフェイスをイネーブルにします。Cisco NAC Profiler での LDAP インターフェイスのイネーブル化による ACS との通信（8-46 ページ）を参照してください。
- ACS で NAC Profiler を設定します。ID ポリシーで使用するための ACS での NAC Profiler LDAP 定義の設定（8-48 ページ）を参照してください。

Cisco NAC Profiler での LDAP インターフェイスのイネーブル化による ACS との通信

（注）　NAC Profiler で LDAP インターフェイスをイネーブルにする前に、NAC Profiler Collector で NAC Profiler を設定しておきます。Cisco NAC Profiler 設定の詳細については、次の Web サイトで『*Cisco NAC Profiler Installation and Configuration Guide*』を参照してください。
http://www.cisco.com/c/en/us/support/security/nac-profiler/products-installation-and-configuration-guides-list.html

NAC Profiler で LDAP インターフェイスをイネーブルにして ACS と通信するには、次の手順を実行します。

ステップ 1　Cisco NAC Profiler にログインします。

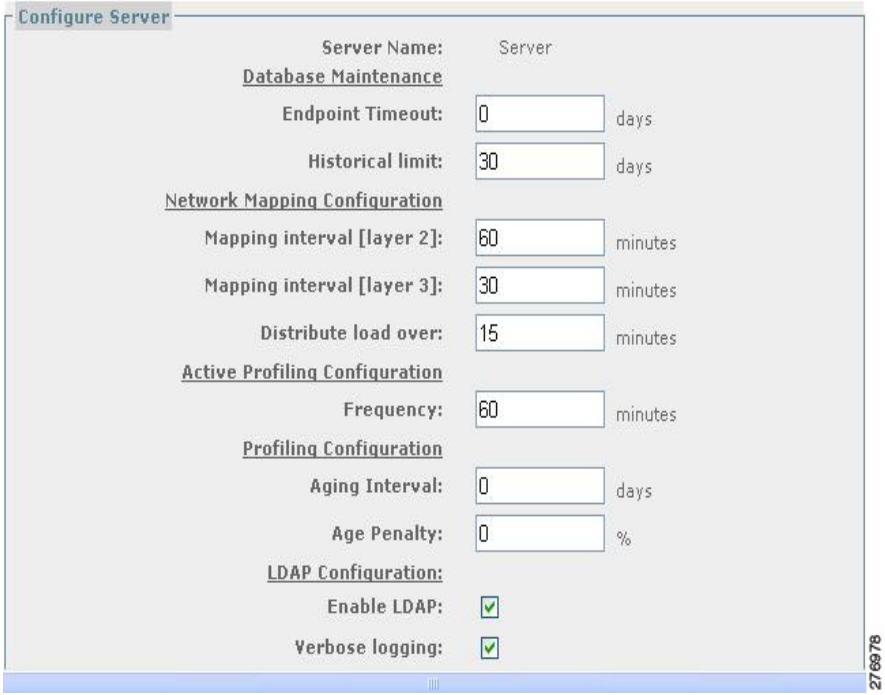
ステップ 2　[Configuration] > [NAC Profiler Modules] > [List NAC Profiler Modules] を選択します。

ステップ 3　[Server] をクリックします。

[Configure Server] ページが表示されます。

ステップ 4　[LDAP Configuration] 領域で、図 8-1 に示すように [Enable LDAP] チェックボックスをオンにします。

図 8-1　NAC Profiler での LDAP インターフェイス設定



ステップ 5　[Update Server] をクリックします。

ステップ 6　[Configuration] タブをクリックし、[Apply Changes] をクリックします。

[Update NAC Profiler Modules] ページが表示されます。

ステップ 7　[Update Modules] をクリックして、ACS で LDAP を使用できるようにします。

Cisco NAC Profiler に対して認証するエンドポイント プロファイルをイネーブルにする必要があります。その実行方法については、LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定（8-47 ページ）を参照してください。

適切なアクティブ応答イベントを確保するため、Cisco NAC Profiler UI からアクティブ応答遅延時間を設定する必要があります。これには、[Configuration] > [NAC Profiler Modules] > [Configure Server] > [Advanced Options] > [Active Response Delay] を選択します。

LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定

認証する非 802.1X エンドポイントについて、LDAP 認証に対して NAC Profiler で対応するエンドポイント プロファイルをイネーブルにする必要があります。

（注）　プロファイルが LDAP に対してイネーブルになっていない場合、Cisco NAC Profiler によるプロファイルのエンドポイントの認証は行われません。

LDAP 認証に対してエンドポイント プロファイルをイネーブルにするには、次の手順を実行します。

ステップ 1　NAC Profiler にログインします。

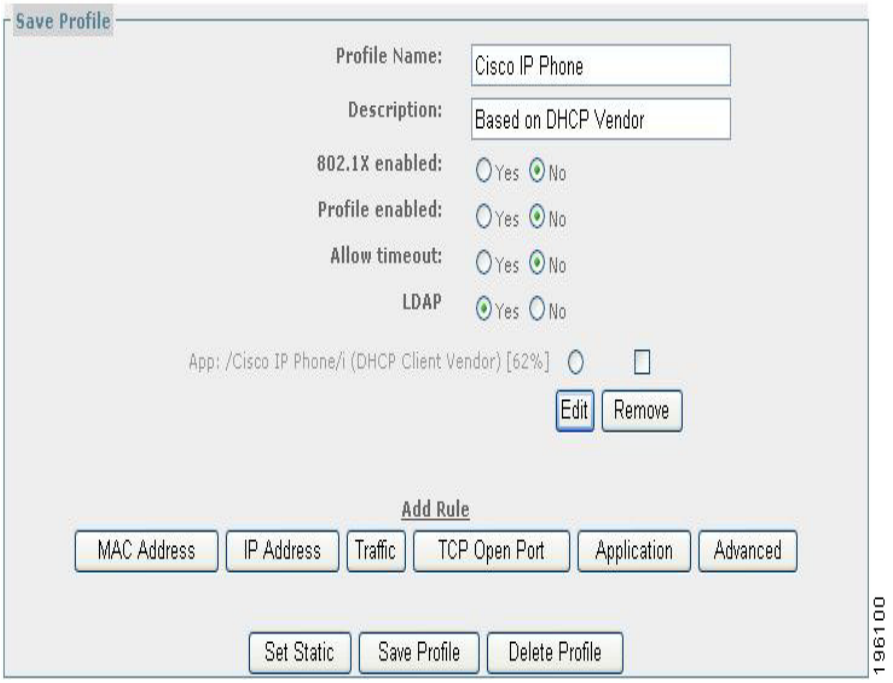
ステップ 2　[Configuration] > [Endpoint Profiles] > [View/Edit Profiles List] を選択します。

プロファイルのリストがテーブルに表示されます。

ステップ 3　プロファイルの名前をクリックして編集します。

ステップ 4　[Save Profile] ページで、図 8-2に示すように LDAP オプションをイネーブルにしていない場合は、LDAP オプションをイネーブルにし、**[Yes]** オプション ボタンをクリックします。

図 8-2　　NAC Profiler でのエンドポイント プロファイルの設定



ステップ 5　[Save Profile] をクリックします。

ID ポリシーで使用するための ACS での NAC Profiler LDAP 定義の設定

ACS をインストールすると、NAC Profiler 用の事前定義済み LDAP データベース定義がインストールされます。NAC Profiler に対して事前に定義されたこのデータベースの定義には、初期接続の確立に必要なすべてのデータが含まれています。ただし、特定の展開設定によって異なるホスト情報を除きます。

次の手順では、ホスト情報の設定方法、接続の確認方法、およびポリシーでのプロファイル データベースの使用方法について説明します。

（注）　[Access Policies] > [Access Services] > [Default Network Access] > [Identity] で ACS NAC Profiler が選択されていることを確認します。

（注）　LDAP 外部 ID ストアで使用できる ACS の **NAC Profiler** テンプレートは、Cisco NAC Profiler バージョン 2.1.8 以降で使用できます。

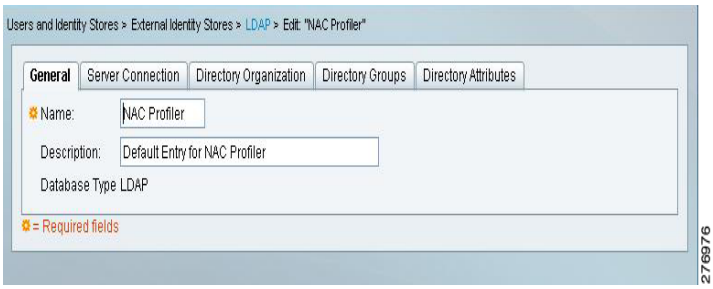
ACS で NAC Profiler テンプレートを編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

ステップ 2　NAC Profiler テンプレートの名前をクリックします。または、NAC Profiler テンプレート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。

図 8-3 に示すように、[Edit NAC Profiler definition] ページが表示されます。

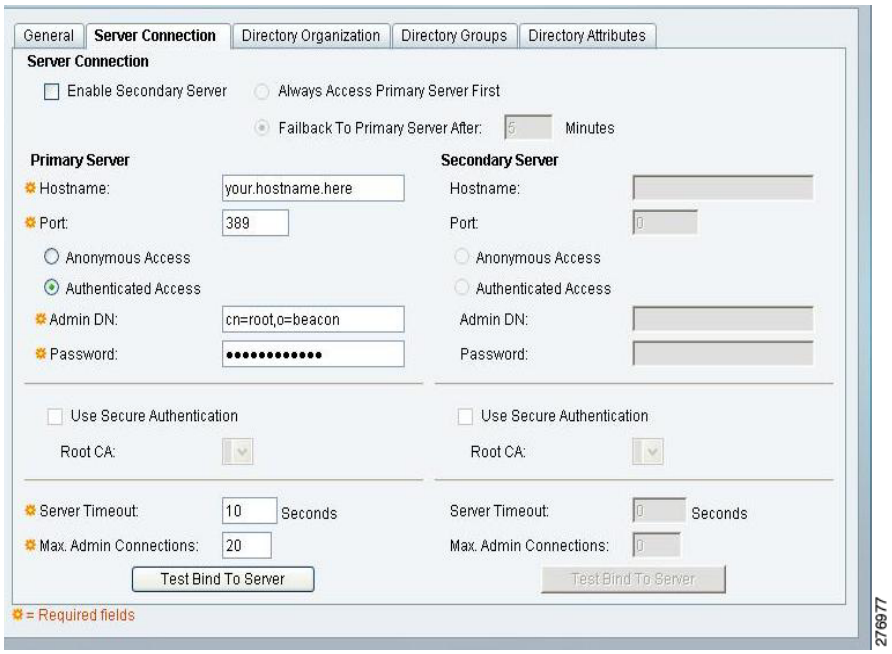
図 8-3　[Edit NAC Profiler Definition - General] ページ



ステップ 3　[Server Connection] タブをクリックします。

図 8-4 に示すように、[Edit] ページが表示されます。

図 8-4　[Edit NAC Profiler Definition - Server Connection] ページ



ステップ 4　[Primary Server Hostname] フィールドに、Profiler Server の IP アドレスまたは完全修飾ドメイン名を入力します。または、Profiler がハイ アベイラビリティ設定されている場合は、Profiler ペアのサービス IP を入力します。

ステップ 5　[Test Bind to Server] をクリックして、接続をテストし、ACS が LDAP を使用して Profiler と通信できることを確認します。

図 8-5 に示すような小さなポップアップ ダイアログが表示されます。

図 8-5　[Test Bind to Server] ダイアログボックス

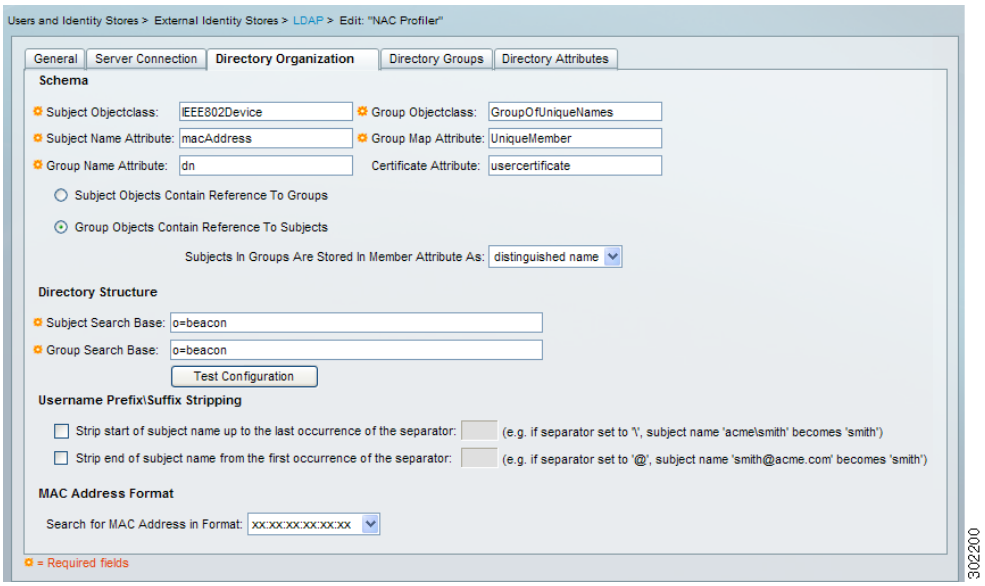
詳細については、外部 LDAP ID ストアの作成（8-35 ページ）を参照してください。

（注）　LDAP のデフォルト パスワードは *GBSbeacon* です。このパスワードを変更する場合は、『*Cisco NAC Profiler Installation and Configuration Guide*』を参照してください。

ステップ 6　成功した場合は、[Directory Organization] タブに移動します。

図 8-6 に示すように、[Edit] ページが表示されます。

図 8-6　[Edit NAC Profiler Definition - Directory Organization] ページ

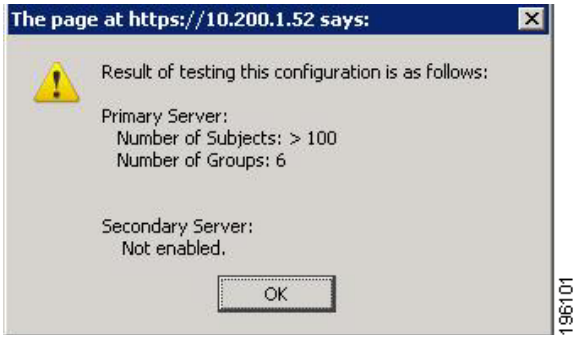


ステップ 7　[Test Configuration] をクリックします。

図 8-7（ 51 ページ）に示すダイアログボックスが表示され、Profiler に対応するデータが示されます。次に例を示します。

- Primary Server
- Number of Subjects: 100
- Number of Directory Groups: 6

図 8-7　[Test Configuration] ダイアログボックス



Number of Subjects：この値は、Cisco NAC Profiler によってすでにプロファイリングされている実際のサブジェクト デバイス（Profiler に対してイネーブルな実際のデバイス）に対応します。

Profiler が初期 SNMP トラップ情報をスイッチから受信したあと、Profiler は SNMP を使用してスイッチをポーリングし、スイッチおよび接続するエンドポイントに関する MIB（管理情報ベース）情報を収集できます。

Profiler は、エンドポイントについて学習すると（MAC アドレス、スイッチ ポートなど）、エンドポイントをデータベースに追加します。Profiler のデータベースに追加されたエンドポイントは、1 つのサブジェクトと見なされます。

Number of Directory Groups：この値は、Profiler で LDAP に対してイネーブルにされた実際のプロファイルに対応します。ネットワークで Profiler をすでに実行している場合は、エンドポイントのデフォルト プロファイルが事前設定されています。

ただし、すべてのプロファイルは LDAP に対してイネーブルではなく、LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定（8-47 ページ）の説明に従って設定する必要があります。Profiler を初めて設定した場合、Profiler が稼働すると、最初は 0 グループと表示される点に注意してください。

サブジェクトおよびディレクトリ グループは、数が 100 未満の場合に表示されます。サブジェクトまたはディレクトリ グループの数が 100 を超えた場合、サブジェクトおよびディレクトリ グループは表示されません。代わりに、次のようなメッセージが表示されます。

More than 100 subjects are found.

