ユーザおよび外部 ID ソースの管理

この章では、Cisco ISE のユーザ アカウント、および認証と認可の目的でユーザ情報を保存するために使用できるさまざまな ID ソースを管理する方法について説明します。

この章では、ユーザという用語は、従業員、請負業者、スポンサー ユーザを意味します。ゲスト ユーザについては、第 16 章「ゲストに許可されるネットワーク アクセスのサポート」で詳しく説明します。

この章の内容は、次のとおりです。

Cisco ISE ユーザ

この章では、ユーザという用語はネットワークに定期的にアクセスする従業員と請負業者に加え、スポンサーおよびゲスト ユーザを意味します。スポンサーは、スポンサー ポータルからゲスト ユーザ アカウントを作成および管理する組織の従業員または請負業者です。ゲスト ユーザは、限られた期間に組織のネットワーク リソースにアクセスする必要がある外部訪問者です。

Cisco ISE ネットワーク上のリソースとサービスにアクセスするすべてのユーザのアカウントを作成する必要があります。従業員、請負業者、およびスポンサー ユーザは、管理者ポータルで作成されます。

関連項目

- 「スポンサーおよびゲスト アカウントの管理」（P.16-3）
- *『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2』*

ユーザ アイデンティティ

ユーザ ID は、ユーザに関する情報を保持するコンテナに似ており、ユーザのネットワーク アクセス クレデンシャルを形成します。各ユーザの ID はデータにより定義され、ユーザ名、電子メール アドレス、パスワード、アカウントの説明、関連付けられている管理者グループ、ユーザ グループ、ロールなどが含まれます。

ユーザ グループ

ユーザ グループは、特定の一連の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザの集合です。

ユーザ ID グループ

ユーザのグループ ID は、同じグループに属している特定のユーザ グループを識別および説明する要素で構成されています。グループ名は、このグループのメンバーが持っている機能ロールの説明です。グループは、そのグループに属しているユーザのリストです。

デフォルトのユーザ ID グループ

Cisco ISE には、次の事前定義されたユーザ ID グループが用意されています。

- 従業員：組織の従業員がこのグループに属します。
- SponsorAllAccount：Cisco ISE ネットワークのすべてのゲスト アカウントを中断または再開できるスポンサー ユーザ。
- SponsorGroupAccounts：同じスポンサー ユーザ グループのスポンサー ユーザによって作成されたゲスト アカウントを中断できるスポンサー ユーザ。
- SponsorOwnAccounts：自分が作成したゲスト アカウントのみ中断できるスポンサー ユーザ。
- ゲスト：ネットワーク内のリソースに一時的にアクセスする必要がある訪問者。
- ActivatedGuest：アカウントが有効でアクティブになっているゲスト ユーザ。

ユーザ ロール

ユーザ ロールは、ユーザが Cisco ISE ネットワークで実行できるタスクやアクセスできるサービスを決定する権限セットです。ユーザ ロールは、ユーザ グループに関連付けられています。たとえば、ネットワーク アクセス ユーザ。

ユーザ アカウントのカスタム属性およびパスワード ポリシー

Cisco ISE では、ユーザ属性に基づいてユーザのネットワーク アクセスを制限することができます。Cisco ISE では、一連の事前定義されたユーザ属性が用意されており、カスタム属性を作成することもできます。両方のタイプの属性が認証ポリシーを定義する条件で使用できます。パスワードが指定された基準を満たすように、ユーザ アカウントのパスワード ポリシーも定義できます。

ここでは、次の内容について説明します。

カスタム ユーザ属性

[ユーザ カスタム属性設定（User Custom Attributes Setting）] ページで、[カスタム属性（Custom Attributes）] ペインを使用して追加のユーザ アカウント属性を定義することができます。Cisco ISE では、設定できない事前定義された属性のリストが用意されています。ただし、次を設定して、カスタム属性を定義できます。

- 属性名
- データ型

ユーザ パスワード ポリシーの設定

[ユーザ パスワード ポリシー（User Password Policy）] ページで、ユーザ アカウント パスワードが満たす必要がある基準を定義できます。[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザ パスワード ポリシー（User Password Policy）] を選択します。

表 A-34 では、[ユーザ パスワード ポリシー（User Password Policy）] ページの設定フィールドについて説明します。

（注）

- パスワード ライフタイム機能は、ユーザおよびスポンサー ユーザが自分のパスワードを定期的に変更できるようにするために存在します。
- この機能はローカル「管理者」ユーザには影響しません。
- 「アカウントの無効」を使用している場合は、ユーザがロックされないようにするため「リマインダ」機能を使用することを推奨します。
- ユーザ時間切れスレッドは深夜 0 時に動作し、パスワード ライフタイムを超えるアカウントを無効にします。

ユーザの追加

Cisco ISE では、Cisco ISE ユーザの属性の表示、作成、変更、複製、削除、ステータスの変更、インポート、エクスポート、または検索を実行できます。

Cisco ISE 内部データベースを使用している場合、Cisco ISE ネットワーク上のリソースまたはサービスにアクセスする必要があるすべての新しいユーザのアカウントを作成する必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] を選択します。

ステップ 2　[追加（Add）]（[+]）をクリックして、新しいユーザを作成します。

ステップ 3　フィールドに値を入力します。

ユーザ名にはスペースは使用できません。

ステップ 4　[送信（Submit）] をクリックして、新しいユーザを Cisco ISE 内部データベースに作成します。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「ユーザ アカウントのカスタム属性およびパスワード ポリシー」（P.14-2）
- 「Cisco ISE ユーザ データのエクスポート」（P.14-4）
- 「Cisco ISE ユーザ データのインポート」（P.14-4）

Cisco ISE ユーザ データのエクスポート

Cisco ISE 内部データベースからユーザ データをエクスポートしなければならない場合があります。Cisco ISE では、パスワードで保護された CSV ファイル形式でユーザ データをエクスポートすることができます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] を選択します。

ステップ 2　データをエクスポートするユーザに対応するチェックボックスをオンにします。

ステップ 3　[選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 4　[キー（Key）] フィールドに、パスワードを暗号化するためのキーを入力します。

ステップ 5　[エクスポートの開始（Start Export）] をクリックして、users.csv ファイルを作成します。

ステップ 6　[OK] をクリックして、users.csv ファイルをエクスポートします。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「ユーザ アカウントのカスタム属性およびパスワード ポリシー」（P.14-2）
- 「ユーザの追加」（P.14-3）
- 「Cisco ISE ユーザ データのインポート」（P.14-4）

Cisco ISE ユーザ データのインポート

Cisco ISE では、CSV ファイル形式のユーザ データを内部データベースにエクスポートすることができます。ユーザ アカウントを手動で Cisco ISE に入力する代わりに、それらをインポートできます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] を選択します。

ステップ 2　[インポート（Import）] をクリックし、カンマ区切りのテキスト ファイルからユーザをインポートします。

ヒント（任意）カンマ区切りのテキスト ファイルがない場合は、[テンプレートの生成（Generate a Template）] をクリックして、このタイプのファイルを作成します。

ステップ 3　[ファイル（File）] テキスト ボックスに、インポートするユーザが含まれたファイル名を入力するか、[参照（Browse）] をクリックして、ファイルが配置されている場所に移動します。

ステップ 4　新しいユーザの作成、および既存のユーザの更新の両方を実行する必要がある場合は、[新しいユーザの作成、および新しいデータで既存のユーザを更新（Create new user(s) and update existing user(s) with new data）] チェックボックスをオンにします。

ステップ 5　[保存（Save）] をクリックして、変更を Cisco ISE 内部データベースに保存します。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「ユーザ アカウントのカスタム属性およびパスワード ポリシー」（P.14-2）
- 「ユーザの追加」（P.14-3）
- 「Cisco ISE ユーザ データのエクスポート」（P.14-4）

ユーザ ID グループの作成

ユーザをユーザ ID グループに割り当てる前に、ユーザ ID グループを作成する必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] > [追加（Add）] を選択します。