ステップ 8　サブジェクト レコードのディレクトリ属性をポリシー規則でポリシー条件として使用する場合は、[Directory Attributes] タブをクリックします。詳細については、「LDAP 属性の表示（8-44 ページ）」を参照してください。

ステップ 9　ID ポリシーの結果（ID ソース）として NAC Profiler を選択します。詳細については、ID ポリシーの表示（10-23 ページ）を参照してください。

ACS サーバからエンドポイントが正常に認証されると、ACS はただちに認可変更（CoA）を実行し、VLAN を変更します。この目的のために、ACS サーバにスタティック VLAN マッピングを設定できます。詳細については、認可プロファイルの共通属性の指定（9-20 ページ）を参照してください。

エンドポイントが正常に認証されると、スイッチに次のメッセージが表示されます。

```
ACCESS-Switch# #show authentication sessions
Interface MAC Address Method Domain Status Session ID
Fa1/0/1 0014.d11b.aa36 mab DATA Authz Success 505050010000004A0B41FD15
```

イベント配信方法やアクティブ応答などの機能の詳細については、『*Cisco NAC Profiler Installation and Configuration Guide, Release 3.1*』を参照してください。

（注）　LDAP サーバとして Microsoft Active Directory を使用し、ACS に対し認証を行うことができます。

Profiler の統合による MAB 認証のトラブルシューティング

NAC Profiler との統合中に MAB 認証のトラブルシューティングを行い、エンドポイントが正常に認証されることを確認するには、次の手順を実行します。

ステップ 1　エンドポイント デバイスに接続されたスイッチで次のコマンドを実行します。

```
ACCESS-Switch# show authentication sessions
```

次の出力が表示されます。

```
Interface  MAC Address    Method   Domain  Status         Session ID
Fa1/0/1    0014.d11b.aa36 mab      DATA    Authz Success  505050010000004A0B41FD15 reject
```

ステップ 2　スイッチで、SNMP、AAA、および 802.1X に対するデバッグをイネーブルにします。

ステップ 3　認証の失敗または成功について、[Monitoring and Reports Viewer] > [Troubleshooting] で MAB 認証ログを確認します。

Microsoft AD

ACS は Microsoft Active Directory（AD）を外部 ID ストアとして使用して、ユーザ、マシン、グループ、属性などのリソースを格納します。ACS は、これらのリソースを AD に対して認証します。

サポートされる認証プロトコル

- EAP-FAST および PEAP：ACS では、MSCHAPv2 および EAP-GTC という内部方式による EAP-FAST と PEAP を使用した、AD に対するユーザとマシンの認証およびパスワード変更がサポートされます。
- PAP：ACS では、TACACS PAP または ASCII 方式を使用した AD に対する認証がサポートされ、AD ユーザ パスワードを変更することもできます。
- MSCHAPv1：ACS では、MSCHAPv1 を使用した AD に対するユーザとマシンの認証がサポートされます。MSCHAPv1 バージョン 2 を使用すると、AD ユーザ パスワードを変更できます。ACS では、ユーザの MS-CHAP MPPE-Keys はサポートされませんが、MPPE-Send-Key および MPPE-Recv-Key はサポートされます。

（注）　ACS では、MSCHAP バージョン 1 を使用した AD に対するユーザ パスワードの変更はサポートされません。

- MSCHAPv2：ACS では、MSCHAPv2 を使用した AD に対するユーザとマシンの認証がサポートされます。ACS では、ユーザの MS-CHAP MPPE-Keys はサポートされませんが、MPPE-Send-Key および MPPE-Recv-Key はサポートされます。
- EAP-GTC：ACS では、EAP-GTC を使用した AD に対するユーザとマシンの認証がサポートされます。

- EAP-TLS：ACS では、EAP-TLS を使用した AD に対するユーザとマシンの認証をサポートするために、証明書取得オプションが使用されます。

ACS 5.x では、TACACS+ PAP/ASCII、EAP-MSCHAP および EAP-GTC 方式で Active Directory に対して認証されたユーザのパスワード変更をサポートします。内部 MSCHAPv2 による EAP-FAST および PEAP のパスワード変更もサポートされています。

上記の方法を使用した AD ユーザ パスワードの変更では、AD パスワード ポリシーに準拠する必要があります。AD 管理者と相談して、AD パスワード ポリシーのすべてのルール セットを決定してください。特に重要な AD パスワード ポリシーは次のとおりです。

- Enforce password history: N passwords are remembered.
- Maximum password age is N days.
- Minimum password age is N days.
- Minimum password length is N characters.
- Password must meet complexity requirements.

AD は、[Maximum password age is N days] ルールを使用して、パスワードの期限切れを検出します。他のルールはすべてパスワードの変更を試行する際に使用されます。

ACS では、次に示す AD ドメインがサポートされています。

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 Update 2

ACS Machine Access Restriction（MAR）機能は、AD を使用してマシン認証をユーザ認証および認可にマッピングし、マシン認証と、同じマシンからのユーザの認証の間で許可される最大時間を設定します。

通常、MAR は、ユーザのホスト マシンが認証に成功しない場合、またはマシンおよびユーザの認証間の時間が指定されたエージング タイムを超えた場合に、ユーザの認証に失敗します。必要に応じて、認証および認可規則の条件として MAR を追加できます。

ACS を AD ドメインに追加しようとするときに、ACS と AD は同期化されている必要があります。ACS の時間は、ネットワーク タイム プロトコル（NTP）サーバに従って設定されます。AD と ACS は、いずれも同じ NTP サーバによって同期化されている必要があります。ACS を AD ドメインに追加するときに時間が同期化されていない場合、ACS によってクロック スキュー エラーが表示されます。アプライアンスでコマンドライン インターフェイスを使用して、AD ドメインが同期化されている同じ NTP サーバと連携するように NTP クライアントを設定する必要があります。

NTP プロセスがダウンした場合は、自動的に再起動します。2 種類の方法で NTP プロセスのステータスを調べることができます。

- CLI インターフェイスで **`sh app status acs`** コマンドを使用します。
- ACS Web インターフェイスで [Monitoring and Reports] > [Reports] > [ACS Reports] > [ACS Instance] > [ACS_Health_Summary] を選択します。

詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.8*』を参照してください。

(注)　ACS は Active Directory ドメインとの間で双方向の信頼をサポートします。

ACS アプライアンスは、パフォーマンスを最適化するために、AD グループによって異なるキャッシング レベルを使用します。AD グループは固有識別子（SID、セキュリティ ID）で識別されます。ACS は、ユーザに属する SID を取得し、グループの完全な名前およびパスと SID とのキャッシュされたマッピングを使用します。AD クライアント コンポーネントは 24 時間マッピングをキャッシュしています。ACS のランタイム コンポーネントは、ACS が動作している限り、AD クライアントを照会し、結果をキャッシュします。

（注）　ACS が古いマッピングを使用しないように、既存のマッピングを変更または移動するのではなく、新しい AD グループを作成する必要があります。既存のグループを変更または移動した場合、すべてのキャッシュ データを更新するために、24 時間待ってから ACS サービスを再起動しなければなりません。

関連項目

- Active Directory と ACS との統合の前提条件（8-54 ページ）
- Active Directory 通信用に開放するネットワーク ポート（8-55 ページ）

Active Directory と ACS との統合の前提条件

次に、Active Directory と ACS とを統合するための前提条件を示します。

- Network Time Protocol（NTP）サーバ設定を使用して、ACS サーバと Active Directory との間で時間を同期します。ACS CLI から NTP を設定できます。
- Active Directory 構造にマルチドメインのフォレストがある場合、または複数のフォレストに分割されている場合は、ACS が接続されるドメインと、アクセスする必要があるユーザおよびマシン情報があるその他のドメインとの間に信頼関係があることを確認します。信頼関係の確立の詳細については、Microsoft Active Directory のドキュメントを参照してください。
- ACS を参加させるドメインでは、少なくとも 1 つのグローバル カタログ サーバが動作し、ACS からアクセス可能である必要があります。

表 8-11　さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退操作	ACS のマシン アカウント
参加操作の実行に使用するアカウントには、次の権限が必要です。 • Active Directory を検索する権限（ACS のマシン アカウントがすでに存在するかどうかの確認） • ドメインに ACS のマシン アカウントを作成する権限（マシン アカウントが存在しない場合） • 新しいマシン アカウントに属性を設定する権限（ACS のマシン アカウントのパスワード、SPN、dnsHostname など） （注）　参加操作を実行するために、ドメイン管理者である必要はありません。	脱退操作の実行に使用するアカウントには、次の権限が必要です。 • Active Directory を検索する権限（ACS のマシン アカウントがすでに存在するかどうかの確認） • ドメインから ACS のマシン アカウントを削除する権限 （注）　強制脱退（ドメイン クレデンシャルなしでの脱退）を実行する場合、ドメインからマシン アカウントは削除されません。	Active Directory 接続との通信に使用する、新規作成の ACS マシン アカウントには、次のアクセス許可が必要です。 • 自分のパスワードを変更する権限 • 認証されるユーザ/マシンに対応するユーザ/マシン オブジェクトを読み取る権限 • 必要な情報（信頼ドメイン、代替 UPN サフィックスなど）を取得するために Active Directory の一部を照会する権限 • tokenGroups 属性を読み取る権限 （注）　Active Directory でマシン アカウントを事前に作成できます。SAM の名前が ACS アプライアンスのホスト名と一致する場合は、参加操作中に検出して再利用する必要があります。 （注）　複数の参加操作を実行すると、参加操作ごとに 1 つずつ、複数のマシン アカウントが ACS 内で保持されます。

（注）　参加操作または脱退操作に使用するクレデンシャルは、ACS に保存されません。新しく作成された ACS のマシン アカウントのクレデンシャルのみが保存されます。

関連項目

Active Directory 通信用に開放するネットワーク ポート（8-55 ページ）

Active Directory 通信用に開放するネットワーク ポート

ACS では、証明書認証がサポートされています。ACS と AD の間にファイアウォールがある場合は、ACS が AD と通信できるように特定のポートを開く必要があります。開く必要があるデフォルトのポートは次のとおりです。

表 8-12　Active Directory 通信用に開放するネットワーク ポート

プロトコル	ポート（リモート - ローカル）	ターゲット	認証	注
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバ/AD ドメイン コントローラ	いいえ	—
MSRPC	445	ドメイン コントローラ	はい	—
Kerberos（TCP/UDP）	88	ドメイン コントローラ	はい（Kerberos）	MS AD/KDC
LDAP（TCP/UDP）	389	ドメイン コントローラ	はい	—

表 8-12　Active Directory 通信用に開放するネットワーク ポート

プロトコル	ポート（リモート - ローカル）	ターゲット	認証	注
LDAP（GC）	3268	グローバル カタログ サーバ	はい	—
NTP	123	NTP サーバ/ドメイン コントローラ	いいえ	—
KPASS	464	ドメイン コントローラ	はい（Kerberos）	MS AD/KDC
DNS（TCP/UDP）	53	DNS サーバ/AD ドメイン コントローラ	いいえ	—
IPC	80	展開内の他の ACS ノード	はい（RBAC クレデンシャルを使用）	—

（注）　ACS では、ダイヤルイン ユーザは AD によってサポートされません。

ここでは、次の内容について説明します。

マシン認証

マシン認証では、Active Directory にリストされているコンピュータに対してだけ、ネットワーク サービスへのアクセスが提供されます。このことは、無線ネットワークの場合に特に重要になります。権限のないユーザがオフィスの建物の外から無線アクセス ポイントにアクセスしようとする場合があるためです。

マシン認証は、コンピュータの起動時またはコンピュータへのログイン時に発生します。Funk Odyssey などのサプリカントは、サプリカントの実行中にマシン認証を定期的に実行します。

マシン認証を有効にすると、ACS は、ユーザ認証要求が送信される前にコンピュータを認証します。ACS は、Windows ユーザ データベースに対し、コンピュータから提供されるクレデンシャルをチェックします。クレデンシャルが一致した場合に、ネットワークへのアクセスがコンピュータに与えられます。

(注)　EAP-TLS プロトコルを使用してマシン認証を実行する場合、[Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory] オプションを有効にするか、または該当する LDAP または Active Directory を [Certificate Authentication Profile] > [CN User Name] > [Edit] ページで選択する必要があります。

関連項目

- 認可のための属性取得（8-57 ページ）
- Active Directory または LDAP のブール属性のサポート（8-58 ページ）
- AD または LDAP の複数値属性のサポート（8-59 ページ）
- 認可のためのグループ取得（8-62 ページ）
- EAP-TLS 認証のための証明書取得（8-62 ページ）

認可のための属性取得

認可およびグループ マッピング規則で使用される Active Directory ユーザまたはマシンの属性を取得するように ACS を設定できます。属性は ACS ポリシー結果にマッピングされ、ユーザまたはマシンの承認レベルが決定されます。

ACS は、ユーザまたはマシンの認証が成功したあとにユーザおよび Active Directory マシンの属性を取得します。認証とは別に、認可およびグループ マッピングのために属性を取得することもできます。

msRADIUSFramedIPAddress Attribute

ACS で、AD 属性から値を動的に取得するように Framed-IP-Address 属性を動的値として設定できます。ACS の IP アドレスとしてのみ AD から取得した、msRADIUSFramedIPAddress 属性を使用できます。この属性型は、文字列、整数、ブールなどに変換できません。

AD では、ダイヤルイン ユーザの場合、AD 管理者が静的 IP アドレスを割り当てます。ダイヤルイン ユーザがネットワークに接続しようとすると、要求が ACS に転送されます。ACS はその要求を処理し、AD に対してユーザを認証子、AD から取得した静的 IP アドレスを、ネットワークに接続しようとしているダイヤルアップ クライアントに割り当てます。ACS 5.8 では、msRADIUSFramedIPAdress 属性型は IP アドレスです。

msRADIUSFramedIPAddress 属性は、ACS の Active Directory 設定の [Directory Attributes] タブで msRADIUSFramedIPAddress 属性を設定する必要があり、この属性を ACS のネットワーク アクセス許可プロファイルに使用して、この値をダイヤルアップ クライアントに割り当てます。ネットワーク アクセス認可プロファイルの詳細については、ネットワーク アクセスの認可プロファイル（3-17 ページ）を参照してください。

関連項目

- Active Directory または LDAP のブール属性のサポート（8-58 ページ）
- AD または LDAP の複数値属性のサポート（8-59 ページ）
- 認可のためのグループ取得（8-62 ページ）
- EAP-TLS 認証のための証明書取得（8-62 ページ）

Active Directory または LDAP のブール属性のサポート

ACS 5.8 では、AD または LDAP の [Directory Attributes] ページでブール属性を設定して、AD または LDAP の ID ストアに対する認証中に AD または LDAP からブール属性を取得できます。ACS は、AD または LDAP の ID ストアに対して認証を行おうとしているユーザ固有の属性を取得します。

ACS は、ブール属性の次の値をサポートしています。

- True：t、T、true、TRUE、True、および 1。
- False：f、F、false、FALSE、False、および 0。

AD または LDAP の [Directory Attributes] ページでブール属性を設定し、それらを許可プロファイルに使用できます。前述のサポート値以外の値を設定した場合、ACS はブール属性を認識しません。

- AD または LDAP のブール属性を文字列として設定できます。ACS は LDAP または AD から取得中に特定の属性のブール値を文字列値に変換します。

  例として、ブール属性 msTSAllowLogon の場合を検討します。

  AD または LDAP で、属性 msTSAllowLogon はブール属性です。ACS では、msTSAllowLogon 属性を文字列として設定できます。
- AD または LDAP のブール属性の値が 0 または 1 である場合、その属性を整数に変換できます。
- AD または LDAP のブール属性は、ACS ではブール型の属性としてのみを取得できます。
- また、文字列または整数型 AD または LDAP 属性をACS のブール属性として設定できます。

  例として、属性 displayName を検討します。

  AD または LDAP で、属性 displayName は文字列型または整数型の属性です。ACS では、displayName 属性の値が前述のサポートされているブール値のいずれかである場合にのみ、displayName をブールとして設定できます。

（注） ACS は、RADIUS および TACACS+ 認証でブール属性の属性置換をサポートしません。

関連項目

- 認可のための属性取得（8-57 ページ）
- AD または LDAP の複数値属性のサポート（8-59 ページ）
- 認可のためのグループ取得（8-62 ページ）
- EAP-TLS 認証のための証明書取得（8-62 ページ）

AD または LDAP の複数値属性のサポート

ACS 5.8 では、AD または LDAP の [Directory Attributes] ページで複数値属性を設定して、AD または LDAP の ID ストアに対する認証中に AD または LDAP から複数値属性を取得できます。ACS は、AD または LDAP の ID ストアに対して認証を行おうとしているユーザ固有の属性を取得します。

ACS は、複数値属性に次の AD または LDAP の属性型をサポートします。

- 文字列
- 整数
- IP アドレス

これらの複数値属性を設定すると、許可プロファイルで使用できます。

複数値属性を含むアクセス ポリシーの条件を次の形式で構築できます。

- [複数値属性] [演算子] [複数値属性]
- [単一値属性] [演算子] [複数値属性]
- [複数値属性] [演算子] [単一値属性]
- [複数値属性] [演算子] [静的な値]

文字列の演算子：複数値属性型

ACS は文字列型複数値属性の次の演算子をサポートします。

- Equals
- Not Equals
- Starts with
- Ends with
- Contains
- Not contains

表 8-13 に、複数値、単一値、および静的な値属性のオペランド間に前述のオペレータを使用した場合の結果を表示します。

表 8-13　演算子を文字列型複数値属性間で使用した場合の結果

左側のオペランド	右側のオペランド	Equals	Not Equals	Starts with	Ends with	Contains	Not contains
複数値属性	複数値属性	左側のオペランドのすべての値が右側のオペランドの 1 つ以上の値と等しい場合は True。	左側のオペランドのどの値も右側のオペランドのどの値とも等しくない場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドのすべての値から始まる場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドのすべての値で終わる場合は True。	左側のオペランドの 1 つ以上の値に右側のオペランドのすべての値かが含まれている場合は True。	左側のオペランドの値に右側のオペランドのどの値も含まれていない場合は True。
単一値属性	複数値属性						
複数値属性	単一値属性						
複数値属性	静的な値	左側のオペランドの 1 つ以上の値が右側のオペランドの値と等しい場合は True。	左側のオペランドのどの値も右側のオペランドの値と等しくない場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値で始まる場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値で終わる場合は True。	左側のオペランドの 1 つ以上の値に右側のオペランドが含まれている場合は True。	左側のオペランドのどの値にも右側のオペランドが含まれていない場合は True。

例

- 左側の属性値 = 11 は右側の属性値 = {22,11,33} に**等しい**
  結果 = True
- 左側の属性値 = 11 は右側の属性値 = {22,44} に**等しい**
  結果 = False
- 左側の属性値 = 11 は右側の属性値 = {22,33,44} に**等しくない**
  結果 = True
- 左側の属性値 = 11 には右側の属性値 {22,11,33} **含まない**
  結果 = False
- 左側の属性値 = 123 は右側の属性値 = {12,23} を**含む**
  結果 = True

整数の演算子：複数値属性型

ACS は整数型複数値属性の次の演算子をサポートします。

- =
- !=
- >
- >=
- <
- <=

表 8-14 に、複数値、単一値、および静的な値属性のオペランド間に前述のオペレータを使用した場合の結果を表示します。

表 8-14　演算子を整数型複数値属性間で使用した場合の結果

左側のオペランド	右側のオペランド	=	!=	>	>=	<	<=
複数値属性	複数値属性	左側のオペランドの 1 つ以上の値が右側のオペランドのいずれかの値と等しい場合は True。	左側のオペランドのどの値も右側のオペランドのどの値とも等しくない場合は True。	左側のオペランドの 1 つ以上の値が右オペランドのいずれかの値より大よりも大きい場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドのいずれかの値以上の場合は True。	左側のオペランドの 1 つ以上の値が右オペランドのいずれかの値より小さい場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドのいずれかの値以下の場合は True。
単一値属性	複数値属性						
複数値属性	単一値属性						
複数値属性	静的な値	左側のオペランドの 1 つ以上の値が右側のオペランドの値と等しい場合は True。	左側のオペランドのどの値も右側のオペランドの値と等しくない場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値よりも大きい場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値以上の場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値よりも小さい場合は True。	左側のオペランドの 1 つ以上の値が右側のオペランドの値以下の場合は True。

例

- 左側の属性値 = {11,22,33} **=** 右側の属性値 = 11

  結果 = True
- 左側の属性値 = {11,22,33} **!=** 右側の属性値 = 11

  結果 = False
- 左側の属性値 = {11,22,33} **>** 右側の属性値 = 11

  結果 = True
- 左側の属性値 = {11,22,33} **<** 右側の属性値 = 11

  結果 = False

IP アドレスの演算子：複数値属性型

ACS は IP アドレス型複数値属性の次の演算子をサポートします。

- Equals
- Not Equals

表 8-15 に、複数値、単一値、および静的な値属性のオペランド間に前述のオペレータを使用した場合の結果を表示します。

表 8-15　演算子を IP アドレス型複数値属性間で使用した場合の結果

左側のオペランド	右側のオペランド	Equals	Not Equals
複数値属性	複数値属性	左側のオペランドの 1 つ以上の値が右側のオペランドのいずれかの値と等しい場合は True。	左側のオペランドのどの値も右側のオペランドのどの値とも等しくない場合は True。
単一値属性	複数値属性		
複数値属性	単一値属性		
複数値属性	静的な値		

関連項目

- 認可のための属性取得（8-57 ページ）
- Active Directory または LDAP のブール属性のサポート（8-58 ページ）
- 認可のためのグループ取得（8-62 ページ）
- EAP-TLS 認証のための証明書取得（8-62 ページ）

認可のためのグループ取得

ACS は、認証が成功したあとにユーザまたはマシン グループを Active Directory から取得できます。認証とは別に、認可およびグループ マッピングのためにユーザまたはマシン グループを取得することもできます。AD グループ データを認可およびグループ マッピング テーブルで使用でき、特殊条件を導入して、取得したグループと突き合せることができます。

関連項目

- 認可のための属性取得（8-57 ページ）
- Active Directory または LDAP のブール属性のサポート（8-58 ページ）
- AD または LDAP の複数値属性のサポート（8-59 ページ）
- EAP-TLS 認証のための証明書取得（8-62 ページ）

EAP-TLS 認証のための証明書取得

ACS 5.8 では、EAP-TLS プロトコルを使用するユーザまたはマシン認証のための証明書取得がサポートされています。AD 上のユーザまたはマシン レコードには、バイナリ データ型の証明書属性が含まれています。これに 1 つ以上の証明書を含めることができます。ACS ではこの属性は userCertificate として参照され、この属性に対して他の名前を設定することはできません。

ACS は、ユーザまたはマシンの ID を確認するためにこの証明書を取得します。証明書認証プロファイルによって、証明書を取得するために使用されるフィールド（SAN、CN、SSN、SAN-Email、SAN-DNS、またはその他の SAN 名）が決まります。

ACS は、証明書を取得したあと、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、ACS は、それらのいずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ACS はユーザまたはマシンにネットワークへのアクセスを付与します。

関連項目

- 同時接続管理（8-63 ページ）
- ユーザおよびマシン アカウントの制限（8-63 ページ）
- マシン アクセス制限（8-63 ページ）

同時接続管理

起動時に、ACS が AD ドメインに接続したあと、ACS はパフォーマンス向上のために、AD ID ストアによって使用される数多くのスレッドを作成します。各スレッドに独自の接続があります。

関連項目

- ユーザおよびマシン アカウントの制限（8-63 ページ）
- マシン アクセス制限（8-63 ページ）

ユーザおよびマシン アカウントの制限

ユーザまたはマシンの認証または問い合わせ中に、ACS は次のことをチェックします。

- ユーザ アカウントがディセーブルかどうか
- ユーザ アカウントがロックアウトされているかどうか
- ユーザのアカウントが期限切れかどうか
- クエリー実行が指定されたログイン時間外かどうか

ユーザにこれらの制限のいずれかがある場合、AD 専用ディクショナリ上の *AD1::IdentityAccessRestricted* 属性が設定され、ユーザのアクセスが制限されることが示されます。この属性は、グループ マッピングおよび認可規則に使用できます。

関連項目

- マシン アクセス制限（8-63 ページ）
- 分散 MAR キャッシュ（8-65 ページ）
- ダイヤルイン アクセス権（8-67 ページ）
- ダイヤルイン ユーザのコールバック オプション（8-67 ページ）
- AD ドメインへの ACS の追加（8-69 ページ）

マシン アクセス制限

MAR は、マシン認証の結果をユーザ認証および認可プロセスに結びつけるのに役立ちます。MAR の最も一般的な使用法は、ホスト マシンが正常に認証されないユーザの認証を拒否することです。MAR は、すべての認証プロトコルに効果的です。

MAR の機能は、次の点に基づいています。

- マシンの RADIUS `Calling-Station-ID attribute (31)` は、マシン認証の結果として今後の参照用にキャッシュされます。
- 管理者は、AD の設定ページで上記のキャッシュ エントリの存続可能時間（TTL）を設定できます。

- 管理者は、[AD settings] ページから、MAR を有効化することも無効化することもできます。ただし、MAR を動作させる場合は、次の制限事項を考慮する必要があります。
  - 認証プロトコルの設定で、マシン認証をイネーブルにする必要があります。
  - AAA クライアントは、Internet Engineering Task Force（IETF）RADIUS `Calling-Station-Id attribute (31)` で値を送信する必要があります。
  - ACS は、正常なマシン認証から `Calling-Station-Id attribute` 値のキャッシュを複製しません。
  - ACS は、`Calling-Station-Id attribute` のキャッシュを保持しません。そのため、ACS が突然クラッシュした場合はコンテンツが失われます。管理者がマシン認証に影響する可能性のある設定変更を行った場合、内容の整合性は確認されません。
- ユーザが AD 外部 ID ストアに対して PEAP または EAP-FAST を使用した認証を行うと、ACS は追加のアクションを実行します。ACS は、ユーザの `Calling-Station-Id` のキャッシュを検索します。このキャッシュが見つかった場合は、セッション コンテキストで **Was-Machine-Authenticated** 属性を true に設定し、見つからなかった場合は false に設定します。

（注） EAP-TLS プロトコルを使用してマシン認証を実行する場合、[Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory] オプションを有効にするか、または該当する LDAP または Active Directory を [Certificate Authentication Profile] > [CN User Name] > [Edit] ページで選択する必要があります。

- 上記を正しく機能させるため、ユーザ認証要求に `Calling-Station-Id` が含まれていることが必要です。この属性が含まれていない場合は、**Was-Machine-Authenticated** 属性を false に設定します。
- 管理者は、AD GM 属性とマシン認証の必須属性に基づいた規則を認可ポリシーに追加できます。これらの 2 つの属性を含む規則は、次の条件を満たしている場合のみ適用されます。
  - MAR 機能がイネーブルであること
  - 認証プロトコルの設定で、マシン認証がイネーブルであること
  - 外部 ID ストアが AD であること
- 上記のような規則が評価されると、AD GM および **Was-Machine-Authenticated** の属性がセッション コンテキストから取得され、規則の条件と照合されます。この評価の結果に応じて、認可結果が設定されます。
- 免除リストの機能は、（ACS 4.x とは対照的に）暗黙的にサポートされています）。所定のユーザ グループを MAR から免除するため、管理者は、[AD Group] カラムを免除するグループで構成し、[Machine Authentication Required] カラムを [*No*] で構成するように規則を設定できます。次に示すテーブルの 2 番めの規則がその一例です。

  たとえば、管理者は、次のように認可ポリシーに規則を追加します。

AD Group	Machine Authentication Required	…	ATZ profile
Engineers	はい	…	VLAN X
Managers	いいえ	…	VLAN B
…	…	…	DENY ACCESS

[Engineers] の規則は、マシンが Windows DB に対して正常に認証された場合に限り、エンジニアにアクセスを許可する MAR 規則の例です。

[Managers] の規則は、MAR からの免除の例です。

関連項目

- 分散 MAR キャッシュ（8-65 ページ）
- ダイヤルイン アクセス権（8-67 ページ）
- ダイヤルイン ユーザのコールバック オプション（8-67 ページ）
- AD ドメインへの ACS の追加（8-69 ページ）

分散 MAR キャッシュ

ACS 5.8 では、ACS の配置ごとにマシン アクセス制限キャッシュをサポートします。つまり、マシン認証結果を配置内の各ノードにキャッシュできます。

MAR キャッシュ分散グループ

ACS 5.8 では、ACS ノードを MAR キャッシュ分散グループにグループ化できます。このオプションは、ACS のパフォーマンスとメモリ使用量に与える MAR キャッシュ分散操作による影響を制御するために使用されます。

MAR キャッシュ分散グループ値と呼ばれるテキスト ラベルが各 ACS ノードに割り当てられます。ACS ノードは MAR キャッシュ分散グループ値に基づいてグループ化されます。同じ MAR キャッシュ分散グループに割り当てられた ACS ノード間でのみ、MAR キャッシュ分散操作を実行できます。

ACS ノードのグループ値が空の場合は、MAR キャッシュ分散グループに割り当てられていないと見なされます。このような ACS ノードは MAR キャッシュ分散操作の一部ではありません。

分散 MAR キャッシュの操作

ACS ランタイム コンポーネントは分散 MAR キャッシュを実装するために、2 種類の操作を組み合わせます。

- 配信保証なしの MAR キャッシュのレプリケーション
- MAR キャッシュ分散検索

MAR キャッシュのレプリケーション

ACS ランタイム コンポーネントは、マシン認証の間に、MAR エントリ `authenticated Calling-Station-ID` を MAR キャッシュに保存します。最初に、ACS はローカル MAR キャッシュに MAR エントリを保存します。次に、ACS ランタイム コンポーネントが、同じ MAR キャッシュ分散グループに属している ACS ノードに MAR エントリを複製します。

レプリケーションは、ACS Web インターフェイスで設定された [Cache entry replication attempts] および [Cache entry replication timeout] に基づいて実行されます。

レプリケーション操作はバックグラウンドで行われ、このレプリケーションを発生させたユーザ認証を中断または遅延させません。

MAR キャッシュ分散検索

認証要求を受信すると、ACS はローカル MAR キャッシュの MAR エントリを検索します。MAR エントリがローカルの MAR キャッシュに存在しない場合、ACS は同じ MAR キャッシュ分散グループに割り当てられた ACS ノードに問い合わせます。

分散検索は、ACS Web インターフェイスで設定された [Cache entry query attempts] および [Cache entry query timeout] に基づいて実行されます。また、MAR エントリ検索は、照会された ACS ノードのいずれかから最初の成功応答が返されるまで、最大で設定された [Cache entry query timeout] の時間まで延期されます。MAR キャッシュの問合せを含む認証について、ACS View で次のメッセージを表示できます。

- 24422：ACS は、Active Directory ユーザの以前の成功したマシン認証を確認しました。
- 24423：ACS は、Active Directory ユーザの以前の成功したマシン認証を確認できませんでした。
- 24701：ACS ピアは、Active Directory ユーザの以前の成功したマシン認証を確認しました。
- 24702：ACS ピアは、Active Directory ユーザの以前の成功したマシン認証を確認できませんでした。

分散 MAR キャッシュの信頼性

ACS ランタイム コンポーネントは分散型の MAR キャッシュ操作を実行するための信頼できるメカニズムを提供します。

分散検索オプションは、レプリケーション メッセージが何らかの理由で配信されない場合にフォール バック機能を提供します。この場合、マシン認証を実行する ACS ノードか、同じ MAR キャッシュ分散グループの ACS ノードのいずれかで、キャッシュ エントリを検索できます。また、分散検索オプションは、マシン認証を実行する ACS ノードの再起動時にフォールバック機能を提供します。この場合も、同じ MAR キャッシュ分散グループの ACS ノードのいずれかで MAR キャッシュ エントリを検索できます。

分散 MAR キャッシュの永続性

手動で ACS ランタイム サービスが停止された場合、ACS 5.8 は、MAR キャッシュ コンテンツ、calling-station-ID リスト、および対応するタイム スタンプをローカル ディスクのファイルに保存します。この ACS インスタンスのランタイム サービスがダウンした場合、MAR キャッシュ分配グループの他の ACS インスタンスは ACS インスタンスの MAR キャッシュにアクセスできません。ランタイム サービスを誤って再起動した場合、ACS は インスタンスの MAR キャッシュ エントリを保存しません。

ACS ランタイム サービスが再起動した場合、ACS はキャッシュ エントリの存続時間に基づいてローカル ディスク上のファイルから MAR キャッシュ エントリを読み取ります。再起動後に ACS インスタンスのランタイム サービスが稼働した場合、ACS はインスタンスの現在の時刻と MAR キャッシュ エントリの時刻を比較します。現在の時刻と MAR エントリの時刻の差が MAR キャッシュ エントリの存続時間よりも大きい場合、ACS はディスクからエントリを取得しません。それ以外の場合、ACS は MAR キャッシュ エントリを取得し、MAR キャッシュ エントリ存続時間を更新します。

関連項目

- ダイヤルイン アクセス権（8-67 ページ）
- ダイヤルイン ユーザのコールバック オプション（8-67 ページ）
- AD ドメインへの ACS の追加（8-69 ページ）

ダイヤルイン アクセス権

ユーザのダイヤルイン アクセス権は、認証または Active Directory からのクエリーで確認されます。ダイヤルインのチェックは、次の認証プロトコルで、マシンではなくユーザの認証でサポートされます。

- PAP
- MSCHAPv2
- EAP-FAST
- PEAP
- EAP-TLS。

結果は次のとおりです。

- Allow Access
- Deny Access
- Control Access through Remote Access Policy。このオプションは、Windows 2000 ネイティブ ドメイン、Windows Server 2003 ドメインの場合のみ使用可能です。
- Control Access through NPS Network Policy。これはデフォルトの結果です。このオプションは、Windows Server 2008 および Windows 2008 R2、および Windows 2012 のドメインの場合のみ使用可能です。

関連項目

- ダイヤルイン ユーザのコールバック オプション（8-67 ページ）
- AD ドメインへの ACS の追加（8-69 ページ）

ダイヤルイン ユーザのコールバック オプション

コールバック オプションがイネーブルの場合、サーバは接続プロセス中に発信者にコールバックします。サーバによって使用される電話番号は、発信者またはネットワーク管理者によって設定されます。

コールバック オプションは次のいずれかです。

- No callback
- Set by Caller（ルーティングとリモート アクセス サービスのみ）。このオプションは、接続が行われたときにルーティングとリモート アクセス サービスを実行しているサーバのルーティング テーブルに追加される一連のスタティック IP ルートの定義に使用できます。
- Always callback to（番号を設定するオプションを含む）。このオプションは、接続が行われたときにユーザに特定の IP アドレスを割り当てるために使用できます。