ステップ 2　[名前（Name）] および [説明（Description）] フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は、スペース # $ & ' ( ) * + - ./ @ _ です。

ステップ 3　[送信（Submit）] をクリックします。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「デフォルトのユーザ ID グループ」（P.14-2）
- 「ユーザ ID グループのエクスポート」（P.14-5）
- 「ユーザ ID グループのインポート」（P.14-6）

ユーザ ID グループのエクスポート

Cisco ISE では、ローカルで設定されているユーザ ID グループを CSV ファイル形式でエクスポートすることができます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] を選択します。

ステップ 2　エクスポートするユーザ ID グループに対応するチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3　[OK] をクリックします。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「ユーザ ID グループの作成」（P.14-5）
- 「ユーザ ID グループのインポート」（P.14-6）

ユーザ ID グループのインポート

Cisco ISE では、ユーザ ID グループを CSV ファイル形式でインポートすることができます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] を選択します。

ステップ 2　[テンプレートの生成（Generate a Template）] をクリックして、インポート ファイルに使用するテンプレートを取得します。

ステップ 3　[インポート（Import）] をクリックし、カンマ区切りのテキスト ファイルからネットワーク アクセス ユーザをインポートします。

ステップ 4　新しいユーザ ID グループの追加、および既存のユーザ ID グループの更新の両方を実行する必要がある場合は、[新しいデータで既存のデータを上書き（Overwrite existing data with new data）] チェックボックスをオンにします。

ステップ 5　[インポート（Import）] をクリックします。

ステップ 6　[保存（Save）] をクリックして、変更を Cisco ISE データベースに保存します。

関連項目

- 「Cisco ISE ユーザ」（P.14-1）
- 「ユーザ ID グループ」（P.14-2）
- 「ユーザ ID グループの作成」（P.14-5）
- 「ユーザ ID グループのエクスポート」（P.14-5）

ID ソース

ID ソースには、ユーザの認証中にクレデンシャルを検証したり、ユーザに関連付けられているグループ情報やその他の属性を取得して許可ポリシーで使用したりするために Cisco ISE が使用するユーザ情報が含まれます。それらは、レコードの形式でユーザ情報を保存するデータベースです。ID ソースからユーザ情報を追加、編集、および削除できます。

Cisco ISE は、内部および外部 ID ソースをサポートします。両方のソースは、スポンサー ユーザとゲスト ユーザの認証のための認証ソースとして使用できます。

関連項目

- 「内部 ID ソース」（P.14-7）
- 「外部 ID ソース」（P.14-7）

内部 ID ソース

Cisco ISE には、ユーザ情報を保存するために使用できる内部ユーザ データベースがあります。内部ユーザ データベース内のユーザは、内部ユーザと呼ばれます。Cisco ISE には、Cisco ISE に接続するすべてのデバイスおよびエンドポイントに関する情報を格納する内部エンドポイント データベースがあります。

外部 ID ソース

Cisco ISE では、ユーザ情報を含む外部 ID ソースを設定することができます。Cisco ISE は、認証のためのユーザ情報を取得するために、外部 ID ソースに接続します。外部 ID ソースには、Cisco ISE サーバ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。Cisco ISE は、外部 ID ソースとの通信に認証プロトコルを使用します。表 14-1 に、認証プロトコルおよび認証プロトコルがサポートする外部 ID ソースを示します。

表 14-1　認証プロトコルおよびサポートされる外部 ID ソース

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP[1]	RADIUS トークン サーバまたは RSA
EAP-GTC[2]、PAP[3]（プレーン テキスト パスワード）	Yes	Yes	Yes	Yes
MS-CHAP[4] パスワード ハッシュ： MSCHAPv1/v2[5] EAP-MSCHAPv2[6] LEAP[7]	Yes	Yes	No	No
EAP-MD5[8] CHAP[9]	Yes	No	No	No
EAP-TLS[10] PEAP-TLS[11] （証明書取得） **（注）** TLS 認証（EAP-TLS および PEAP-TLS）では、ID ソースは必要ありませんが、任意で許可ポリシー条件に追加できます。	Yes	Yes	Yes	No

1. LDAP = Lightweight Directory Access Protocol。
2. EAP-GTC = 拡張認証プロトコル -- 汎用トークン カード。

3. PAP = パスワード認証プロトコル。
4. MS-CHAP = Microsoft チャレンジ ハンドシェイク認証プロトコル。
5. MS-CHAPv1/v2 = Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 1/バージョン 2。
6. EAP-MSCHAPv2 = 拡張認証プロトコル-Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2。
7. LEAP = Lightweight Extensible Authentication Protocol
8. EAP-MD5 = 拡張認証プロトコル-Message Digest 5。
9. CHAP = チャレンジ ハンドシェイク認証プロトコル。
10. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
11. PEAP-TLS = 拡張認証プロトコル - トランスポート層セキュリティ。

関連項目

- 「証明書認証プロファイル」（P.14-8）
- 「外部 ID ソースとしての Active Directory」（P.14-9）
- 「LDAP」（P.14-20）
- 「RADIUS トークン ID ソース」（P.14-27）
- 「RSA ID ソース」（P.14-33）
- 「ID ソース順序」（P.14-39）
- 「レポートでの ID ソースの詳細」（P.14-41）

証明書認証プロファイル

プロファイルごとに、プリンシパル ユーザ名として使用する必要がある証明書フィールド、および証明書のバイナリ比較を実行する必要があるかどうかを指定する必要があります。

関連項目

「証明書認証プロファイルの追加」（P.14-8）

証明書認証プロファイルの追加

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）証明書ベースの認証方式を使用する場合は、証明書認証プロファイルを作成する必要があります。従来のユーザ名とパスワードの方式で認証する代わりに、Cisco ISE はユーザの信頼性を確認するためにクライアントから受信した証明書をサーバ内の証明書と比較します。

はじめる前に

スーパー管理者またはシステム管理者である必要があります。

Windows 証明書ベースの認証の場合、サブジェクト代替名またはサブジェクト名を指定する必要があります。

Anyconnect 3.1 を介して認証を実行する場合、クライアント証明書認証で EAP-FAST プロトコルを使用するときに Microsoft 証明書のサブジェクト代替名を指定する必要があります。

他の認証局によって発行された証明書を使用する場合は、一般名を指定する必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）] を選択します。

ステップ 2　証明書認証プロファイルの名前と説明を入力します。

ステップ 3　**プリンシパル ユーザ名 X509** 属性を選択します。

ステップ 4　選択した Lightweight Directory Access Protocol（LDAP）または Microsoft Active Directory 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。[LDAP または Active Directory から取得された証明書とバイナリ証明書比較を実行（Perform Binary Certificate Comparison with Certificate Retrieved from LDAP or Active Directory）] チェックボックスをオンにします。

（注）　このチェックボックスをオンにした場合は、使用可能なリストから LDAP または Active Directory ID ソースを選択する必要があります。

ステップ 5　認証の証明書情報を検証する LDAP または Active Directory の ID ソースを選択します。

ステップ 6　[送信（Submit）] をクリックして、証明書認証プロファイルを追加するか、変更を保存します。

次の作業

1. 認証ポリシーの作成方法については、第 19 章「認証ポリシーの管理」を参照してください。
2. 許可プロファイルおよびポリシーの作成方法については、第 20 章「許可ポリシーおよびプロファイルの管理」を参照してください。

外部 ID ソースとしての Active Directory

Cisco ISE は、ユーザ、マシン、グループ、属性などのリソースにアクセスするために、Microsoft Active Directory を外部 ID ソースとして使用します。

Active Directory でのユーザとマシンの認証

Active Directory でのユーザとマシンの認証では、Active Directory にリストされているユーザとデバイスに対してのみネットワーク アクセスを許可します。

Active Directory でサポートされる認証プロトコルおよび機能

Active Directory は、一部のプロトコルを使用したユーザとマシンの認証、Active Directory ユーザ パスワードの変更などの機能をサポートしています。表 14-2 に、Active Directory でサポートされる認証プロトコルおよびそれぞれの機能を示します。

表 14-2　Active Directory でサポートされる認証プロトコル

認証プロトコル	機能
EAP-FAST および保護拡張認証プロトコル（PEAP）	内部方式が MS-CHAPv2 および EAP-GTC の EAP-FAST と PEAP を使用した、パスワード変更機能を備えたユーザとマシンの認証
パスワード認証プロトコル（PAP）	認証、およびパスワードを変更する機能
Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 1（MS-CHAPv1）	ユーザとマシンの認証
Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2（MS-CHAPv2）	ユーザとマシンの認証
Extensible Authentication Protocol-Generic Token Card（EAP-GTC; 拡張認証プロトコル - 汎用トークンカード）	ユーザとマシンの認証
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）	証明書取得オプションを使用したユーザとマシンの認証
Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）	ユーザとマシンの認証
Lightweight Extensible Authentication Protocol（LEAP）	ユーザ認証

認可ポリシーで使用する Active Directory 属性およびグループ検索

Cisco ISE は、認可ポリシー ルールで使用するために Active Directory からユーザまたはマシンの属性を取得します。これらの属性は Cisco ISE ポリシーにマッピングされ、ユーザまたはマシンの承認レベルが決定されます。Cisco ISE は、認証が成功した後にユーザおよびマシンの Active Directory 属性を取得します。認証とは別に、許可のために属性を取得することもできます。

Cisco ISE は、ユーザとグループのメンバーシップのルックアップを LDAP 経由で Active Directory に対して行います。グループ メンバーシップは、ISE においてスポンサー ユーザを対応するスポンサー グループにマッピングするために使用されます。ユーザが直接 Active Directory グループ内に存在せず、Active Directory グループのメンバーであるグループのメンバー（ネスト グループ）である場合は、ユーザ許可は拒否されます。

ルールに、/!@\#$%^&*()_+~ のような特殊文字を含む Active Directory グループ名が含まれる場合、認可ポリシーに基づくユーザ認証は失敗します。

証明書ベースの認証のための Active Directory 証明書取得

Cisco ISE では、EAP-TLS プロトコルを使用するユーザおよび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。Active Directory 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。この証明書属性に 1 つ以上の証明書を含めることができます。Cisco ISE ではこの属性は userCertificate として識別され、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。Cisco ISE はこの証明書を取得し、ユーザまたはマシンの ID を確認するために使用します。

証明書認証プロファイルは、証明書の取得に使用するフィールド（たとえば、サブジェクト代替名（SAN）、一般名、または社会保障番号（SSN））を決定します。Cisco ISE 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、Cisco ISE は、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、ユーザまたはマシンにネットワークへのアクセスが付与されます。

Active Directory ユーザ認証プロセス フロー

ユーザの認証または問い合わせ時に、Cisco ISE は次のことをチェックします。

- ユーザ アカウントが無効かどうか
- ユーザがロックアウトされているかどうか
- ユーザ 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、Active Directory ディクショナリ内の *Active Directory Identifier*: 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、すべてのポリシー ルールで使用できます。*Active Directory identifier* は、Active Directory ID ソースに対して入力する名前です。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストがある Active Directory がサポートされています。Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

（注）　Cisco ISE は、ネットワーク アドレス トランスレータの背後にあり、ネットワーク アドレス変換（NAT）アドレスを持つ Microsoft Active Directory サーバをサポートしません。

Active Directory サービスをサポートする Windows サーバ オペレーティング システムのリストについては、『*Release Notes for Cisco Identity Services Engine, Release 1.2*』を参照してください。

外部 ID ソースとして Active Directory を設定するためのガイドライン

これらの設定を正しく設定して、　Cisco ISE が Active Directory に接続し、正常にユーザを認証できるようにするには、次の内容をよく読んでください。

- Cisco ISE サーバと Active Directory 間の時間を同期するために、ネットワーク タイム プロトコル（NTP）サーバ設定を使用します。
- Cisco ISE と Active Directory 間にファイアウォールがある場合は、次のポートが Cisco ISE と Active Directory 間の通信用に開いていることを確認します。

プロトコル	ポート番号
LDAP	389（UDP）
SMB[1]	445（TCP）
KDC[2]	88（TCP）

プロトコル	ポート番号
グローバル カタログ	3268（TCP）、3269
KPASS	464（TCP）
NTP	123（UDP）
LDAP	389（TCP）
LDAPS[3]	636（TCP）

1. SMB = サーバ メッセージ ブロック。
2. KDC = キー発行局。
3. LDAPS = Lightweight Directory Access Protocol over TLS/SSL。

- Active Directory にマルチドメイン フォレストがある場合は、Cisco ISE が接続されているドメインと、アクセスする必要があるユーザおよびマシン情報が含まれている他のドメインの間に信頼関係が存在す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* のマニュアルを参照してください。
- 展開内のすべての Cisco ISE ノードは、効果的に Active Directory と相互運用するために、ドメイン ネーム サーバ（DNS）のルックアップを正引きと逆引きで実行できる必要があります。Cisco ISE で **ip name-server** コマンドを使用して設定した DNS サーバは、Active Directory ID ソースのドメイン名を正確に解決できる必要があります。Active Directory 展開に含まれる DNS サーバは通常、Cisco ISE で設定されます。複数の DNS サーバを設定する必要がある場合は、**application configure ise** コマンドを使用して設定できます。
- Cisco ISE を追加するドメインで、少なくとも 1 つのグローバル カタログ サーバが動作している必要があります。
- Active Directory ドメインに参加するときに入力する Active Directory ユーザ名は、Active Directory で定義済みであり、次のいずれかの権限が割り当てられている必要があります。
  - 接続先のドメインにワークステーションを追加する。
  - Cisco ISE をドメインに追加する前に、Cisco ISE アカウントが作成されたコンピュータ上で、コンピュータ オブジェクトを作成または削除する権限を確立する。
  - 認証に必要なユーザおよびグループを検索する権限。

  Cisco ISE を Active Directory ドメインに追加した後にも、次のことを実行する権限が必要な場合があります。
  - そのドメインにいずれかのセカンダリ Cisco ISE サーバを追加する
  - データをバックアップまたは復元する
  - アップグレード プロセスにバックアップと復元が含まれる場合、Cisco ISE を以降のバージョンにアップグレードする

関連項目

- 「システム時刻と NTP サーバ設定の指定」（P.5-3）
- *『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』*

外部 ID ソースとしての Active Directory の設定

はじめる前に

- Cisco ISE ホスト名が 15 文字以下であることを確認します。Active Directory では 15 文字を超えるホスト名は検証されません。
- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作に使用する Microsoft Active Directory 管理者アカウントが有効であり、Microsoft Active Directory で Change Password on Next Login を使用して設定されていないことを確認します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） Cisco ISE が Active Directory に接続されている場合にも、操作に関する問題があることがあります。それらを特定するには、[操作（Operations）] > [レポート（Reports）] で認証レポートを参照してください。

外部 ID ソースとして Active Directory を設定するには、次のタスクを実行する必要があります。

- 「Active Directory ドメインへの接続」（P.14-13）
- 「パスワード変更、マシン認証、およびマシン アクセス制限の有効化」（P.14-14）
- 「Active Directory ユーザ グループの設定」（P.14-14）

Active Directory ドメインへの接続

ステップ 1　ユーザおよびマシン情報を含む Active Directory ドメインに接続します。

ステップ 2　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 3　ドメイン名とフレンドリ名を入力します。

ステップ 4　[設定の保存（Save Configuration）] をクリックします。設定を正常に保存すると、すべての Cisco ISE ノード、ノードのロール、およびそのステータスを含む展開の参加 / 脱退の表が表示されます。