コールバック属性は、デバイスへの RADIUS 応答で返される必要があります。

ダイヤルイン サポートの属性

Active Directory のユーザ属性は、次のサーバでサポートされます。

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2

ACS は、Windows 2000 のダイヤルイン ユーザをサポートしません。

ACS 応答

ACS Active Directory でダイヤルインのチェックをイネーブルにした場合、ユーザのダイヤルイン オプションが Active Directory で [Deny Access] の場合、認証要求は拒否され、ダイヤルイン アクセスが拒否されたことを示すメッセージがログに記録されます。ダイヤルインがイネーブルでない場合に、ユーザが MSCHAP v1/v2 の認証で失敗すると、ACS は EAP 応答で適切なエラー コード（NT エラー = 649）を設定します。

コールバック オプションがイネーブルの場合、ACS RADIUS 応答には、次のように返されたサービス タイプおよびコールバック番号属性が含まれます。

- コールバック オプションが [Set by Caller] または [Always Callback To] の場合、service-type 属性は、ユーザ認証時に Active Directory に問い合わせる必要があります。service-type は次のようになります。
  - 3 = コールバック ログイン
  - 4 = コールバック構築
  - 9 = コールバック NAS プロンプト

  この属性は、service-type RADIUS 属性でデバイスに返す必要があります。RADIUS 応答で service-type 属性を返すように ACS がすでに設定されている場合、Active Directory のユーザを問い合わせるための service-type 値に置き換えられます。
- コールバック オプションが [Always Callback To] の場合、Active Directory ユーザのコールバック番号も問い合わせる必要があります。この値は、RADIUS 応答の Cisco-AV-Pair 属性に次の値で設定されます。
  - cisco-av-pair=lcp:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Shell:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Slip:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Arap:callback-dialstring=[コールバック番号値]

  コールバック番号値も、RADIUS 属性 CallbackNumber（#19）を使用して、RADIUS 応答で返されます。
- コールバック オプションが [Set by Caller] の場合、RADIUS 応答には、値なしで次の属性が含まれます。
  - cisco-av-pair=lcp:callback-dialstring=
  - cisco-av-pair=Shell:callback-dialstring=
  - cisco-av-pair=Slip:callback-dialstring=
  - cisco-av-pair=Arap:callback-dialstring=

関連項目

- AD ドメインへの ACS の追加（8-69 ページ）
- AD ID ストアの設定（8-69 ページ）

AD ドメインへの ACS の追加

同じ展開の ACS ノードを、相互に双方向の信頼がある別の AD ドメインに参加させることができます。ただし、各ノードは、単一の AD ドメインにのみ追加できます。これらの ACS ノードのポリシー定義は変更されず、同じ AD ID ストアを使用します。

(注)

- ACS の以前のリリースでは、ACS CLI から手動で AD クライアント プロセスを停止すると Active Directory ドメインを切断し、[Active Directory Connection Details] ページに「joined but disconnected」というステータスが表示されます。一方、ACS 5.8 では、ACS CLI から手動で AD クライアント プロセスを停止すると、ACS は Active Directory ドメインを切断し、[Active Directory Connection Details] ページに「None」というステータスが表示されます。ACS CLI から AD クライアント プロセスを再度起動すると、ACS は Active Directory ドメインに接続し、[Active Directory Connection Details] ページに「joined and connected」というステータスが表示されます。
- ACS 5.8 の場合、ACS 5.x から ACS 5.8 にアップグレードしたら、ACS を Active Directory に手動で参加させる必要があります。アップグレード方法の詳細については、『Installation and Upgrade Guide for Cisco Secure Access Control System』を参照してください。
- リリース 5.8 より前の ACS では、Active Directory に ACS が参加してからのみ、AD クライアント プロセスが起動しました。しかし ACS 5.8 では、インストールするとすぐに AD クライアント プロセスが起動します。
- AD ドメインに ACS を追加する Windows AD アカウントは、独自の組織ユニット(OU)で作成できます。アカウントを作成するときまたは後で独自 OU で作成できますが、アプライアンスの名前が AD アカウント名に一致する必要があります。
- ACS では、ユーザ名が OU レベルで設定した代替 UPN サフィックスで指定されている場合は、AD のユーザ認証をサポートしません。UPN サフィックスがドメイン レベルで設定されている場合、認証は正常に動作します。

AD ID ストアの設定方法の詳細については、AD ID ストアの設定（8-69 ページ）を参照してください。

関連項目

- AD ID ストアの設定（8-69 ページ）
- AD グループの選択（8-74 ページ）
- AD 属性の設定（8-75 ページ）
- マシン アクセス制限の設定（8-77 ページ）

AD ID ストアの設定

AD の設定はデフォルトで表示されず、最初に ACS をインストールしたとき、AD ドメインに追加されません。AD の設定ページを開くと、分散展開内のすべての ACS ノードのリストが表示されます。

AD ID ストアを設定すると、ACS によって次のものも作成されます。

- 2 個の属性（ExternalGroup 属性と、[Directory Attributes] ページから取得される属性用の別の属性）を持つそのストア用の新しいディクショナリ。
- 新しい属性 IdentityAccessRestricted。この属性のカスタム条件を手動で作成できます。

- ExternalGroup 属性からのグループ マッピングのカスタム条件（カスタム条件名は AD1:ExternalGroups）、および [Directory Attributes] ページで選択された各属性用の別のカスタム条件（AD1:cn など）。

事前定義済みの条件名を編集でき、[Custom condition] ページからカスタム条件を作成できます。カスタム セッション条件の作成、複製、および編集（9-5 ページ）を参照してください。

ユーザを認証し、ACS を AD ドメインに追加するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

AD の設定ページは、すべての ACS ノードの集中 AD 管理ツールとして機能します。単一の ACS ノードまたは複数の ACS ノードに対して、このページで参加操作および脱退操作を実行できます。また、展開内のすべての ACS ノードの追加結果が一目でわかるように表示されます。

ステップ 2　表 8-16 の説明に従って、[General] タブのフィールドを変更します。

表 8-16　[Active Directory: General] ページ

オプション	説明
Connection Details	
Join	クリックすると、入力したユーザ、ドメイン、パスワードを使用して、AD ドメインに ACS を参加させます。AD ドメインへのノードの追加（8-72 ページ）を参照してください。
Leave	入力したユーザ、ドメイン、パスワードを使用して、AD ドメインから単一ノードまたは複数ノードを切断する場合にクリックします。AD ドメインからノードの接続解除（8-73 ページ）を参照してください。
End User Authentication Settings	
Enable password change	パスワード変更を許可する場合にクリックします。
Enable machine authentication	マシン認証を許可する場合にクリックします。
Enable dial-in check	認証またはクエリー時にユーザのダイヤルイン アクセス権を確認する場合にクリックします。ダイヤルイン アクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。 結果は AD ディクショナリに保存されません。
Enable callback check for dial-in clients	認証またはクエリー時にユーザのコールバック オプションを検査する場合にクリックします。チェックの結果は、RADIUS 応答でデバイスに返されます。 結果は AD ディクショナリに保存されません。
Use Kerberos for Plain Text	プレーン テキスト認証に Kerberos を使用する場合にクリックします。ACS 5.8 では、デフォルトの推奨オプションは MS-RPC です。ACS 5.7 までは、Kerberos がデフォルト オプションとして使用されていました。
Identity Resolution：ID 解決設定では、Active Directory 展開に一致するようセキュリティおよびパフォーマンスのバランスを調整する重要な設定ができます。これらの設定を使用すると、ドメイン マークアップのないユーザ名およびホスト名の認証を調整できます。	
If identity does not include the AD domain	

表 8-16　[Active Directory: General] ページ（続き）

オプション	説明
Reject the request	SAM 名などのドメイン マークアップがないユーザの認証要求を拒否するには、このオプションをクリックします。このことは、複数参加ドメインの場合に役立ちます。参加しているすべてのグローバル カタログで ID を ACS が検索する必要があるため、安全性が低下する可能性があるためです。このオプションによって、ユーザに対し、ドメイン マークアップを含むユーザ名を使用することが強制されます。
Only search in the “Authentication Domains” from the joined forest	認証ドメイン セクションで指定したフォレスト内の信頼できるドメインのみで ID を検索するには、このオプションをクリックします。これはデフォルト オプションであり、SAM アカウント名に対する ACS 5.7 の動作と同じです。
Search in all the “Authentication Domains” section	すべての信頼できるフォレスト内のすべての認証ドメインで ID を検索するには、このオプションをクリックします。これにより、遅延が増加し、パフォーマンスに影響する可能性があります。
If some of the domains are unreachable	
Proceed with available domains	いくつかのドメインに到達できない場合に、利用可能ないずれかのドメインで一致が見つかったら認証を続行するには、このオプションをクリックします。
Drop the request	ID 解決で到達不能または使用不可能なドメインが検出された場合に認証要求をドロップするには、このオプションをクリックします。

ステップ 3　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。
- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、次のことを確認したあとで [Clear Configuration] 。
  - AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がない。
  - 使用可能なアクセス サービスで AD が ID ソースとして選択されていない。
  - AD に ID ストア順序がない。
- ACS を AD ドメインに参加/から脱退させた後に [Directory Groups] タブ、[Authentication Domains] タブ、[Diagnostic Tool] タブのデータを更新するには、[Refresh]。

Active Directory の設定が保存されます。[Active Directory] ページが新しい設定で表示されます。

（注）

- AD ドメインとの ACS 接続をテストする間、サーバの応答が遅い場合、AD の設定が影響を受けます（または切断されることがあります）。ただし、設定は他のアプリケーションでは正常に機能します。
- ACS 5.8 の [Active Directory] ページは、60 秒間隔で自動的にリフレッシュされます。AD ページで操作を実行すると、操作のステータスはわずか 60 秒後に AD ページで更新されます。更新ステータスをすぐに確認するには、[General] タブ下部の [Refresh] オプションをクリックする必要があります。
- NETBIOS の制限により、ACS ホスト名は 15 文字以下にする必要があります。

（注）　AD ユーザの [User change password at next logon] オプションが有効化されると、次のようになります。
(a) ユーザ認証に Kerberos を使用する場合、パスワードは、次のログイン時にパスワードを変更した直後に変更されます。
(b) ユーザ認証に MSRPC を使用する場合、次のログイン時にパスワードを変更してから、新しいパスワードが ACS と同期されるまで、相応の時間待機する必要があります。この間、古いパスワードが機能することがあります。詳細については、https://support.microsoft.com/en-us/kb/906305 を参照してください。

AD ドメインへのノードの追加

1 つの ACS ノードが参加できる AD ドメインは、1 つのみです。ACS では、単一 ACS ノードの複数 AD ドメインへの参加はサポートしていません。ただし ACS は、複数 ACS ノードの単一 AD ドメインへの参加はサポートしています。

ACS ノードを AD ドメインに参加させるには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

ステップ 2　単一ノードまたは複数のノードを選択し、[Join] をクリックします。

[Join] ページが表示されます。

ステップ 3　表 8-17 の説明に従って、[Join] ページのフィールドに入力します。

表 8-17　[Join/Test Connection] ページ

オプション	説明
Active Directory Domain Name	ACS を追加する AD ドメインの名前。
Username	事前定義された AD ユーザのユーザ名を入力します。ACS でのドメイン アクセスに必要な AD アカウントには、次のいずれかが必要です。 • 対応するドメインのドメイン ユーザにワーク ステーションを追加する権限。 • ACS マシンのアカウントが事前に作成される（ACS マシンをドメインに追加する前に作成される）対応するコンピュータ コンテナに対してコンピュータ オブジェクトを作成する権限またはコンピュータ オブジェクトを削除する権限。 ACS アカウントのロックアウト ポリシーをディセーブルにし、不正なパスワードがこのアカウントに使用された場合に管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。これは、誤ったパスワードを入力した場合、ACS が必要なときにマシン アカウントを作成または変更しないため、すべての認証が拒否されるためです。
Password	ユーザ パスワードを入力します。パスワードは、少なくとも 1 文字の小文字、1 文字の大文字、1 文字の数字、および 1 文字の特殊文字を組み合わせて、8 文字以上にする必要があります。すべての特殊文字がサポートされています。

ステップ 4　次のいずれかをクリックします。

- [Join]：AD ドメインに選択したノードを追加します。ノードの状態が結合の結果によって変化します。
- [Cancel]：接続をキャンセルします。

（注）　Active Directory ドメインに ACS を参加させてから、ACS CLI からネーム サーバを削除した場合、ACS からサービスを再起動するよう要求されます。サービスの再起動に [No] を入力すると、ACS はサービスを再起動せず、設定からネーム サーバが削除されます。ただし ACS は、[Active Directory General] ページでは Active Directory ドメインのステータスを「None」と表示します。

AD ドメインからノードの接続解除

AD ドメインから単一ノードまたは複数ノードを接続解除するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

ステップ 2　単一ノードまたは複数ノードを選択し、[Leave] をクリックします。

[Leave Connection] ページが表示されます。

ステップ 3　表 8-18 の説明に従って、[Leave Connection] ページのフィールドに入力します。

表 8-18　[Leave Connection] ページ

オプション	説明
Username	事前定義された AD ユーザのユーザ名を入力します。ACS でのドメイン アクセスに必要な AD アカウントには、次のいずれかが必要です。 • 対応するドメインのドメイン ユーザにワーク ステーションを追加する権限。 • ACS マシンのアカウントが事前に作成される（ACS マシンをドメインに追加する前に作成される）対応するコンピュータ コンテナに対してコンピュータ オブジェクトを作成する権限またはコンピュータ オブジェクトを削除する権限。 ACS アカウントのロックアウト ポリシーをディセーブルにし、不正なパスワードがこのアカウントに使用された場合に管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。これは、誤ったパスワードを入力した場合、ACS が必要なときにマシン アカウントを作成または変更しないため、すべての認証が拒否されるためです。
Password	ユーザ パスワードを入力します。
Do not try to remove machine account	クレデンシャルがわからない場合または DNS の問題がある場合に、選択したノードを AD ドメインから接続解除するには、このチェックボックスをオンにします。 この操作は、AD ドメインからノードを切断し、データベースにこのノードのエントリをそのまま残します。管理者だけが、データベースからこのノード エントリを削除できます。

ステップ 4　次のいずれかをクリックします。

- [Leave]：選択したノードを AD ドメインから切断します。
- [Cancel]：操作をキャンセルします。

(注)
- 管理者は、セカンダリ サーバから参加または脱退の操作を実行できます。セカンダリ サーバで次の操作を実行すると、セカンダリ サーバだけに影響します。
- 認証失敗は必ずしも、Active Directory ドメインから ACS アカウントを無効にした直後に発生するわけではありません。接続または TGT チケットが確立されている限り、認証は実行されます。認証失敗の原因となるエラーは、ACS への接続に使用する接続方法が LDAP か Kerberos か RPC かによって異なることがあります。また、ドメイン コントローラ間のレプリケーションによっても異なります。

関連項目

- AD グループの選択（8-74 ページ）
- AD 属性の設定（8-75 ページ）
- マシン アクセス制限の設定（8-77 ページ）
- 高度な調整（8-78 ページ）
- 認証ドメインの設定（8-78 ページ）
- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

AD グループの選択

このページは、ポリシー条件に使用できるグループを選択する場合に使用します。

(注)　AD からグループおよび属性を選択するには、ACS がその AD に接続されている必要があります。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Directory Groups] タブをクリックします。

対応する Security Identifier（SID）の [Groups] ページが表示されます。[Selected Directory Groups] フィールドに、選択して保存した AD グループが表示されます。[External User Groups] ページで選択した AD グループが表示され、規則テーブルのグループ マッピング条件でオプションとして使用できます。

表示されていない他の信頼ドメインまたはフォレストにさらにグループがある場合は、検索フィルタを使用して検索結果を絞り込むことができます。[Add] ボタンを使用して新しい AD グループを追加することもできます。

(注)
- ACS ではドメイン ローカル グループを取得しません。ACS ポリシーでドメイン ローカル グループを使用することは推奨されません。その理由は、ドメイン ローカル グループでのメンバーシップ評価には時間がかかるためです。そのため、デフォルトでは、ドメイン ローカル グループは評価されません。
- ACS 5.5、5.6、5.7 には、ディレクトリ グループに関連付けられている SID はありません。そのため、ACS 5.5、5.6、5.7 から ACS 5.8 にアップグレードすると、ディレクトリ グループは SID 値なしで表示されます。SID という新しい列がすべてのディレクトリ グループに対して追加されており、すべてのディレクトリ グループで SID の値が空になっています。グループの SID 値を設定するには、ディレクトリ グループを再度取得する必要があります。

ステップ 2　[Select] をクリックして、ドメインとその子ドメインで使用可能な AD グループを表示します。同じフォレスト内の AD の信頼ドメイン グループを表示するには、信頼ドメインの詳細を [search base DN] フィールドで明示的に指定する必要があります。

[External User Groups] ダイアログボックスが表示され、ドメインおよび同じフォレスト内の他の信頼ドメインの AD グループのリストが表示されます。