設定を保存すると、Active Directory ドメインの設定が（プライマリおよびセカンダリのポリシー サービス ノードに）グローバルに保存されますが、いずれの Cisco ISE ノードもドメインに参加しません。

ステップ 5　[参加（Join）] をクリックして、Active Directory ドメインに Cisco ISE ノードを接続します。設定を保存した場合でも、これを明示的に行う必要があります。展開内のセカンダリ ポリシー サービス ノードをそれぞれ個別に参加させる必要があります。

ステップ 6　Cisco ISE ノードの隣のチェックボックスをオンにし、[テスト接続（Test Connection）] をクリックして Cisco ISE ノードを Active Directory ドメインに接続できるかどうかを確認します。基本または詳細テストを実行できます。詳細テストは、大規模な Active Directory 展開では完了するのに時間がかかる場合があります。

ステップ 7　Active Directory のユーザ名とパスワードを入力し、[OK] をクリックします。

（注） Active Directory ドメインにサブドメインがあり、ユーザがサブドメインの 1 つに属している場合、ユーザ名にサブドメイン名も含める必要があります。たとえば、example.com ドメインに sub1 および sub2 と呼ばれる 2 つのサブドメインがあります。ユーザが sub1 に属している場合、ユーザ名は sub1\user1 にしてください。

ステップ 8　[OK] をクリックします。

ステップ 9　Cisco ISE ノードが Active Directory ドメインに参加するためには、Cisco ISE ノードの隣のチェックボックスをオンにして、[参加（Join）] をクリックします。

ステップ 10　Active Directory のユーザ名とパスワードを入力し、[OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、ポップアップに失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示できます。

ステップ 11　[閉じる（Close）] をクリックします。

次の作業

「パスワード変更、マシン認証、およびマシン アクセス制限の有効化」（P.14-14）

パスワード変更、マシン認証、およびマシン アクセス制限の有効化

はじめる前に

- Active Directory ドメインに Cisco ISE を参加させる必要があります。
- 詳細設定を行います。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2　[高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3　[パスワード変更の有効化（Enable Password Change）] チェックボックスをオンにして、ユーザが Active Directory のユーザ パスワードを変更できるようにします。

ステップ 4　[マシン認証の有効化（Enable Machine Authentication）] チェックボックスをオンにして、マシン認証を可能にします。

ステップ 5　[マシン アクセス制限の有効化（Enable Machine Access Restrictions）]（MARs）チェックボックスをオンにして、マシン認証の結果がユーザ認証および許可の結果に関連付けられるようにします。

ステップ 6　MARs を有効にした場合は、エージング タイムを入力する必要があります。

この値は、時間単位であり、マシン認証の有効期限を設定します。たとえば、MARs を有効にし、2 の値を入力した場合、ユーザが 2 時間後に認証を試みると、認証は失敗します。

ステップ 7　[設定の保存（Save Configuration）] をクリックします。

次の作業

「Active Directory ユーザ グループの設定」（P.14-14）

Active Directory ユーザ グループの設定

Active Directory ユーザ グループを認可ポリシーで使用できるように設定する必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2　[グループ（Groups）] タブをクリックします。

ディレクトリからグループを追加する場合は、フィルタを使用してグループを検索できます。たとえば、フィルタ基準として **cn=users** と入力し、[グループの取得（Retrieve Groups）] をクリックして、cn=users から始まるユーザ グループを表示します。結果をフィルタリングするために、アスタリスク（*）ワイルドカード文字を入力することもできます。

ステップ 3　[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して既存のグループを選択します。

ステップ 4　グループの追加を選択した場合は、新しいグループの名前を入力します。

ステップ 5　許可ポリシーで使用可能にするグループの隣のチェックボックスをオンにして、[OK] をクリックします。

ステップ 6　[設定の保存（Save Configuration）] をクリックします。

次の作業

「Active Directory ユーザ属性の設定」（P.14-15）

Active Directory ユーザ属性の設定

Active Directory ユーザ属性を認可ポリシー条件で使用できるように設定する必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2　[属性（Attributes）] タブをクリックします。

ディレクトリからの属性の追加を選択した場合、ユーザの名前を [サンプル ユーザ（Example User）] フィールドに入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性のリストを取得します。たとえば、管理者属性のリストを取得するには、**admin** と入力します。結果をフィルタリングするために、アスタリスク（*）ワイルドカード文字を入力することもできます。

ステップ 3　[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択してディレクトリから属性のリストを選択します。

（注）　サンプル ユーザ名を入力するときは、Cisco ISE が接続されている Active Directory ドメインからユーザを選択することを確認してください。
マシン属性を取得するためにサンプル マシンを選択するときは、マシン名に「host/」というプレフィックスを付加してください。たとえば、host/myhost などを使用します。

ステップ 4　属性の追加を選択した場合は、新しい属性の名前を入力します。

ステップ 5　選択する Active Directory の属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6　[設定の保存（Save Configuration）] をクリックします。

次の作業

1. 認証ポリシーの作成方法については、第 19 章「認証ポリシーの管理」を参照してください。
2. 許可プロファイルおよびポリシーの作成方法については、第 20 章「許可ポリシーおよびプロファイルの管理」を参照してください。

Active Directory ドメインの脱退

Active Directory のユーザまたはマシンを認証する必要がなくなった場合、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE アプリケーション設定をリセットすると、ISE ノードがすでに参加している場合に Active Directory ドメインからそれを切断する脱退操作が実行されます。ただし、Cisco ISE ノードのアカウントは、Active Directory ドメインから削除されません。Active Directory クレデンシャルを使用して管理者ポータルから脱退操作を実行することを推奨します。それにより、Active Directory ドメインからノード アカウントが削除されます。

はじめる前に

認証ポリシーの ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用していないことを確認します。Active Directory ドメインを脱退したが、認証の ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用している場合、認証が失敗する可能性があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2　Cisco ISE ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 3　Active Directory のユーザ名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE データベースから設定を削除します。

ステップ 4　Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにした場合、プライマリ Cisco ISE ノードは Active Directory ドメインを脱退します。Active Directory 管理者は、参加中に作成された Active Directory データベースで作成されたエントリを手動で削除する必要があります。

Active Directory クレデンシャルを入力した場合、Cisco ISE は Active Directory ドメインを脱退し、Active Directory データベースから設定が削除されます。

（注）　ここに入力した Active Directory クレデンシャルには、Cisco ISE アカウントが作成されたコンピュータ上のコンピュータ オブジェクトの作成権限またはコンピュータ オブジェクトの削除権限が必要です。

関連項目

「Active Directory の設定の削除」（P.14-17）

Active Directory の設定の削除

外部 ID ソースとして Active Directory を使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。

はじめる前に

Active Directory ドメインを脱退していることを確認します。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2　[ローカル ノード ステータス（Local Node Status）] がドメインに [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 3　[設定の削除（Delete Configuration）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

関連項目

「Active Directory ドメインの脱退」（P.14-16）

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。このオプションは、デバッグ情報を取得する展開内のポリシー サービス ペルソナを担当した Cisco ISE ノードで有効にする必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログ設定（Debug Log Configuration）] を選択します。

ステップ 2　Active Directory のデバッグ情報を取得する Cisco ISE ポリシー サービス ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3　[Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4　[Active Directory] の横のドロップダウン リストから、[DEBUG] を選択します。

ステップ 5　[保存（Save）] をクリックします。

トラブルシューティング用の Active Directory ログ ファイルの取得

Active Directory の設定に関する問題がある場合、問題をトラブルシュートするために Active Directory のデバッグ ログをダウンロードして、表示できます。

はじめる前に

Active Directory デバッグ ログの設定を有効にする必要があります。

ステップ 1　[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）] を選択します。

ステップ 2　Active Directory のデバッグ ログ ファイルを取得するノードをクリックします。

ステップ 3　[デバッグ ログ（Debug Logs）] タブをクリックします。

ステップ 4　このページを下にスクロールして ad_agent.log ファイルを見つけます。このファイルをクリックしてダウンロードします。

関連項目

「Active Directory デバッグ ログの有効化」（P.14-17）

Active Directory を使用した Cisco ISE をセット アップするための補足情報

ここでは、Active Directory を使用した Cisco ISE をセット アップするための指針を示します。

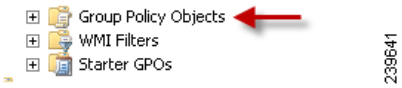
- 「Active Directory でのグループ ポリシーの設定」（P.14-18）
- 「Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定」（P.14-19）
- 「マシン認証のための AnyConnect エージェント」（P.14-20）

Active Directory でのグループ ポリシーの設定

グループ ポリシー管理エディタにアクセスする方法の詳細については、*Microsoft Active Directory* のマニュアルを参照してください。

ステップ 1　図 14-1 に示すように、グループ ポリシー管理エディタを開き、新しいポリシー オブジェクトを作成するか、既存のドメイン ポリシーに追加します。

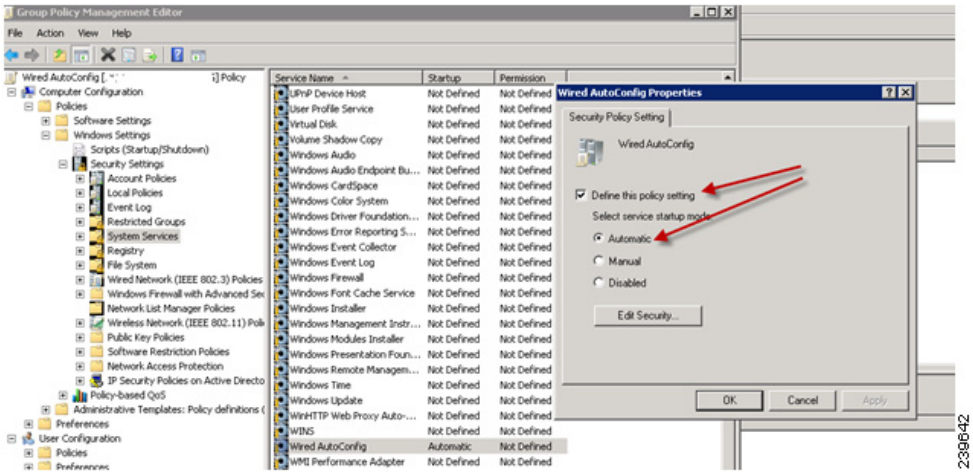
図 14-1　グループ ポリシー オブジェクト



ステップ 2　新しいポリシーを作成し、説明的な名前を入力します。たとえば、優先自動設定などを使用します。

ステップ 3　図 14-2 に示すように、[このポリシー設定を定義する（Define this policy setting）] チェックボックスをオンにして、サービス起動モードの [自動（Automatic）] オプション ボタンをクリックします。

図 14-2　　ポリシー プロパティ



ステップ 4　目的の組織ユニットまたはドメイン Active Directory レベルでポリシーを適用します。コンピュータは次回再起動したときにポリシーを受信し、このサービスが有効になります。

Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定

Active Directory に対する EAP-TLS マシン認証に Odyssey 5.x サプリカントを使用している場合は、サプリカントで次の設定を行う必要があります。

ステップ 1　Odyssey アクセス クライアントを起動します。

ステップ 2　[ツール（Tools）] メニューから、[Odyssey アクセス クライアント管理者（Odyssey Access Client Administrator）] を選択します。

ステップ 3　[マシン アカウント（Machine Account）] アイコンをダブルクリックします。

ステップ 4　[マシン アカウント（Machine Account）] ページから、EAP-TLS 認証のプロファイルを設定する必要があります。

a.　[設定（Configuration）] > [プロファイル（Profiles）] を選択します。

b.　EAP-TLS プロファイルの名前を入力します。

c.　[認証（Authentication）] タブで、認証方式として [EAP-TLS] を選択します。

d.　[証明書（Certificate）] タブで、[証明書を使用したログインを許可（Permit login using my certificate）] チェックボックスをオンにして、サプリカント マシンの証明書を選択します。

e.　[ユーザ情報（User Info）] タブで、[マシン クレデンシャルを使用（Use machine credentials）] チェックボックスをオンにします。

このオプションが有効になっている場合、Odyssey サプリカントは host\<*machine_name*> の形式でマシン名を送信します。Active Directory は要求をマシンから送信されていると識別し、認証を実行するコンピュータ オブジェクトを検索します。このオプションが無効になっている場合、Odyssey サプリカントは host\ プレフィックスなしでマシン名を送信します。Active Directory はユーザ オブジェクトを検索し、認証は失敗します。

マシン認証のための AnyConnect エージェント

マシン認証のために AnyConnect エージェントを設定する場合、次のいずれかを実行できます。

- デフォルトのマシン ホスト名（プレフィックス「host/」を含む）を使用する。
- 新しいプロファイルを設定する。その場合、マシン名の前にプレフィックス「host/」を付加する必要があります。

LDAP

Lightweight Directory Access Protocol（LDAP）は、RFC 2251 で規定されている、TCP/IP 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。

Cisco ISE は、LDAP プロトコルを使用して LDAP 外部データベース（ID ソースとも呼ばれる）と統合します。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP ディレクトリ サービス

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 サーバに接続し、操作要求をサーバに送信することで LDAP セッションを開始します。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、つまり識別名（DN）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相対識別名（RDN）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。

関連項目

「LDAP ID ソースの追加」（P.14-25）

複数の LDAP インスタンス

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、Cisco ISE 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、Cisco ISE LDAP ID ソース インスタンスに対応する LDAP インスタンスを形成します。

Cisco ISE では、個々の LDAP インスタンスが一意の 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、Cisco ISE が認証要求を送信するユーザ ディレクトリとグループ 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。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP フェールオーバー

Cisco ISE 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をサポートします。フェールオーバーは、LDAP サーバがダウンしているか、そうでなければ到達不能であることから Cisco ISE 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発生します。

フェールオーバー設定を確立し、Cisco ISE 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 Cisco ISE は 2 番めの LDAP サーバへの接続を試みます。Cisco ISE に最初の LDAP サーバを再度使用させる場合は、[フェールバック再試行遅延（Failback Retry Delay）] テキスト ボックスに値を入力します。

（注）　Cisco ISE では、常にプライマリ LDAP サーバを使用して、認証ポリシーで使用するグループと属性が管理者ポータルから取得されます。このため、プライマリ LDAP サーバはこれらの項目を設定するときにアクセス可能である必要があります。Cisco ISE では、フェールオーバーの設定に従って、実行時に認証と許可にのみセカンダリ LDAP サーバが使用されます。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP 接続管理

Cisco ISE 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。開いている接続の数は、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基づいて決まります。

Cisco ISE は、Cisco ISE で設定されている LDAP サーバごとに、開いている LDAP 接続（バインディング情報を含む）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後、Connection Manager は接続を解放します。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP ユーザ認証

LDAP は、Cisco ISE ユーザ認証用の外部データベースとして使用できます。Cisco ISE では、プレーン パスワード認証がサポートされます。ユーザ認証は次のとおりです。

- 要求内のユーザ名と一致するエントリの LDAP サーバを検索する
- ユーザ パスワードを LDAP サーバで見つかったパスワードと照合する
- ポリシーで使用するために、グループのメンバーシップ情報を取得する
- ポリシーおよび許可プロファイルで使用するために指定した属性の値を取得する

ユーザを認証するために、Cisco ISE は LDAP サーバにバインド要求を送信します。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。

Secure Sockets Layer（SSL）を使用して LDAP サーバへの接続を保護することを推奨します。

関連項目

「LDAP ID ソースの追加」（P.14-25）

認可ポリシーで使用する LDAP グループおよび属性検索

Cisco ISE は、ディレクトリ サーバでバインド操作を実行し、サブジェクトを検索および認証することによって、LDAP ID ソースに対してサブジェクト（ユーザまたはホスト）を認証できます。認証が成功した後、Cisco ISE は要求された場合は常にサブジェクト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、Cisco ISE 管理者ポータルで [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択して設定できます。Cisco ISE は、これらのグループおよび属性を使用してサブジェクトを許可できます。