表示されていないグループがさらにある場合は、検索フィルタを使用して検索を絞り込み、[Go] をクリックします。

ステップ 3　AD グループを入力するか、リストから選択し、[OK] をクリックします。

AD グループをリストから削除するには、AD グループをクリックして [Deselect] をクリックします。

ステップ 4　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。
- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[Clear Configuration] をクリックします。

（注）

- ACS 5.x で AD ID ストアを設定する場合、Active Directory に定義されているセキュリティ グループが列挙され、使用できますが、分散グループは表示されません。Active Directory の分散グループはセキュリティ対応でないため、ユーザの集合に電子メールを送信するために電子メール アプリケーションで使用することしかできません。分散グループの詳細については、Microsoft のマニュアルを参照してください。
- ACS が外部 ID ストアの 1015 グループ以上に属するユーザを認証しようとすると、Active Directory でログイン認証が失敗することがあります。これは、Active Directory のローカル セキュリティ認証（LSA）の制限によるものです。

関連項目

- AD 属性の設定（8-75 ページ）
- マシン アクセス制限の設定（8-77 ページ）
- 高度な調整（8-78 ページ）
- 認証ドメインの設定（8-78 ページ）
- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

AD 属性の設定

このページは、ポリシー条件に使用できる属性を選択する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Directory Attributes] タブをクリックします。

ステップ 2　表 8-19 の説明に従って、[Active Directory: Attributes] ページのフィールドに入力します。

表 8-19　[Active Directory: Attributes] ページ

オプション	説明
Name of example Subject to Select Attributes	追加されたドメインで見つかったユーザまたはコンピュータの名前を入力します。ユーザまたはコンピュータの CN または識別名を入力できます。 表示される属性のセットは、指定するサブジェクトに所属します。属性のセットは、ユーザおよびコンピュータごとに異なります。
Select	[Attributes] セカンダリ ウィンドウにアクセスする場合にクリックします。このウィンドウには、上記のフィールドに入力した名前の属性が表示されます。
Attribute Name List：セカンダリ [Selected Attributes] ウィンドウで選択した属性が表示されます。複数の属性を選択し、同時に送信できます。	
Attribute Name	• 次のいずれかを実行します。 – 属性の名前を入力します。 – リストから属性を選択し、[Edit] をクリックして属性を編集することもできます。 • [Add] をクリックして、属性を [Attribute Name list] に追加します。
Type	属性名に関連付けられた属性タイプ。有効なオプションは次のとおりです。 • 文字列 • 整数 64 • IP Address：IPv4 または IPv6 アドレスを指定できます。 • Unsigned Integer 32 • ブール
Default	選択した属性に対して指定されている属性デフォルト値。 • String：属性名。 • Integer 64：0 • Unsigned Integer 64：0。 • IP Address：デフォルト設定なし。 • Boolean：デフォルト設定なし。
Policy Condition Name	この属性のカスタム条件名を入力します。たとえば、カスタム条件名が *AAA* の場合は、このフィールドに **AAA** を入力します。**AD1:*att_name*** ではありません。
[Select Attributes] セカンダリ ウィンドウ	[Attributes] セカンダリ ウィンドウからだけ使用できます。
Search Filter	ユーザ名またはマシン名を指定します。 • ユーザ名の場合、認定者名、SAM、NetBios、または UPN フォーマットを指定できます。 • マシン名の場合、MACHINE$、NETBiosDomain\MACHINE$、host/MACHINE、または host/machine.domain フォーマットのいずれかを指定できます。ユーザ名およびマシン名には英語以外の文字を指定できます。
Attribute Name	上記のフィールドで入力したユーザ名またはマシン名の属性の名前。
Attribute Type	属性のタイプ。
Attribute Value	指定したユーザまたはマシンの属性の値。

ステップ 3　次のいずれかを実行します。

- [Save Changes] をクリックして、設定を保存します。
- すべての変更を破棄するには、[Discard Changes] をクリックします。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[Clear Configuration] をクリックします。

関連項目

- マシン アクセス制限の設定（8-77 ページ）
- 高度な調整（8-78 ページ）
- 認証ドメインの設定（8-78 ページ）
- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

マシン アクセス制限の設定

マシン アクセス制限を設定するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択してから、[Machine Access Restrictions] タブをクリックします。

ステップ 2　表 8-20 の説明に従って、[Active Directory: Machine Access Restrictions] ページのフィールドに入力します。

表 8-20　[Active Directory: Machine Access Restrictions] ページ

オプション	説明
Enable Machine Access Restrictions	Web インターフェイスでのマシン アクセス制限の制御をイネーブルにするには、このチェックボックスをチェックします。これにより、マシン認証結果がユーザの認証および認可に結び付けられます。この機能をイネーブルにした場合は、[Aging time] を設定する必要があります。
Aging time (hours)	マシンが認証されたあと、そのマシンからユーザを認証できる時間。この時間が経過すると、ユーザ認証は失敗します。デフォルト値は 6 時間です。有効な範囲は 1 ～ 8760 時間です。
MAR Cache Distribution	
Cache entry replication timeout	キャッシュ エントリのレプリケーションがタイムアウトする時間を秒単位で入力します。デフォルト値は 5 秒です。有効な範囲は 1 ～ 10 です。
Cache entry replication attempts	ACS が MAR キャッシュ エントリのレプリケーションを実行しなければならない回数を入力します。デフォルト値は 2 です。有効な範囲は 0 ～ 5 です。
Cache entry query timeout	キャッシュ エントリのクエリーがタイムアウトする時間を秒単位で入力します。デフォルト値は 2 秒です。有効な範囲は 1 ～ 10 です。
Cache entry query attempts	ACS がキャッシュ エントリのクエリーを実行しなければならない回数を入力します。デフォルト値は 1 です。有効な範囲は 0 ～ 5 です。

表 8-20　[Active Directory: Machine Access Restrictions] ページ（続き）

オプション	説明
Node	この AD ドメインに接続されているすべてのノードが表示されます。
Cache Distribution Group	選択したノードのキャッシュ分散グループを入力します。ここには、最大 64 文字のテキスト文字列を入力できます。キャッシュ分散グループには特殊文字の「(」と「)」は使用できません。

ステップ 3　次のいずれかを実行します。

- [Save Changes] をクリックして、設定を保存します。
- すべての変更を破棄するには、[Discard Changes] をクリックします。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[**Clear Configuration**] をクリックします。

関連項目

- 高度な調整（8-78 ページ）
- 認証ドメインの設定（8-78 ページ）
- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

高度な調整

高度な調整機能により、ノード固有の変更および設定が可能となり、システムのさらに深いレベルでパラメータを調整できます。このページでは、優先ドメイン コントローラ、グローバル カタログ、ドメイン コントローラのフェールオーバー パラメータ、およびタイムアウトを設定できます。このページには、暗号化の無効化など、トラブルシューティング オプションもあります。これらの設定は、通常の管理フローを対象としていません。シスコ サポートのガイダンスのみに従って使用する必要があります。

関連項目

- 認証ドメインの設定（8-78 ページ）
- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

認証ドメインの設定

ACS を Active Directory ドメインに参加させると、ACS では信頼関係のある他のドメインが可視化されます。デフォルトでは、ACS はそうした信頼ドメインすべてに対し、認証を許可します。Active Directory 展開と対話している間は、ACS を認証ドメインのサブセットに限定することもできます。認証ドメインを設定すると、特定のドメインを選択し、選択したドメインに対してのみ認証が実行されるようにできます。認証ドメインでは、参加ポイントで信頼されたすべてのドメインではなく、選択したドメインのユーザのみを認証するよう ACS に指示するので、セキュリティが向上します。また、認証ドメインでは検索範囲が制限される（着信したユーザ名または ID に一致するアカウントが検索される）ため、認証要求処理のパフォーマン

スと遅延が改善されます。このことは、着信したユーザ名または ID にドメイン マークアップ（プレフィックスまたはサフィックス）が含まれていない場合、特に重要です。これらの理由から、認証ドメインを設定することをベスト プラクティスとして強く推奨します。

認証ドメインを設定するには、次の手順を実行します。

はじめる前に

ACS インスタンスが Active Directory ドメインに参加していることを確認します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Authentication Domains] タブをクリックします。

テーブルに、信頼ドメインのリストが表示されます。デフォルトでは、ACS はすべての信頼ドメインに対する認証を許可します。

ステップ 2　指定したドメインのみを許可するには、認証を許可するドメインの隣にあるチェックボックスをオンにし、[Enable Selected] をクリックします。

ステップ 3　[Save Changes] をクリックします。

[Authenticate] 列で、選択したドメインのステータスが「Yes」に変わります。

関連項目

- Active Directory の問題の診断（8-79 ページ）
- Active Directory のアラームおよびレポート（8-80 ページ）

Active Directory の問題の診断

診断ツールは、各 ACS ノードで実行するサービスです。診断ツールを使用すると、Active Directory 展開を自動的にテストおよび診断したり、ACS が Active Directory を使用するときに機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

ACS が Active Directory に参加できない、または Active Directory で認証されない理由は、複数あります。このツールは、ACS を Active Directory に接続するための前提条件が正しく設定されているようにするのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザ認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明するガイドとして機能し、各レイヤの問題を（必要に応じて）途中で修正するのに役立ちます。

次の 3 つのテストは、ACS を Active Directory に参加させなくても実行でき、Active Directory デーモンが正しく実行しているかどうかを確認できます。

- System health - check AD service
- System health - check DNS configuration
- System health - check NTP

ACS を Active Directory に参加させたら、次のテストが実行可能になります。

- DNS A record high level API query
- DNS A record low level API query
- DNS SRV record query
- DNS SRV record size
- LDAP test AD site association

- LDAP test DCs availability
- LDAP test DCs response time
- LDAP test - DC locator
- LDAP test - GC locator
- Kerberos test obtaining join point TGT
- Kerberos test bind and query to ROOT DSE
- Kerberos check SASL connectivity to AD

Active Directory の問題を診断するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Diagnostic Tools] タブをクリックします。

Active Directory のドメイン機能を確認するために ACS で実行可能なすべてのテストのリストが [Diagnostic Tools] タブに表示されます。

ステップ 2　実行するテストの横にあるチェックボックスをオンにします。複数のボックスを選択できます。

ステップ 3　次のいずれかをクリックします。

- 選択したテストのみを実行するには、[Run Selected Tests]。
- すべてのテストを実行するには、[Run All Tests]。
- ACS ですべてのテストの実行を停止するには、[Stop All Running Tests]。

テスト結果は [Result and Remedy] 列に表示されます。

関連項目

Active Directory のアラームおよびレポート（8-80 ページ）

Active Directory のアラームおよびレポート

アラーム

ACS 5.8 では、Active Directory に関連するアクティビティをモニタしてトラブルシューティングを実行するためのさまざまなアラームおよびレポートが導入されています。

次のような Active Directory のエラーおよび問題に対して、アラームがトリガーされます。

- 設定したネーム サーバが使用できない
- 参加したドメインが使用できない
- 認証ドメインが使用できない
- Active Directory フォレストが使用できない
- AD コネクタを再起動する必要があった
- AD：ACS アカウント パスワードの更新に失敗した
- AD：マシン TGT の更新に失敗した

レポート

次の 2 つのレポートで、Active Directory に関連するアクティビティをモニタできます。

- RADIUS Authentications Report：このレポートは、Active Directory の RADIUS 認証および許可に関する詳細な手順が示されています。このレポートは [Launch Monitoring and Report Viewer] > [Monitoring and Reports] > [Reports] > [ACS Reports] > [AAA Protocol] > [RADIUS Authentications] で確認できます。
- TACACS+ Authentications Report：このレポートは、Active Directory の TACACS+ 認証および許可に関する詳細な手順が示されています。このレポートは [Launch Monitoring and Report Viewer] > [Monitoring and Reports] > [Reports] > [ACS Reports] > [AAA Protocol] > [TACACS Authentications] で確認できます。
- AD Connector Operations Report：AD Connector Operations Report には、ACS サーバのパスワード更新、Kerberos チケットの管理、DNS クエリー、DC 検出、LDAP、および RPC 接続管理など、AD コネクタによって実行されるバックグラウンド操作のログが示されています。Active Directory の障害が発生した場合、このレポートの詳細を確認することで、考えられる原因を特定することができます。このレポートは [Launch Monitoring and Report Viewer] > [Monitoring and Reports] > [Reports] > [ACS Reports] > [ACS Instance] > [AD Connector Operations] で確認できます。

(注)　多数のグループに属するユーザの最初の認証がタイムアウト エラーで失敗することがあります。しかし、同じユーザまたは同じグループに属する他のユーザの後続の認証は適切に動作します。

ドメイン コントローラへの ACS の結合

ACS でドメイン コントローラまたはグローバル カタログを接続する必要がある場合、ACS は SRV 要求を設定済みの DNS サーバに送信し、ドメインのドメインコントローラの使用可能リストと、フォレストのグローバルカタログを検索します。

ACS マシンの Active Directory コンフィギュレーションがサイトに割り当てられ、それがサイトに割り当てられている場合、ACS は対象の DNS クエリーをサイトに送信します。つまり、DNS サーバは、サブネットが割り当てられているその特定のサイトにサービスを提供しているドメイン コントローラとグローバル カタログを返すことが前提となっています。

ACS マシンがサイトに割り当てられていない場合、ACS は対象の DNS クエリーをサイトに送信しません。つまり、サイトに関係なく、使用可能なすべてのドメイン コントローラとグローバル カタログを返すことが前提となっています。

ACS はドメイン コントローラまたはグローバル カタログのリストを繰り返し、DNS サーバから受け取った DNS 応答のドメイン コントローラまたはグローバル カタログの順序に従って、接続を確立しようとします。

関連項目

- RSA SecurID サーバ（8-81 ページ）
- RADIUS ID ストア（8-88 ページ）

RSA SecurID サーバ

ACS では、外部データベースとして RSA SecurID サーバがサポートされています。RSA SecurID の 2 要素認証は、ユーザの Personal Identification Number（PIN）と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別登録の RSA SecurID トークンとで構成されます。

異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。

そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザである確実性が高くなります。したがって、RSA SecurID サーバでは、従来の再利用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザは、RSA のネイティブ プロトコルによってユーザ名およびパスコードで認証されます。
- RADIUS プロトコルの使用：ユーザは、RADIUS プロトコルによってユーザ名およびパスコードで認証されます。

ACS 5.8 の RSA SecurID トークン サーバは、RSA SecurID エージェントを使用して RSA SecurID 認証テクノロジーと統合します。

RSA SecurID エージェントの設定

RSA SecurID サーバ管理者は、次のことを実行できます。

- エージェント レコード（sdconf.rec）の作成（8-82 ページ）
- ノード秘密（SecurID）のリセット（8-82 ページ）
- 自動ロード バランシングの無効化（8-83 ページ）
- 手動介入によるダウンした RSA SecurID サーバの削除（8-83 ページ）
- パスコードのキャッシング（8-83 ページ）

エージェント レコード（sdconf.rec）の作成

ACS 5.8 の RSA SecurID トークン サーバを設定するには、ACS 管理者に *sdconf.rec* ファイルが必要です。*sdconf.rec* ファイルは、RSA エージェントと RSA SecurID サーバ領域との通信方法を指定する設定レコード ファイルです。

sdconf.rec ファイルを作成するために、RSA SecurID サーバ管理者は、RSA SecurID サーバ上のエージェント ホストとして ACS ホストを追加し、このエージェント ホストの設定ファイルを生成する必要があります。

ノード秘密（SecurID）のリセット

エージェントが最初に RSA SecurID サーバと通信してから、サーバは SecurID というノード秘密ファイルをエージェントに提供します。サーバとエージェント間のその後の通信は、ノード秘密の交換による相手の認証の確認によって行われます。

ノード秘密をリセットする必要がある場合があります。ノード秘密をリセットするには、次の手順を実行します。

- RSA SecurID サーバ管理者は、RSA SecurID サーバの Agent Host レコードの [Node Secret Created] チェックボックスをオフにする必要があります。
- ACS 管理者は、SecurID ファイルを ACS から削除する必要があります。

自動ロード バランシングの無効化

RSA SecurID エージェントでは、RSA SecurID サーバ上の要求された負荷は領域内で自動的に分散されます。ただし、負荷を手動で分散するオプションがあります。エージェント ホストが認証要求を一部のサーバに他のサーバよりも頻繁に送信するように、各エージェント ホストが使用する必要があるサーバを指定し、各サーバに優先順位を割り当てることができます。

優先順位設定をテキスト ファイルに指定し、sdopts.rec として保存する必要があります。それを ACS にアップロードできます。

手動介入によるダウンした RSA SecurID サーバの削除

RSA SecurID サーバがダウンした場合、自動除外メカニズムが迅速に機能しないことがあります。このプロセスを迅速化するために、*sdstatus.12* ファイルを ACS から削除できます。

パスコードのキャッシング

パスコードのキャッシングにより、RSA SecurID サーバで複数の認証を同じパスコードを使用して実行することが可能になります。

ACS 5.8 では、キャッシュのパスコードでユーザを保存します。ユーザおよびパスコードは RSA SecurID サーバでの認証成功後にキャッシュに格納されます。RSA SecurID サーバでの認証時に、ACS はキャッシュの認証ユーザとパスコードの検索を試行します。見つからない場合、ACS は RSA SecurID サーバで認証します。