ユーザの認証または LDAP ID ソースの問い合わせを行うために、Cisco ISE は LDAP サーバに接続し、接続プールを保持します。

関連項目

- 「LDAP ID ソースの追加」（P.14-25）
- 「LDAP 接続管理」（P.14-21）

LDAP 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、Cisco ISE 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、次のものとしてグループに供給できます。
  - 識別名
  - 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 ソースには、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。

- [参照方向（Reference direction）]：このパラメータは、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（グループからサブジェクトへまたはサブジェクトからグループへ）。
- [グループ マップ属性（Group map attribute）]：このパラメータは、グループ メンバーシップ情報を含む属性を示します。
- [グループ オブジェクト クラス（Group object class）]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー（Group search subtree）]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバー タイプ オプション（Member type option）]：このパラメータは、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）。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP 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、Cisco ISE 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 ソースのインスタンスごとに、ID ソース 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。

- String
- 符号なし 32 ビット整数
- IPv4 address

符号なし整数および IPv4 属性の場合、Cisco ISE 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、Cisco ISE 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 Cisco ISE で属性に対して値が取得されなかった場合、Cisco ISE 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。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP 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、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP サーバによって返されたエラー

次のエラーが認証プロセス中に発生する可能性があります。

- 認証エラー：Cisco ISE は認証エラーを Cisco ISE ログ ファイルにロギングします。

LDAP サーバがバインディング（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。

- 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（無効、ロックアウト、期限切れ、パスワード期限切れなど）
- 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 Cisco ISE 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。

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

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP ユーザ ルックアップ

Cisco ISE では、LDAP サーバによるユーザ ルックアップ機能がサポートされます。この機能を使用すると、認証なしで LDAP データベース内のユーザを検索し、情報を取得できます。ユーザ ルックアップ プロセスには次のアクションが含まれます。

- 要求内のユーザ名と一致するエントリの LDAP サーバを検索する
- ポリシーで使用するために、ユーザのグループ メンバーシップ情報を取得する
- ポリシーおよび許可プロファイルで使用するために指定した属性の値を取得する

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP MAC アドレス ルックアップ

Cisco ISE では、MAC アドレス ルックアップ機能がサポートされます。この機能を使用すると、認証なしで LDAP データベース内の MAC アドレスを検索し、情報を取得できます。MAC アドレス ルックアップ プロセスには次のアクションが含まれます。

- デバイスの MAC アドレスと一致するエントリの LDAP サーバを検索する
- ポリシーで使用するために、デバイスの MAC アドレス グループ情報を取得する
- ポリシーで使用するために指定した属性の値を取得する

関連項目

「LDAP ID ソースの追加」（P.14-25）

LDAP ID ソースの追加

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE では、常にプライマリ LDAP サーバを使用して、認証ポリシーで使用するグループと属性が取得されます。このため、プライマリ LDAP サーバはこれらの項目を設定するときに到達可能である必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] > [追加（Add）] を選択します。

ステップ 2　値を入力します。

ステップ 3　[送信（Submit）] をクリックして、LDAP インスタンスを作成します。

関連項目

「LDAP ID ソース設定」（P.A-31）

次の作業

- 「プライマリおよびセカンダリ LDAP サーバの設定」（P.14-25）
- 「LDAP サーバから属性を取得するための Cisco ISE の有効化」（P.14-26）
- 「LDAP サーバからのグループ メンバーシップ詳細の取得」（P.14-26）
- 「LDAP サーバからのユーザ属性の取得」（P.14-27）

プライマリおよびセカンダリ LDAP サーバの設定

LDAP インスタンスを作成したら、プライマリ LDAP サーバの接続設定を行う必要があります。セカンダリ LDAP サーバの設定は任意です。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2　編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3　[接続（Connection）] タブをクリックして、プライマリおよびセカンダリ サーバを設定します。

ステップ 4　LDAP の接続設定に説明されているように値を入力します。

ステップ 5　[送信（Submit）] をクリックして接続パラメータを保存します。

関連項目

- 「LDAP ID ソースの追加」（P.14-25）
- 「LDAP サーバから属性を取得するための Cisco ISE の有効化」（P.14-26）
- 「LDAP サーバからのグループ メンバーシップ詳細の取得」（P.14-26）
- 「LDAP サーバからのユーザ属性の取得」（P.14-27）

LDAP 接続タブのフィールドの設定

次の表では、[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] 編集ページのフィールドについて説明します。

LDAP サーバから属性を取得するための Cisco ISE の有効化

Cisco ISE が LDAP サーバからユーザおよびグループのデータを取得するには、Cisco ISE で LDAP ディレクトリの詳細を設定する必要があります。LDAP ID ソースでは、次の 3 つの検索が適用されます。

- 管理のためのグループ サブツリーのすべてのグループの検索
- ユーザを特定するためのサブジェクト サブツリーのユーザの検索
- ユーザが所属するグループの検索

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2　編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3　[ディレクトリ構成（Directory Organization）] タブをクリックします。

ステップ 4　[LDAP] の [ディレクトリ構成（Directory Organization）] タブに説明されているように値を入力します。

ステップ 5　設定を保存するには、[送信（Submit）] をクリックします。

LDAP サーバからのグループ メンバーシップ詳細の取得

新しいグループを追加するか、または LDAP ディレクトリからグループを選択できます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2　編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3　[グループ（Groups）] タブをクリックします。

ステップ 4　[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。

a. グループの追加を選択した場合は、新しいグループの名前を入力します。

b. ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。検索条件には、アスタリスク（*）ワイルドカード文字を含めることができます。

ステップ 5　選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

選択したグループが [グループ（Groups）] ページに表示されます。

ステップ 6　グループ選択を保存するには、[送信（Submit）] をクリックします。

LDAP サーバからのユーザ属性の取得

認可ポリシーで使用するために LDAP サーバからユーザ属性を取得できます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2　編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3　[属性（Attributes）] タブをクリックします。

ステップ 4　[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバから属性を選択します。

a. 属性を追加する場合は、新しい属性の名前を入力します。

b. ディレクトリから選択する場合、サンプル ユーザを入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。アスタリスク（*）ワイルドカード文字を使用できます。

ステップ 5　選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6　属性選択を保存するには、[送信（Submit）] をクリックします。

次の作業

1. 認証ポリシーの作成方法については、第 19 章「認証ポリシーの管理」を参照してください。
2. 許可プロファイルおよびポリシーの作成方法については、第 20 章「許可ポリシーおよびプロファイルの管理」を参照してください。

RADIUS トークン ID ソース

RADIUS プロトコルをサポートし、ユーザおよびデバイスに認証、許可、アカウンティング（AAA）サービスを提供するサーバは、RADIUS サーバと呼ばれます。RADIUS ID ソースは、サブジェクトとそのクレデンシャルの集合を含み、通信に RADIUS プロトコルを使用する外部 ID ソースです。たと

えば、Safeword トークン サーバは、複数のユーザおよびそのクレデンシャルをワンタイム パスワードとして含めることができる ID ソースであり、Safeword トークン サーバによって提供されるインターフェイスでは、RADIUS プロトコルを使用して問い合わせることができます。

Cisco ISE では、RADIUS RFC 2865 準拠のいずれかのサーバが外部 ID ソースとしてサポートされています。Cisco ISE 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 ソースは、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 ソースでは、認証セッションにユーザ データグラム プロトコル（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。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバによってサポートされる認証プロトコル

Cisco ISE では、RADIUS ID ソース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
- 内部拡張認証プロトコル - 汎用トークン カード（EAP-GTC）を含む保護拡張認証プロトコル（PEAP）
- 内部 EAP-GTC を含む EAP-FAST