ACS のパスコード キャッシュは 1 ～ 300 秒で設定可能な時間の間使用できます。キャッシュの RSA SecurID サーバ パスコード エントリは、ユーザが設定した時間の間使用できます。この期間内にユーザは同じパスコードでインターネットにアクセスできます。

RSA SecurID トークン サーバの作成および編集

ACS 5.8 では、ワンタイム パスワードによるセキュリティを向上させるために、ユーザ認証用の RSA SecurID トークン サーバがサポートされています。RSA SecurID トークン サーバによって、ユーザの認証を確実にする 2 要素認証が提供されます。

RSA ID ストアに対してユーザを認証するには、最初に ACS で RSA SecurID トークン サーバを作成し、領域、ACS インスタンス、および高度な設定を設定する必要があります。

ACS 5.8 では、1 つの RSA 領域だけがサポートされています。RSA 領域設定を設定できます。1 つの領域に数多くの ACS インスタンスを含めることができます。

（注）　RSA SecurID サーバ管理者から *sdconf.rec* ファイルを受け取り、ACS に保存する必要があります。

RSA SecurID トークン サーバを作成または編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [RSA SecurID Token Servers] を選択します。

[RSA SecurID Token Servers] ページが表示されます。

ステップ 2　[Create] をクリックします。

変更する ID ストア名をクリックするか、名前の隣にあるボックスをオンにして [Edit] をクリックすることもできます。

ステップ 3　表 8-21 の説明に従って、[RSA Realm Settings] タブのフィールドに入力します。

表 8-21　[RSA Realm Settings] タブ

オプション	説明
General	
Name	RSA 領域の名前。
Description	（任意）RSA 領域の説明。
Server Connection	
Server Timeout *n* seconds	タイムアウトまでに、ACS は RSA SecurID トークン サーバへの接続を *n* 秒間待機します。
Reauthenticate on Change PIN	変更 PIN で再認証する場合に、このチェックボックスをオンにします。
Realm Configuration File	
Import new ‘sdconf.rec’ file	[Browse] をクリックして、マシンから *sdconf.rec* ファイルを選択します。
Node Secret Status	ユーザが RSA SecurID トークン サーバに対して最初に認証されると、[Node Secret Status] に [Created] と表示されます。

ステップ 4　[ACS Instance Settings] タブをクリックします。詳細については、「ACS インスタンス設定の設定（8-84 ページ）」を参照してください。

ステップ 5　[Advanced] タブをクリックします。詳細については、「高度なオプションの設定（8-87 ページ）」を参照してください。

ステップ 6　[Submit] をクリックして、RSA SecurID ストアを作成します。

設定したサーバが含まれた [RSA SecurID Token Server] ページが表示されます。

関連トピック：

- RSA SecurID サーバ（8-81 ページ）
- ACS インスタンス設定の設定（8-84 ページ）
- 高度なオプションの設定（8-87 ページ）

ACS インスタンス設定の設定

[ACS Instance Settings] タブには、アクティブな ACS インスタンスの最新のリストが表示されます。これらのエントリを追加または削除することはできません。ただし、これらの ACS インスタンスそれぞれの使用可能な RSA 領域設定は編集できます。

表 8-22 に、[ACS Instance Settings] タブのフィールドを示します。

表 8-22　[ACS Instance Settings] タブ

オプション	説明
ACS Instance	ACS インスタンスの名前。
Options File	オプション ファイルの名前。

表 8-22　[ACS Instance Settings] タブ

オプション	説明
Node Secret Status	ノード秘密のステータス。次のいずれかになります。 • Created • Not created

このページに表示される ACS インスタンスの設定を編集できます。目的

ステップ 1　編集する ACS インスタン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。

[ACS instance settings] ダイアログボックスが表示されます。このダイアログボックスには、次のタブがあります。

- RSA Options File：詳細については、ACS インスタンス設定の編集（8-85 ページ）を参照してください。
- Reset Agents Files：詳細については、ACS インスタンス設定の編集（8-85 ページ）を参照してください。

ステップ 2　[OK] をクリックします。

関連項目

- RSA SecurID サーバ（8-81 ページ）
- RSA SecurID トークン サーバの作成および編集（8-83 ページ）
- ACS インスタンス設定の編集（8-85 ページ）
- ACS インスタンス設定の編集（8-85 ページ）
- 高度なオプションの設定（8-87 ページ）

ACS インスタンス設定の編集

ACS インスタンス設定を編集して、次のことを実行できます。

- RSA オプション ファイルのイネーブル化（8-85 ページ）
- エージェント ファイルのリセット（8-86 ページ）

RSA オプション ファイルのイネーブル化

各 ACS インスタンスで RSA オプション ファイル（*sdopts.rec*）をイネーブルにして、領域内の RSA エージェントと RSA サーバ間の接続のルーティング優先順位を制御できます。

表 8-23 に、[RSA Options File] タブのフィールドを示します。

表 8-23　[RSA Options File] タブ

オプション	説明
各 ACS インスタンスで RSA オプション ファイル（sdopts.rec）をイネーブルにして、領域内の RSA エージェントと RSA サーバ間の接続のルーティング優先順位を制御できます。sdopts.rec のフォーマットの詳細については、RSA のマニュアルを参照してください。	
Use the Automatic Load Balancing status maintained by the RSA Agent	RSA エージェントが保持する自動ロード バランシング ステータスを使用する場合に、このオプションを選択します。

表 8-23　[RSA Options File] タブ

オプション	説明
Override the Automatic Load Balancing status with the sdopts.rec file selected below	sdopts.rec ファイルで指定される自動ロード バランシング ステータスを使用する場合に、このオプションを選択します。
Current File	現在選択されている sdopts.rec ファイルが表示されます。
Time stamp	sdopts.rec ファイルが最後に変更された時刻。
File Size	sdopts.rec ファイルのサイズ。
Import new ‘sdopts.rec’ file	[Browse] をクリックして、ハード ドライブから新しい sdopts.rec ファイルをインポートします。
（注） このポップアップを起動したページが送信されるまで、変更は有効になりません。	

次のいずれかを実行します。

- [OK] をクリックしてコンフィギュレーションを保存します。
- 領域内のアクティブおよび非アクティブ サーバの秘密キー情報またはステータスをリセットするには、[Reset Agent Files] タブをクリックします。

関連項目

- RSA SecurID サーバ（8-81 ページ）
- RSA SecurID トークン サーバの作成および編集（8-83 ページ）
- ACS インスタンス設定の設定（8-84 ページ）
- ACS インスタンス設定の編集（8-85 ページ）
- 高度なオプションの設定（8-87 ページ）

エージェント ファイルのリセット

このページは、次の項目をリセットする場合に使用します。

- ノード秘密キー ファイル。RSA サーバとの通信が暗号化されるようにします。
- 領域内のサーバのステータス。

ステップ 1　次のオプションのいずれかを選択します。

- エージェント ホストのノード秘密をリセットするには、[Remove secure id file on submit] チェックボックスをオンにします。

  エージェント ホストのノード秘密をリセットする場合、RSA サーバでエージェント ホストのノード秘密をリセットする必要があります。
- 領域内のサーバのステータスをリセットするには、[Remove sdstatus.12 file on submit] チェックボックスをオンにします。

ステップ 2　[OK] をクリックします。

関連項目

- RSA SecurID サーバ（8-81 ページ）
- RSA SecurID トークン サーバの作成および編集（8-83 ページ）
- ACS インスタンス設定の設定（8-84 ページ）

- ACS インスタンス設定の編集（8-85 ページ）
- 高度なオプションの設定（8-87 ページ）

高度なオプションの設定

このページは、次のことを実行する場合に使用します。

- RSA SecurID トークン サーバからのアクセス拒否がどのような意味を持つかを定義します。
- ID キャッシングのイネーブル化：RSA でのユーザのキャッシングは、キャッシングのロジックと目的が同じであるため、RADIUS トークンでのユーザのキャッシングと似ています。唯一の違いは、RSA ではユーザの属性取得がないため、属性のキャッシングがないことです。認証されたユーザはキャッシュされますが、属性はキャッシュされません。
- Enable passcode caching：このオプションは、RAS セキュア ID トークンでの認証が最初に成功した後にパスコードを保存し、設定した期間内に後続の認証が発生した場合にその認証にキャッシュされたユーザ クレデンシャルを使用します。

RSA 領域の高度なオプションを設定するには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- **[Treat Rejects as Authentication failed]** オプション ボタンをクリック：ACS はこれを RSA SecurdID ストアからの認証拒否を解釈し、認証失敗として見なします。
- [Treat Rejects as User not found] オプション ボタンをクリック：ACS はこれを RSA SecurID ストアからの認証拒否と解釈し、「user not found」と見なします。

ステップ 2　[Enable identity caching] チェックボックスをオンにします。

ID キャッシングをイネーブルにして、RSA サーバによって認証されない要求を ACS で処理できるようにします。

最後に成功した認証から取得された結果が、指定された時間、キャッシュ内で使用可能になります。

ステップ 3　エージング タイムを分単位で入力します。

ID キャッシュには、ここで指定した時間だけ、成功したログインの結果が格納されます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。

ステップ 4　[Enable passcode caching] チェックボックスをオンにします。

パスコード キャッシングをイネーブルにし、ACS がパスコードをキャッシュし、ユーザが指定された期間に同じパスコードでネットワークへアクセスできるようにします。

ステップ 5　エージング タイムを秒単位で入力します。

パスコード キャッシュには、ここで指定した時間だけ、成功したログインの結果が格納されます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

ステップ 6　[Submit] をクリックします。

（注）　RSA ID サーバおよび RSA SecurID サーバを外部 ID ソースとして、ユーザおよび管理者を認証する際、次の場合に ACS によって ACS View に「InvalidPassword」というエラーメッセージが表示されます。
1）無効なパスワードが入力されている場合
2）外部 ID ストアでユーザが無効になっている場合
3）外部 ID ストアにユーザが存在しない場合

関連項目

- RSA SecurID サーバ（8-81 ページ）
- RSA SecurID トークン サーバの作成および編集（8-83 ページ）
- ACS インスタンス設定の設定（8-84 ページ）
- ACS インスタンス設定の編集（8-85 ページ）
- 高度なオプションの設定（8-87 ページ）

RADIUS ID ストア

RADIUS サーバは、RADIUS インターフェイスをサポートするサードパーティ製サーバです。ACS の一部である RADIUS ID ストアは、RADIUS サーバに接続されます。

RADIUS サーバとは、標準 RADIUS インターフェイスが組み込まれたサーバ、および RADUIS インターフェイスをサポートするその他のサーバのことです。ACS 5.8 では、RADIUS RFC 2865 準拠の任意のサーバが外部 ID ストアとしてサポートされています。ACS 5.8 では、複数の RADIUS トークン サーバ ID がサポートされています。

たとえば、RSA SecurID サーバや SafeWord サーバなどです。RADIUS ID ストアは、ユーザを認証するために使用される任意の RADIUS トークン サーバと連携できます。RADIUS ID ストアでは、認証セッションに UDP ポートが使用されます。すべての RADIUS 通信に同じ UDP ポートが使用されます。

（注）　ACS で RADIUS メッセージを RADIUS 対応サーバに正常に送信するには、RADIUS 対応サーバと ACS の間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、ACS Web インターフェイスを介して設定できます。

ここでは、次の内容について説明します。

- サポートされる認証プロトコル（8-88 ページ）
- フェールオーバー（8-89 ページ）
- パスワード プロンプト（8-89 ページ）
- ユーザ グループ マッピング（8-89 ページ）
- グループおよび属性マッピング（8-89 ページ）
- ID 順序での RADIUS ID ストア（8-90 ページ）
- 認証失敗メッセージ（8-90 ページ）
- Safeword サーバでのユーザ名の特殊フォーマット（8-90 ページ）
- ユーザ属性キャッシュ（8-91 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）

サポートされる認証プロトコル

ACS では、RADIUS ID ストアに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- TACACS+ ASCII/PAP
- 内部 EAP-GTC を含む PEAP
- 内部 EAP-GTC を含む EAP-FAST

フェールオーバー

ACS 5.8 では、複数の RADIUS ID ストアを設定できます。各 RADIUS ID ストアには、プライマリ RADIUS サーバとセカンダリ RADIUS サーバを指定できます。ACS からプライマリ サーバに接続できない場合は、セカンダリ サーバが使用されます。

パスワード プロンプト

RADIUS ID ストアでは、パスワード プロンプトを設定できます。パスワード プロンプトは、ACS Web インターフェイスを介して設定できます。

ユーザ グループ マッピング

ACS 4.x で使用できるユーザ単位のグループ マッピング機能を提供するために、ACS 5.8 では、RADIUS ID ストアによって認証されるユーザの属性取得および認可メカニズムが使用されます。

このために、[009\001] cisco-av-pair 属性を含む認証応答を返すように RADIUS ID ストアを設定する必要があります。属性の値は次のとおりです。

ACS:CiscoSecure-Group-Id=*N*。ここで、*N* は、ACS によってユーザに割り当てられる 0 ～ 499 の任意の ACS グループ番号です。

この属性は、認可およびグループ マッピング規則の作成時に ACS Web インターフェイスのポリシー設定ページで使用できます。

グループおよび属性マッピング

RADIUS ID ストアに対する認証中に取得された RADIUS 属性を、認可およびグループ マッピングの ACS ポリシー条件で使用できます。RADIUS ID ストアを設定するときに、ポリシー条件で使用する属性を選択できます。これらの属性は、RADIUS ID ストア専用ディクショナリに保持され、ポリシー条件を定義するために使用できます。

（注） 要求された属性を RADIUS サーバに問い合わせることはできません。要求された属性を返すように RADIUS ID ストアを設定できるだけです。これらの属性は、Access-Accept 応答で属性リストの一部として使用できます。

ACS 5.8 の属性サブスクリプション機能を使用して、デバイスへの ACS 応答の RADIUS ID ストア属性を受信できます。次の RADIUS 属性が返されます。

- RADIUS RFS にリストされている属性
- ベンダー固有属性

次の属性タイプがサポートされています。

- String
- Unsigned Integer
- IP Address
- Enumeration

複数の値を持つ属性が返される場合、値は無視され、デフォルト値が設定されている場合はその値が返されます。ただし、この属性は問題がある属性としてカスタマー ログでレポートされます。

ID 順序での RADIUS ID ストア

ID 順序で認証順序用の RADIUS ID ストアを追加できます。ただし、属性取得順序用の RADIUS ID ストアを追加することはできません。これは、認証しないで RADIUS ID ストアを問い合わせることはできないためです。ACS では、RADIUS サーバによる認証中に、異なるエラー状況を区別できません。

すべてのエラー状況に対して RADIUS サーバから Access-Reject メッセージが返されます。たとえば、RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

ただし、ACS Web インターフェイスの RADIUS ID ストアのページで使用できる [Treat Rejects as Authentication Failure] または [Treat Rejects as User Not Found] オプションをイネーブルにすることができます。

認証失敗メッセージ

RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは Access-Reject メッセージが返されます。ACS には、ACS Web インターフェイスを使用して、このメッセージを Authentication Failed または Unknown User として設定するオプションがあります。

ただし、このオプションでは、ユーザが未知の状況だけでなく、すべての失敗状況に対して Unknown User メッセージが返されます。

表 8-24 に、RADIUS ID サーバで発生するさまざまな失敗状況を示します。

表 8-24　　エラー処理

認証失敗の原因	失敗状況
認証失敗	• ユーザが未知である。 • ユーザが不正なパスコードでログインしようとしている。 • ユーザ ログイン時間が期限切れになった。
プロセスの失敗	• RADIUS サーバが ACS で正しく設定されていない。 • RADIUS サーバが使用できない。 • RADIUS パケットが偽装として検出されている。 • RADIUS サーバとのパケットの送受信の問題。 • タイムアウト。
未知ユーザ	認証が失敗し、'Fail on Reject' オプションが false に設定されている。

Safeword サーバでのユーザ名の特殊フォーマット

Safeword トークン サーバでは、次のユーザ名フォーマットでの認証がサポートされています。

ユーザ名：Username, OTP

ACS により、ユーザ名が解析されて次のように変換されます。

ユーザ名：Username

Safeword トークン サーバでは、両方のフォーマットがサポートされています。ACS はさまざまなトークン サーバと連携します。Safeword サーバを設定する場合、ACS でユーザ名を解析して指定のフォーマットに変換するには、[Safeword Server] チェックボックスをオンにする必要があります。

この変換は、要求が RADIUS トークン サーバに送信される前に、RADIUS トークン サーバ ID ストアで実行されます。

ユーザ属性キャッシュ

RADIUS トークン サーバでは、デフォルトではユーザ ルックアップはサポートされていません。ただし、ユーザ ルックアップは次の ACS 機能に不可欠です。

- PEAP セッション再開：認証の成功後、EAP セッションの確立中に発生
- EAP/FAST 高速再接続：認証の成功後、EAP セッションの確立中に発生
- T+ 認可：T+ 認証の成功後に発生

ACS では、これらの機能のユーザ ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の ACS ノード間で複製されません。ACS Web インターフェイスを介してキャッシュの存続可能時間（TTL）制限を設定できます。ID キャッシング オプションを有効にし、エージング タイムを分単位で設定する必要があります。指定した時間、キャッシュはメモリで使用可能です。

パスコードのキャッシング

パスコードのキャッシングにより、同じパスコードを使用して RADIUS ID サーバと複数の認証を実行することが可能になります。

ACS 5.8 では、キャッシュのパスコードでユーザを保存します。ユーザおよびパスコードは RADIUS ID サーバとの認証の成功後にキャッシュに格納されます。RADIUS ID サーバでの認証時に、ACS はキャッシュの認証ユーザとパスコードを検索しようとします。見つからない場合、ACS は RADIUS ID サーバで認証します。

ACS のパスコード キャッシュは 1 ～ 300 秒で設定可能な時間の間使用できます。キャッシュの RADIUS ID サーバ パスコード エントリはユーザが設定した時間の間使用できます。この期間内にユーザは同じパスコードでインターネットにアクセスできます。

RADIUS ID サーバの作成、複製、および編集

ACS 5.8 では、ワンタイム パスワードによるセキュリティを向上させるために、外部 ID ストアとして RADIUS ID サーバがサポートされています。RADIUS ID サーバによって、ユーザの認証を確実にする 2 要素認証が提供されます。

RADIUS ID ストアに対してユーザを認証するには、最初に ACS で RADIUS ID サーバを作成し、RADIUS ID ストア設定を設定する必要があります。ACS 5.8 では、次の認証プロトコルがサポートされています。

- RADIUS PAP
- TACACS+ ASCII\PAP
- 内部 EAP-GTC を含む PEAP
- 内部 EAP-GTC を含む EAP-FAST

RADIUS ID サーバでの正常な認証には、次のことが必要です。

- RADIUS ID サーバと ACS との間のゲートウェイ デバイスで、UDP ポートを介した通信が許可されている。
- ACS Web インターフェイスで RADIUS ID サーバに対して設定する共有秘密情報が、RADIUS ID サーバ上で設定されている共有秘密情報と同一である。

RADIUS ID 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　[Users and Identity Stores] > [External Identity Stores] > [RADIUS Identity Servers] を選択します。

[RADIUS Identity Servers] ページが表示され、RADIUS 外部 ID サーバのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID ストア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 ID ストア名をクリックします。または、名前の隣にあるボックスをオンにして [Edit] をクリックします。

ステップ 3　[General] タブのフィールドに入力します。[General] タブのフィールドについては、一般設定（8-92 ページ）を参照してください。

ステップ 4　次の作業を実行できます。

- [Submit] をクリックして RADIUS ID サーバを保存します。
- [Shell Prompts] タブをクリックします。[Shell Prompts] タブのフィールドについては、シェル プロンプトの設定（8-94 ページ）を参照してください。
- [Directory Attributes] タブをクリックします。[Directory Attributes] タブのフィールドについては、ディレクトリ属性の設定（8-95 ページ）を参照してください。
- [Advanced] タブをクリックします。[Advanced] タブのフィールドについては、高度なオプションの設定（8-96 ページ）を参照してください。

ステップ 5　[Submit] をクリックして変更を保存します。

関連項目

- RADIUS ID ストア（8-88 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）

一般設定

表 8-25 に、[RADIUS Identity Servers] ページの [General] タブのフィールドを示します。

表 8-25　[RADIUS Identity Server] - [General] タブ

オプション	説明
名前	外部 RADIUS ID サーバの名前。
説明	（任意）RADIUS ID サーバの簡単な説明。
SafeWord Server	SafeWord サーバを使用した 2 要素認証をイネーブルにする場合に、このチェックボックスをオンにします。
Server Connection	

表 8-25　[RADIUS Identity Server] - [General] タブ （続き）

オプション	説明
Enable Secondary Server	セカンダリ RADIUS ID サーバを、プライマリ RADIUS ID サーバに障害が発生したときにバックアップ サーバとして使用する場合に、このチェックボックスをオンにします。 セカンダリ サーバをイネーブルにする場合、セカンダリ RADIUS ID サーバのパラメータを設定する必要があり、次のオプションのいずれかを選択する必要があります。 • Always Access Primary Server First：ACS がセカンダリ サーバにアクセスする前に常にプライマリ RADIUS ID サーバにアクセスするようにするには、このオプションを選択します。 • Failback To Primary Server After *n* Minutes：ACS が認証にセカンダリ サーバを使用できる時間（分単位）を設定するには、このオプションを選択します。 この時間を過ぎると、ACS はプライマリ サーバを使用して認証を再試行する必要があります。デフォルト値は 5 分です。
Primary Server	
Server IP Address	プライマリ RADIUS ID サーバの IP アドレス。
Shared Secret	ACS とプライマリ RADIUS ID 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。
Authentication Port	サーバが受信に使用するポート番号。有効なオプションは 1 ～ 65,535 です。デフォルト値は 1812 です。
Server Timeout *n* Seconds	プライマリ サーバへの接続に失敗したと判断する前に ACS がプライマリ RADIUS ID サーバからの応答を待つ秒数 *n*。有効なオプションは 1 ～ 300 です。デフォルト値は 5 です。
Connection Attempts	セカンダリ RADIUS ID サーバに接続するか、セカンダリ サーバが設定されていない場合は接続をドロップする前に、ACS が再接続を試行する回数を指定します。有効なオプションは 1 ～ 10 です。デフォルト値は 3 です。
Secondary Server	
Server IP Address	セカンダリ RADIUS ID サーバの IP アドレス。
Shared Secret	ACS とセカンダリ RADIUS ID サーバ間の共有秘密情報。共有秘密情報は、RADIUS ID サーバ上で設定されている共有秘密情報と同一である必要があります。 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。
Authentication Port	RADIUS セカンダリ サーバが受信に使用するポート番号。有効なオプションは 1 ～ 65,535 です。デフォルト値は 1812 です。

表 8-25　[RADIUS Identity Server] - [General] タブ （続き）

オプション	説明
Server Timeout *n* Seconds	セカンダリ サーバへの接続に失敗したと判断する前に ACS がセカンダリ RADIUS ID サーバからの応答を待つ秒数 *n*。 有効なオプションは 1 ～ 300 です。デフォルト値は 5 です。
Connection Attempts	要求をドロップする前に ACS が再接続を試行する回数を指定します。有効なオプションは 1 ～ 10 です。デフォルト値は 3 です。

関連項目

- RADIUS ID ストア（8-88 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）
- シェル プロンプトの設定（8-94 ページ）
- ディレクトリ属性の設定（8-95 ページ）
- 高度なオプションの設定（8-96 ページ）

シェル プロンプトの設定

TACACS+ ASCII 認証の場合、ACS はパスワード プロンプトをユーザに返す必要があります。RADIUS ID サーバでは、この機能はパスワード プロンプト オプションによってサポートされています。ACS では、ACS Web インターフェイスの [Shell Prompts] ページで設定するプロンプトを使用できます。このプロンプトが空の場合、TACACS+ グローバル設定で設定されているデフォルトのプロンプトがユーザに表示されます。

RADIUS ID サーバとの接続を確立するときに、最初の要求パケットにパスワードが含まれていない場合があります。パスワードを要求する必要があります。このページを使用して、パスワードの要求に使用されるプロンプトを定義できます。目的

ステップ 1　プロンプトのテキストを [Prompt] フィールドに入力します。

ステップ 2　次のいずれかを実行します。

- パスワードを要求するプロンプトを設定するには、[Submit] をクリックします。
- ポリシー規則の条件で使用する属性のリストを定義するには、[Directory Attributes] タブをクリックします。詳細については、「ディレクトリ属性の設定（8-95 ページ）」を参照してください。

関連項目

- RADIUS ID ストア（8-88 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）
- 一般設定（8-92 ページ）
- ディレクトリ属性の設定（8-95 ページ）
- 高度なオプションの設定（8-96 ページ）

ディレクトリ属性の設定

RADIUS ID サーバが要求に応答するときに、RADIUS 属性が応答とともに返されます。これらの RADIUS 属性をポリシー規則で使用できます。

[Directory Attributes] タブで、ポリシー規則の条件で使用する RADIUS 属性を指定できます。ACS では、これらの属性のリストが個別に保持されます。

ステップ 1　表 8-26 の説明に従って、[Directory Attributes] タブのフィールドを変更します。

表 8-26　[RADIUS Identity Servers] - [Directory Attributes] タブ

オプション	説明
Attribute List	このセクションを使用して、ポリシー条件に含める対象リストを作成します。各属性を含めると、その名前、タイプ、デフォルト値、およびポリシー条件名がテーブルに表示されます。変更後： • RADIUS 属性を追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • RADIUS 属性を編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。テーブルの下のフィールドに RADIUS 属性のパラメータが表示されます。必要に応じて編集し、[Replace] をクリックします。
Dictionary Type	RADIUS ディクショナリ タイプ。ドロップダウン リスト ボックスをクリックして、RADIUS ディクショナリ タイプを選択します。
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、RADIUS 属性を選択します。この名前は、選択した属性が Cisco AV-Pair である場合、属性名と AV-pair をサポートする拡張子という 2 つの部分で構成されます。 たとえば、属性 **cisco-av-pair** と AV-pair 名 **some-avpair** の場合、ACS では **cisco-av-pair.some-avpair** と表示されます。 IETF およびベンダー VSA 属性名には、任意のサフィックス *-nnn* が含まれています。*nnn* は属性の ID です。
Type	RADIUS 属性タイプ。有効なオプションは次のとおりです。 • 文字列 • Unsigned Integer 32 • IPv4 アドレス
Default	（任意）RADIUS ID サーバからの応答の属性を使用できない場合に使用できるデフォルト値。この値は、指定した RADIUS 属性タイプである必要があります。
Policy Condition Name	この属性を使用するカスタム ポリシー条件の名前を指定します。

ステップ 2　次のいずれかを実行します。

- 変更を保存して [RADIUS Identity Servers] ページに戻るには、[Submit] をクリックします。
- 失敗メッセージ処理を設定し、ID キャッシングをイネーブルにするには、[Advanced] タブをクリックします。詳細については、「高度なオプションの設定（8-96 ページ）」を参照してください。

関連項目

- RADIUS ID ストア（8-88 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）
- 一般設定（8-92 ページ）
- シェル プロンプトの設定（8-94 ページ）
- 高度なオプションの設定（8-96 ページ）

高度なオプションの設定

[Advanced] タブでは、次のことを実行できます。

- RADIUS ID サーバからのアクセス拒否がどのような意味を持つかを定義します。
- ID キャッシングをイネーブルにします。
- パスコード キャッシングをイネーブルにします。

表 8-27 に、[RADIUS Identity Servers] ページの [Advanced] タブのフィールドを示します。

表 8-27　RADIUS ID サーバ : [Advanced] タブ

オプション	説明
この ID ストアでは、認証試行が拒否された場合に「認証失敗」と「ユーザが見つからない」は区別されません。次のオプションから、ID ポリシーの処理とレポートのために、ID ストアからのそのような認証拒否を ACS でどのように解釈するかを選択します。	
Treat Rejects as 'authentication failed'	不明瞭なアクセス拒否試行をすべて認証失敗と見なす場合に、このオプションをクリックします。
Treat Rejects as 'user not found'	不明瞭なアクセス拒否試行をすべて未知ユーザと見なす場合に、このオプションをクリックします。
ID キャッシングは、サーバに対する認証を実行しない要求の処理を許可するために使用されます。キャッシュには、サブジェクトの最後に成功した認証から取得された結果および属性が保持されます。	
Enable identity caching	ID キャッシングをイネーブルにする場合に、このチェックボックスをオンにします。ID キャッシングをイネーブルにする場合、ACS で ID キャッシュを保持する時間を分単位で入力する必要があります。
Aging Time *n* Minutes	ACS で ID キャッシュを保持する時間を分単位で入力します。有効なオプションは 1 ～ 1440 です。
Enable passcode caching	パスコード キャッシングをイネーブルにする場合に、このチェックボックスをオンにします。パスコード キャッシングをイネーブルにする場合、ACS で パスコード キャッシュを保持する時間を秒単位で入力する必要があります。
Aging Time *n* Seconds	ACS でパスコード キャッシュを保持する時間を秒単位で入力します。有効なオプションは 1 ～ 300 です。デフォルト値は 30 秒です。

[Submit] をクリックして RADIUS ID サーバを保存します。

関連項目

- RADIUS ID ストア（8-88 ページ）
- RADIUS ID サーバの作成、複製、および編集（8-91 ページ）

CA 証明書の設定

クライアントが EAP-TLS プロトコルを使用して ACS サーバに対して自身を認証する場合、自身を識別するクライアント証明書をサーバに送信します。クライアント証明書の ID および正確さを確認するために、サーバにはクライアント証明書をデジタル署名した Certificate Authority（CA; 認証局）からの証明書が事前にインストールされている必要があります。

ACS がクライアントの CA 証明書を信頼しない場合、ACS が信頼する上位レベル CA 証明書まで、連続して署名された CA 証明書のチェーン全体を ACS にインストールする必要があります。CA 証明書は、信頼証明書とも呼ばれます。

CA オプションを使用して、EAP-TLS 認証をサポートするデジタル証明書をインストールします。ACS は、X.509 v3 デジタル証明書標準を使用します。ACS は証明書の手動取得をサポートし、証明書信頼リスト（CTL）と Certificate Revocation List（CRL; 証明書失効リスト）を管理する手段も提供します。

デジタル証明書は、秘密情報も保存データベース クレデンシャルも共有する必要がありません。どちらも規模拡大が可能で、大きく展開しても信頼できます。正しく管理すれば、共有秘密システムより強力でセキュアな認証方式として動作させることができます。

相互信頼には、エンドユーザ クライアント側で確認できる証明書が ACS にインストールされている必要があります。このサーバ証明書は、CA から発行されたものを使用することもできますし、自己署名証明書を使用することもできます。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。

（注） ACS では、追加した CA 証明書で証明書チェーンが作成され、TLS ネゴシエーション中にこのチェーンが使用されます。サーバ証明書に署名した証明書を CA に追加する必要があります。チェーンが正しく署名され、すべての証明書が有効であることを確認する必要があります。

サーバ証明書およびサーバ証明書に署名した CA が ACS にインストールされている場合、ACS は証明書チェーン全体をクライアントに送信します。

（注） ACS はワイルドカード証明書をサポートしていません。

関連項目

- 認証局の追加（8-97 ページ）
- 認証局の編集および証明書失効リストの設定（8-98 ページ）
- 認証局の削除（8-100 ページ）
- 証明書チェーンの一部である CA 証明書の更新または削除（8-101 ページ）
- 認証局のエクスポート（8-102 ページ）

認証局の追加

サポートされている証明書形式は DER、PEM、CER です。

信頼できる認証局（CA）証明書を追加するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate] ページが表示されます。

ステップ 2　[Add] をクリックします。

ステップ 3　表 8-28 の説明に従って、[Certificate File to Import] ページのフィールドに入力します。

表 8-28　[Certificate Authority Properties] ページ

オプション	説明
Certificate File to Import	
Certificate File	証明書ファイルの名前を入力します。[Browse] をクリックして、信頼証明書があるクライアント マシン上の場所に移動します。
Trust for client with EAP-TLS	ACS が EAP プロトコルの証明書信頼リストを使用する場合に、このボックスをオンにします。
Allow Duplicate Certificates	同じ CN および SKI で、Valid From、Valid To、Serial numbers が異なる証明書の追加を許可します。
Description	CA 証明書の説明を入力します。

ステップ 4　[Submit] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Trust Certificate List] ページが表示されます。

関連項目

- ユーザ証明書認証（C-6 ページ）
- EAP-TLS の概要（C-6 ページ）

認証局の編集および証明書失効リストの設定

このページは、信頼できる認証局（CA）証明書を編集する場合に使用します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　変更する名前をクリックします。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。

表 8-29 の説明に従って、[Edit Trust Certificate List Properties] ページのフィールドに入力します。

ACS が CA CRL を遅延すると、CA は、ローカル ファイル システムに保存されます。CA は再送信するまで更新されません。

デフォルトでは、CRL が失効した CA のすべてのユーザ証明書が ACS で失敗します。

- CA 証明書が再送信されると、次のエラーが表示されます。*12514 EAP-TLS failed SSL/TLS handshake*これは、不明な CA が原因です。
- CA 証明書が再送信されていない場合、次のエラーが表示されます。*12515 EAP-TLS failed SSL/TLS handshake*。これは、期限切れの CRL が原因です。