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバにより通信に使用されるポート

RADIUS ID トークン サーバでは、認証セッションに UDP ポートが使用されます。このポートはすべての RADIUS 通信に使用されます。Cisco ISE で RADIUS ワンタイム パスワード（OTP）メッセージを RADIUS 対応トークン サーバに送信するには、Cisco ISE と RADIUS 対応トークン サーバ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、管理者ポータルを介して設定できます。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS 共有秘密

Cisco ISE で RADIUS ID ソースを設定するときに、共有秘密を指定する必要があります。この共有秘密情報は、RADIUS トークン 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。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）

- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバでのフェールオーバー

Cisco ISE では、複数の RADIUS ID ソースを設定できます。各 RADIUS ID ソースには、プライマリとセカンダリの RADIUS サーバを指定できます。Cisco ISE 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。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバで設定可能なパスワード プロンプト

RADIUS ID ソースでは、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、管理者ポータルを介して設定できます。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバのユーザ認証

Cisco ISE は、ユーザ クレデンシャル（ユーザ名とパスコード）を取得し、RADIUS トークン サーバに渡します。また、Cisco ISE は RADIUS トークン サーバ認証処理の結果をユーザに中継します。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバでの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 Cisco ISE 機能に不可欠です。

- PEAP セッション再開：この機能によって、認証の成功後、EAP セッションの確立中に PEAP セッションを再開できます。
- EAP/FAST 高速再接続：この機能によって、認証の成功後、EAP セッションの確立中に高速再接続が可能になります。

Cisco ISE 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 Cisco ISE ノード間で複製されません。管理者ポータル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。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

ID 順序での RADIUS ID ソース

ID ソース順序で認証順序用の RADIUS ID ソースを追加できます。ただし、属性取得順序用の RADIUS ID ソースを追加することはできません。これは、認証しないで RADIUS ID ソースを問い合わせることはできないためです。Cisco ISE では、RADIUS サーバによる認証中に、異なるエラーを区別できません。すべてのエラーに対して 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。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

すべてのエラーに対して同じメッセージを返す RADIUS サーバ

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。Cisco ISE には、管理者ポータルを使用して、このメッセージを、「認証に失敗（Authentication Failed）」か、または「ユーザが見つからない（User Not Found）」メッセージとして設定するオプションがあります。ただし、このオプションを使用すると、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「ユーザが見つからない（User Not Found）」メッセージが返されます。

表 14-3 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 14-3　エラー処理

失敗状況	失敗の理由
認証に失敗	• 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。

表 14-3　エラー処理 （続き）

失敗状況	失敗の理由
プロセスの失敗	• RADIUS サーバが Cisco ISE 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、[拒否で失敗（Fail on Reject）] オプションが false に設定されている。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

Safeword サーバでサポートされる特別なユーザ名フォーマット

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

Cisco ISE では、認証要求を受信するとすぐにユーザ名が解析され、次のユーザ名に変換されます。

ユーザ名：Username

Safeword トークン サーバでは、これらの両方のフォーマットがサポートされています。Cisco ISE 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、Cisco ISE 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、管理者ポータルで [SafeWord サーバ（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 ソースで実行されます。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバでの認証要求と応答

Cisco ISE が RADIUS 対応トークン サーバに認証要求を転送する場合、RADIUS 認証要求には次の属性が含まれます。

- User-Name（RADIUS 属性 1）
- User-Password（RADIUS 属性 2）
- NAS-IP-Address（RADIUS 属性 4）

Cisco ISE では、次のいずれかの受信を要求します。

- Access-Accept：属性は必要ありませんが、応答には RADIUS トークン サーバの設定に基づいてさまざまな属性が含まれる場合があります。
- Access-Reject：属性は必要ありません。
- Access-Challenge：RADIUS RFC ごとに必要な属性は次のとおりです。
  - State（RADIUS 属性 24）
  - Reply-Message（RADIUS 属性 18）
  - 次の 1 つ以上の属性：Vendor-Specific、Idle-Timeout（RADIUS 属性 28）、Session-Timeout（RADIUS 属性 27）、Proxy-State（RADIUS 属性 33）

  Access-Challenge ではそれ以外の属性は使用できません。

関連項目

- 「RADIUS トークン サーバの追加」（P.14-32）
- 「RADIUS トークン サーバの削除」（P.14-33）

RADIUS トークン サーバの追加

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS Token（RADIUS トークン）] > [追加（Add）] を選択します。

ステップ 2　[一般（General）] および [接続（Connection）] タブに値を入力します。

ステップ 3　[認証（Authentication）] タブをクリックします。

このタブでは、RADIUS トークン サーバからの Access-Reject メッセージへの応答を制御できます。この応答は、クレデンシャルが無効であること、またはユーザが不明であることのいずれかを意味する場合があります。Cisco ISE は、認証失敗か、またはユーザが見つからないかのいずれかの応答を受け入れます。このタブでは、ID キャッシングを有効にし、キャッシュのエージング タイムを設定することもできます。パスワードを要求するプロンプトを設定することもできます。

ステップ 4　次のことを選択します。

- RADIUS トークン サーバからの Access-Reject 応答を認証失敗として処理する場合は、[拒否を「認証失敗」として処理（Treat Rejects as 'authentication failed'）] オプション ボタンをクリックします。
- RADIUS トークン サーバからの Access-Reject 応答を未知ユーザ エラーとして処理する場合は、[拒否を「ユーザが見つからない」として処理（Treat Rejects as 'user not found'）] オプション ボタンをクリックします。
- パスワードを要求するプロンプトを入力します。

ステップ 5　[許可（Authorization）] タブをクリックします。

このタブでは、Cisco ISE への Access-Accept 応答を送信中に RADIUS トークン サーバによって返されるこの単一の属性に対して表示される名前を設定できます。この属性は、許可ポリシー条件で使用できます。[属性名 ACS（Attribute Name ACS）] フィールドに、この属性の名前を入力します。デフォルト値は CiscoSecure-Group-Id です。

ステップ 6　[送信（Submit）] をクリックして RADIUS トークン ID ソースを保存します。

次の作業

1. 認証ポリシーの作成方法については、第 19 章「認証ポリシーの管理」を参照してください。
2. 許可プロファイルおよびポリシーの作成方法については、第 20 章「許可ポリシーおよびプロファイルの管理」を参照してください。

関連項目

「RADIUS トークン D ソース設定」（P.A-35）

RADIUS トークン サーバの削除

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ID ソース順序に含まれる RADIUS トークン サーバを選択していないことを確認します。ID ソース順序に含まれる RADIUS トークン サーバを削除用に選択した場合、削除操作は失敗します。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS Token（RADIUS トークン）] を選択します。

ステップ 2　削除する RADIUS トークン サーバの隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3　[OK] をクリックして、選択した RADIUS トークン サーバを削除します。

削除する RADIUS トークン サーバを複数選択し、その 1 つが ID ソース順序で使用されている場合、削除操作は失敗し、いずれの RADIUS トークン サーバも削除されません。

RSA ID ソース

Cisco ISE 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 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に登録された RSA SecurID トークンで構成されます。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。

Cisco ISE では、次の RSA ID ソースがサポートされています。

- RSA ACE/Server 6.x シリーズ
- RSA Authentication Manager 7.x シリーズ

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。

Cisco ISE 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接続します。

Cisco ISE Release 1.2 では、1 つの RSA 領域だけがサポートされています。

この項では、次のトピックを扱います。

- 「Cisco ISE と RSA SecurID サーバとの統合」（P.14-34）
- 「RSA プロンプトの設定」（P.14-38）
- 「RSA メッセージの設定」（P.14-39）

Cisco ISE と RSA SecurID サーバとの統合

Cisco ISE と RSA SecurID サーバを接続するには、次の 2 つの管理ロールが必要です。

- RSA サーバ管理者：RSA システムおよび統合の設定と維持
- Cisco ISE 管理者：RSA SecurID サーバに接続するように Cisco ISE を設定し、設定を維持します