[Ignore CRL Expiration] を選択した場合、失効した証明書の認証に失敗し、失効していない証明書の認証は成功します。

表 8-29　[Edit Certificate Authority Properties] ページ

オプション	説明
発行者	
Friendly Name	証明書に関連付けられている名前。
Description	（任意）CA 証明書の簡単な説明。
Issued To	*表示のみ。*証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	*表示のみ。*証明書を発行した認証局。
Valid from	*表示のみ。*証明書の有効開始日。X509 証明書は、開始日から終了日までの間（両方の日を含む）だけ有効です。
Valid To (Expiration)	*表示のみ。*証明書有効期間の最終日。
Serial Number	*表示のみ。*証明書のシリアル番号。
Description	証明書の説明。
使用法	
Trust for client with EAP-TLS	ACS が TLS 関連の EAP プロトコルの信頼リストを使用する場合に、このボックスをオンにします。
Certificate Status Validation	
OCSP Configuration	
このセクションは、OCSP サービスを設定するために使用します。	
Validate against OCSP service	このボックスをチェックし、ドロップダウン リストから OCSP サービスを選択して、選定した OCSP サービスに対して要求を確認します。
Reject the request if certificate status could not be determined by OCSP	証明書のステータスが OCSP サービスによって判断できない場合に要求を拒否するには、このボックスをチェックします。
証明書失効リストの設定（Certificate Revocation List Configuration）	
このセクションは、CRL を設定するために使用します。	
Download CRL	CRL をダウンロードする場合に、このボックスをオンにします。
CRL Distribution URL	CRL 配布 URL を入力します。HTTP またはセキュア HTTPS 接続を使用する URL を指定できます。HTTPS URL を使用する場合は、ACS 内の対応する HTTPS サーバの CA 証明書をインストールする必要があります。CRL のダウンロード用に ACS にプロキシ サーバを設定して、設定したプロキシ サーバを介して ACS が CRL 分配サーバと通信できるようにします。詳細については、CRL 要求の HTTP プロキシの設定（18-4 ページ）を参照してください。
Retrieve CRL	ACS は最初に CA から CRL をダウンロードしようとします。ACS が CA から新しい CRL を取得する時間設定を切り替えます。 • Automatically：CRL ファイルから次の更新時間を取得します。取得に失敗した場合、ACS は最初の失敗から定期的に、成功するまで CRL の取得を試みます。 • Every：取得試行の頻度を指定します。時間間隔を入力します。
If Download Failed Wait	CRL の取得が失敗した場合に、次に取得を試行する時間を入力します。

表 8-29　[Edit Certificate Authority Properties] ページ（続き）

オプション	説明
Bypass CRL Verification if CRL is not Received	オフの場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、ACS によって CRL が受信されるまで拒否されます。オンの場合、クライアント要求は CRL が受信される前に受け入れられます。
Ignore CRL Expiration	期限切れの CRL に対して証明書をチェックする場合に、このボックスをオンにします。 • オンの場合、ACS は期限切れの CRL を使用し続け、CRL の内容に従って EAP-TLS 認証を許可または拒否します。 • オフの場合、ACS は、CRL ファイルの [Next Update] フィールドで CRL の有効期限を調べます。CRL が期限切れの場合、選択した CA によって署名された証明書を使用するすべての認証は拒否されます。

ステップ 3　[Submit] をクリックします。

編集した証明書が含まれた [Trust Certificate] ページが表示されます。

管理者には、CRL および OCSP 検証を設定する権限があります。CRL と OCSP の検証が同時に設定されている場合、ACS は、まず OCSP の検証を実行します。プライマリまたはセカンダリサーバとの通信の問題が検出された場合、または指定された証明書のステータスが不明として検証から返された場合、ACS は CRL 検証の実行に進みます。

関連項目

- ユーザ証明書認証（C-6 ページ）
- EAP-TLS の概要（C-6 ページ）
- CRL 要求の HTTP プロキシの設定（18-4 ページ）

認証局の削除

このページは、信頼できる認証局（CA）証明書を削除する場合に使用します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate List] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　削除する証明書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。

ステップ 4　確認のために [Yes] をクリックします。

[Trust Certificate] ページが表示されます。このとき、削除した証明書は表示されません。

関連項目

- EAP-TLS の概要（C-6 ページ）

証明書チェーンの一部である CA 証明書の更新または削除

証明書チェーンの一部である CA 証明書の削除を試行すると、ACS で次のエラーが表示されます。

```
This System Failure occurred: Certificate Authority is in use by one of the ACS nodes
certificates.Your changes have not been saved.Click OK to return to the list page.
```

EAP または管理証明書チェーンの一部である CA 証明書を削除または更新するには、EAP または管理プロトコルを、CA 証明書が発行したものではない別のサーバ証明書にマッピングまたはアンバインドしてから、更新または削除する必要があります。

ACS の CA 証明書を更新または削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　次の条件を確認します。

- リストされているサーバ証明書が、更新または削除する CA 証明書が発行したものである場合は、EAP または管理プロトコルがサーバ証明書に適用されているかどうかを確認する必要があります。
- CA 証明書が発行したサーバ証明書のいずれかに、EAP または管理プロトコルがマッピングされている場合は、その EAP または管理プロトコルをサーバ証明書からアンバインドしてから、同じ CA 証明書が発行したものではない別のサーバ証明書にマッピングする必要があります。EAP または管理プロトコルのサーバ証明書からのアンバインドの詳細については、EAP または管理プロトコルのサーバ証明書からのアンバインド（8-101 ページ）を参照してください。

ステップ 3　CA 証明書は、この CA 証明書が発行したサーバ証明書のいずれも EAP や管理プロトコルにマッピングされていない場合に、更新または削除できます。

EAP または管理プロトコルのサーバ証明書からのアンバインド

EAP または管理プロトコルをサーバ証明書からアンバインドするには、次の手順を実行します。

ステップ 1　削除対象の証明書でもデフォルトのサーバ証明書と考えられる証明書でもない CA 証明書が発行した、新しいサーバ証明書をインストールします。詳細については、ローカル サーバ証明書の追加（18-18 ページ）を参照してください。

ステップ 2　次のいずれかの操作を実行します。

- 新しいサーバ証明書を追加する際に、[EAP: Used for EAP protocols that use SSL/TLS tunneling] チェックボックスと [Management Interface: Used to authenticate the web server (GUI)] チェックボックスをオンにします。
- 新しいサーバ証明書を追加すると、証明書が編集可能になり、[EAP: Used for EAP protocols that use SSL/TLS tunneling] チェックボックスと [Management Interface: Used to authenticate the web server (GUI)] チェックボックスをオンにすることができます。

この操作により、EAP または管理プロトコルが、元のサーバ証明書からアンバインドされ、新しいサーバ証明書にバインドされます。

認証局のエクスポート

信頼証明書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　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate List] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　エクスポートする証明書の隣にあるボックスをオンにします。

ステップ 3　[Export] をクリックします。

この操作によって、信頼できる証明書がクライアント マシンにエクスポートされます。

ステップ 4　確認のために [Yes] をクリックします。

エクスポートした証明書をクライアント マシンにインストールするように要求されます。

関連項目

- ユーザ証明書認証（C-6 ページ）
- EAP-TLS の概要（C-6 ページ）

証明書認証プロファイルの設定

証明書認証プロファイルによって、証明書ベースのアクセス要求に使用される X509 証明書情報が定義されます。ユーザ名として使用される属性を証明書から選択できます。

証明書属性のサブセットを選択して、要求のコンテキストにユーザ名フィールドを読み込むことができます。このユーザ名は、要求の残りのユーザを識別する場合に使用されます。ログで使用される識別情報にも使用されます。

証明書認証プロファイルを使用して証明書データを取得し、LDAP または AD クライアントから提示される証明書をさらに確認できます。証明書認証プロファイルのユーザ名を使用して、LDAP または AD ID ストアの問い合わせが行われます。

ACS は、クライアント証明書を LDAP または AD ID ストアから取得されたすべての証明書と 1 つずつ比較し、いずれかが一致するかどうかを確認します。ACS は、要求を受け入れるか、または拒否します。

（注）　ACS が要求を受け入れるには、LDAP または AD ID ストアの証明書が 1 つだけ、クライアント証明書と一致する必要があります。

ACS が証明書ベースの認証要求を処理するときに、次の 2 つのうちのいずれかが行われます。証明書のユーザ名と、要求を処理している ACS のユーザ名とが比較されます。あるいは、選択した LDAP または AD ID ストアに定義されている情報を使用して、ACS によって証明書情報が確認されます。

証明書認証プロファイルを複製して、既存の証明書認証プロファイルと同じか、または類似した新しいプロファイルを作成できます。複製の完了後、各プロファイル（元のプロファイルおよび複製されたプロファイル）に個別にアクセスして、編集または削除します。

ACS 5.8 では、現在、証明書の名前制約拡張をサポートします。これにより、発行元に名前制約拡張が含まれるクライアント証明書を受け入れます。また、CA およびサブ CA 証明書についてクライアント認証を確認します。この拡張は、証明書パスの後続の証明書におけるすべてのサブジェクト名の名前空間を定義します。これは、サブジェクト識別名とサブジェクト代替名の両方に適用されます。これらの制約は、指定された名前形式がクライアント証明書に存在する場合にのみ適用されます。ACS 認証は、クライアント証明書が名前空間により除外されている、または許可されていない場合、失敗します。

サポートされる名前制約

- ディレクトリ名
- DNS
- 電子メール
- URL

サポートされない名前制約

- IP アドレス
- その他の名前

証明書認証プロファイルを作成、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　[Users and Identity Stores] > [Certificate Authentication Profile] を選択します。

[Certificate Authentication Profile] ページが表示されます。

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。
- 複製する証明書認証プロファイル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。
- 変更する証明書認証プロファイルをクリックします。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。

  [Certificate Authentication Profile Properties] ページが表示されます。

ステップ 3　表 8-30 の説明に従って、[Certificate Authentication Profile Properties] ページのフィールドに入力します。

表 8-30　[Certificate Authentication Profile Properties] ページ

オプション	説明
General	
Name	証明書認証プロファイルの名前を入力します。
Description	証明書認証プロファイルの説明を入力します。
Certificate Definition	

表 8-30　[Certificate Authentication Profile Properties] ページ（続き）

オプション	説明
Principal Username X509 Attribute	x509 認証に使用できるプリンシパル ユーザ名属性のセット。選択肢は次のとおりです。 • Common Name • Subject Alternative Name • Subject Serial Number • Subject • Subject Alternative Name - Other Name • Subject Alternative Name - EMail • Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	選択した LDAP または AD ID ストアに対する認証のために証明書情報を確認する場合に、このチェックボックスをオンにします。 このオプションを選択する場合、LDAP または AD ID ストアの名前を入力するか、[Select] をクリックして使用可能なリストから LDAP または AD ID ストアを選択する必要があります。

ステップ 4　[Submit] をクリックします。

[Certificate Authentication Profile] ページが再表示されます。

関連項目

- ID ポリシーの表示（10-23 ページ）
- ID ストア順序の設定（8-104 ページ）
- 外部 LDAP ID ストアの作成（8-35 ページ）

ID ストア順序の設定

アクセス サービス ID ポリシーによって、ACS が認証および属性取得のために使用する ID ソースが決まります。ID ソースは、1 つの ID ストアまたは複数の ID 方式で構成されます。複数の ID 方式を使用する場合、最初にそれらを ID ストア順序内に定義し、次に ID ストア順序を ID ポリシー内に指定する必要があります。

ID ストア順序によって、認証および属性取得のために使用される順序、および追加属性を取得するための任意の追加順序が定義されます。

認証順序

ID ストア順序には、証明書ベースの認証またはパスワードベースの認証あるいはその両方の定義を含めることができます。

- 証明書に基づく認証を実行することを選択した場合は、すでに ACS で定義されている 1 つの証明書認証プロファイルを指定します。
- パスワードに基づく認証を実行することを選択した場合は、アクセスされるデータベースのリストを順番に定義できます。

認証が成功すると、データベース内の定義済み属性が取得されます。ACS でデータベースを定義しておく必要があります。

属性取得順序

追加属性を取得するデータベースのリストを任意に定義できます。これらのデータベースには、パスワードベースの認証を使用するか、証明書ベースの認証を使用するかに関係なくアクセスできます。証明書ベースの認証を使用すると、ACS によって証明書属性からユーザ名フィールドに読み込まれ、ユーザ名を使用して属性が取得されます。

ACS では、次の場合でもユーザの属性を取得できます。

- ユーザのパスワードに変更必須のフラグが付けられている。
- ユーザのアカウントがディセーブルになっている。

パスワードベースの認証を使用する場合、認証リストと属性取得リストに同じ ID データベースを定義できます。ただし、データベースが認証に使用される場合、属性取得フローの一部として再度アクセスされることはありません。

ACS では、ID ストア内のユーザまたはホストは、そのユーザまたはホストで単一の一致が存在する場合にだけ認証されます。外部データベース内に同じユーザの複数のインスタンスがある場合、認証は失敗します。同様に、ACS では、ユーザまたはホストの単一の一致が存在する場合にだけ属性が取得されます。それ以外の場合、そのデータベースからの属性取得はスキップされます。

ここでは、次の内容について説明します。

- ID ストア順序の作成、複製、および編集（8-105 ページ）
- ID ストア順序の削除（8-107 ページ）

ID ストア順序の作成、複製、および編集

ID ストア順序を作成、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　[Users and Identity Stores] > [Identity Store Sequences] を選択します。

[Identity Store Sequences] ページが表示されます。

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。
- 複製する順序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。
- 変更する順序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。

表 8-31 に示すように、[Identity Store Sequence Properties] ページが表示されます。

表 8-31　[Identity Store Sequence Properties] ページ

オプション	説明
General	
Name	ID ストア順序の名前を入力します。
Description	ID ストア順序の説明を入力します。
Authentication Method List	

表 8-31　[Identity Store Sequence Properties] ページ（続き）

オプション	説明
Certificate Based	証明書ベースの認証方式を使用する場合に、このチェックボックスをオンにします。このオプションを選択する場合、証明書認証プロファイルを入力する必要があります。[Select] をクリックして、使用可能なプロファイルのリストからプロファイルを選択します。
Password Based	パスワードベースの認証方式を使用する場合に、このチェックボックスをオンにします。このオプションを選択する場合、一致が見つかるまで ACS が 1 つずつアクセスする ID ストアのセットを選択する必要があります。 このオプションを選択する場合、ACS が ID ストアに 1 つずつアクセスするために、[Authentication and Attribute Retrieval Search List] 領域で ID ストアのリストを選択する必要があります。
Authentication and Attribute Retrieval Search List	
（注）　このセクションは、[Password Based] オプションをオンにした場合にだけ表示されます。	
Available	アクセス対象として使用可能な ID ストアのセット。
Selected	認証が成功するまで順番にアクセスされる選択済み ID ストアのセット。リストの右にある上向きおよび下向き矢印を使用して、アクセスの順序を定義します。 ACS により、認証用に選択した ID ストアから属性が自動的に取得されます。属性を取得するために同じ ID ストアを選択する必要はありません。
Additional Attribute Retrieval Search List	
Available	属性取得用に使用可能なその他の ID ストアのセット。
Selected	（任意）属性取得用に選択されたその他の ID ストアのセット。リストの右にある上向きおよび下向き矢印を使用して、アクセスの順序を定義します。 ACS により、認証用に選択した ID ストアから属性が自動的に取得されます。属性を取得するために同じ ID ストアを選択する必要はありません。
Internal User/Host	
If internal user/host is not found or disabled then exit the sequence and treat as User Not Found	このオプションは、内部 ID ストアが属性取得のリストに含まれている場合に、属性フェーズで適用されます。 このオプションが選択され、ユーザが見つからないか、またはディセーブルにされているとき、ACS はシーケンスを終了し、「ユーザが見つかりません」として扱います。
Advanced Options	
Break sequence	このオプションが選択され、現在の ID ストアに対する認証の試行がプロセス エラーになった場合、フローは ID ストア シーケンスを終了します。次に、ID ポリシーで設定された [Fail-Open] オプションに進みます。 同じことが属性取得にも適用されます。
Continue to next identity store in the sequence	これがオンで、現在の ID ストアに対する認証がプロセス エラーになった場合、フローは認証リストの次の ID ストアで認証を試行します。 同じことが属性取得のフェーズにも適用されます。

ステップ 3　[Submit] をクリックします。

[Identity Store Sequences] ページが再表示されます。

関連項目

- 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（7-8 ページ）
- ID ポリシーの表示（10-23 ページ）
- 内部 ID ストアの管理（8-5 ページ）
- 外部 ID ストアの管理（8-30 ページ）
- 証明書認証プロファイルの設定（8-102 ページ）
- ID ストア順序の削除（8-107 ページ）

ID ストア順序の削除

ID ストア順序を削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Store Sequences] を選択します。

[Identity Store Sequences] ページが表示され、設定されている ID ストア順序のリストが示されます。

ステップ 2　削除する ID ストア順序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。

次のエラー 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。

[Identity Store Sequences] ページが表示されます。このとき、削除した ID ストア順序はリストに含まれません。

関連項目

- 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（7-8 ページ）
- ID ポリシーの表示（10-23 ページ）
- 内部 ID ストアの管理（8-5 ページ）
- 外部 ID ストアの管理（8-30 ページ）
- 証明書認証プロファイルの設定（8-102 ページ）
- ID ストア順序の作成、複製、および編集（8-105 ページ）