この項では、Cisco ISE に RSA SecurID サーバを外部 ID ソースとして接続するために必要なプロセスについて説明します。RSA サーバについての詳細は、RSA に関するドキュメントを参照してください。

Cisco ISE での RSA 設定

RSA 管理システムでは sdconf.rec ファイルが生成されます。このファイルは RSA システム管理者によって提供されます。このファイルを使用すると、Cisco ISE サーバを領域内の RSA SecurID エージェントとして追加できます。このファイルを参照して Cisco ISE に追加する必要があります。プライマリ Cisco ISE サーバは、複製のプロセスによってこのファイルをすべてのセカンダリ サーバに配布します。

RSA SecurID サーバに対する RSA エージェントの認証

sdconf.rec ファイルがすべての Cisco ISE サーバにインストールされると、RSA エージェント モジュールが初期化され、RSA 生成のクレデンシャルによる認証が各 Cisco ISE サーバで実行されます。展開内の各 Cisco ISE サーバ上のエージェントが正常に認証されると、RSA サーバとエージェント モジュールは securid ファイルをダウンロードします。このファイルは Cisco ISE ファイル システムに存在し、RSA エージェントによって定義された既知の場所にあります。

分散 Cisco ISE 環境での RSA ID ソース

分散 Cisco ISE 環境で RSA ID ソースを管理するには、次の操作が必要です。

- sdconf.rec および sdopts.rec ファイルのプライマリ サーバからセカンダリ サーバへの配布。
- securid および sdstatus.12 ファイルの削除。

Cisco ISE 展開での RSA サーバ更新

Cisco ISE で sdconf.rec ファイルを追加した後、RSA サーバを廃止する、または新しい RSA セカンダリ サーバを追加する場合、RSA SecurID 管理者は sdconf.rec ファイルを更新することがあります。更新されたファイルは RSA SecurID 管理者によって提供されます。更新されたファイルによって Cisco ISE を再設定できます。Cisco ISE では、更新されたファイルが複製プロセスによって展開内のセカンダリ Cisco ISE サーバに配布されます。Cisco ISE では、まずファイル システムのファイルを更新し、RSA エージェント モジュールに合わせて調整して再起動プロセスを適切に段階的に行います。sdconf.rec ファイルが更新されると、sdstatus.12 および securid ファイルがリセット（削除）されます。

自動 RSA ルーティングの上書き

領域内に複数の RSA サーバを持つことができます。sdopts.rec ファイルはロード バランサの役割を果たします。Cisco ISE サーバと RSA SecurID サーバはエージェント モジュールを介して動作します。Cisco ISE に存在するエージェント モジュールは、領域内の RSA サーバを最大限に利用するためにコストベースのルーティング テーブルを保持します。ただし、領域の各 Cisco ISE サーバの手動設定を使用してこのルーティングを上書きするには、管理者ポータルで sdopts.rec と呼ばれるテキスト ファイルを使用します。このファイルの作成方法については、RSA に関するドキュメントを参照してください。

RSA ノードの秘密のリセット

securid ファイルは秘密ノード キー ファイルです。RSA が最初に設定されると、RSA では秘密を使用してエージェントが検証されます。Cisco ISE に存在する RSA エージェントが RSA サーバに対して初めて正常に認証されると、securid と呼ばれるファイルがクライアント マシン上に作成され、このファイルを使用して、マシン間で交換されるデータが有効であることが確認されます。展開内の特定の Cisco ISE サーバまたはサーバのグループから securid ファイルを削除する必要がある場合があります（たとえば、RSA サーバでのキーのリセット後など）。このファイルを領域の Cisco ISE サーバから削除するには、Cisco ISE 管理者ポータルを使用できます。Cisco ISE の RSA エージェントが次回正常に認証されたとき、新しい securid ファイルが作成されます。

（注） ISE 1.2 へのアップグレード後に認証が失敗した場合、RSA シークレットをリセットする必要があります。

RSA 自動アベイラビリティのリセット

sdstatus.12 ファイルは、領域内の RSA サーバのアベイラビリティに関する情報を提供します。たとえば、いずれのサーバがアクティブで、いずれのサーバがダウンしているかに関する情報を提供します。エージェント モジュールは領域内の RSA サーバと連携して、このアベイラビリティ ステータスを維持します。この情報は、sdstatus.12 ファイルに連続的に表示されます。このファイルは、Cisco ISE ファイル システムの既知の場所に供給されます。このファイルは古くなり、現在のステータスが反映されていないことがあります。その場合、現在のステータスが反映されるように、このファイルを削除する必要があります。そのファイルを特定の領域の特定の Cisco ISE サーバから削除するには、管理者ポータルを使用できます。Cisco ISE は RSA エージェントに合わせて調整して、再起動が正しく段階的に行われるようにします。

アベイラビリティ ファイル sdstatus.12 は、securid ファイルがリセットされるか、sdconf.rec または sdopts.rec ファイルが更新されるたびに削除されます。

関連項目

- 「RSA コンフィギュレーション ファイルのインポート」（P.14-36）
- 「Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット」（P.14-37）
- 「RSA ID ソースの追加」（P.14-36）

RSA ID ソースの追加

RSA ID ソースを作成するには、RSA コンフィギュレーションファイル（sdconf.rec）をインポートする必要があります。詳細については、「RSA コンフィギュレーション ファイルのインポート」（P.14-36）を参照してください。

はじめる前に

- RSA 管理者から sdconf.rec ファイルを取得する必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

RSA ID ソースを追加するには、次のタスクを実行します。

- 「RSA コンフィギュレーション ファイルのインポート」（P.14-36）
- 「Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット」（P.14-37）
- 「RSA ID ソースに対する認証制御オプションの設定」（P.14-37）

RSA コンフィギュレーション ファイルのインポート

RSA ID ソースを Cisco ISE に追加するには、RSA コンフィギュレーションファイルをインポートする必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）] を選択します。

ステップ 2　[参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdconf.rec ファイルまたは更新された sdconf.rec ファイルを選択します。

初めて RSA ID ソースを作成する場合、[新しい sdconf.rec ファイルのインポート（Import new sdconf.rec file）] フィールドは必須フィールドです。これ以降は、既存の sdconf.rec ファイルを更新されたファイルで置き換えることができますが、既存のファイルの置き換えは任意です。

ステップ 3　サーバのタイムアウト値を秒単位で入力します。Cisco ISE はタイムアウトになる前に、指定された秒数 RSA サーバからの応答を待ちます。この値には、1 ～ 199 の任意の整数を指定できます。デフォルト値は 30 秒です。

ステップ 4　PIN が変更された場合に強制的に再認証するには、[変更 PIN で再認証（Reauthenticate on Change PIN）] チェックボックスをオンにします。

ステップ 5　[保存（Save）] をクリックします。

Cisco ISE は、次のシナリオもサポートします。

- 「Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット」（P.14-37）

• 「RSA ID ソースに対する認証制御オプションの設定」（P.14-37）

Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット

ステップ 1　Cisco ISE Server にログインします。

ステップ 2　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）] を選択します。

ステップ 3　[RSA インスタンス ファイル（RSA Instance Files）] タブをクリックします。

このページには、展開内のすべての Cisco ISE サーバの sdopts.rec ファイルが一覧表示されます。

ステップ 4　特定の Cisco ISE サーバの sdopts.rec ファイルの横にあるオプション ボタンをクリックし、[オプション ファイルの更新（Update Options File）] をクリックします。

[現在のファイル（Current File）] 領域に既存のファイルが表示されます。

ステップ 5　次のいずれかを選択します。

- [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（Use the Automatic Load Balancing status maintained by the RSA agent）] : RSA エージェントでロード バランシングを自動的に管理する場合は、このオプションを選択します。
- [次で選択された sdopts.rec ファイルで自動ロード バランシング ステータスを上書き（Override the Automatic Load Balancing status with the sdopts.rec file selected below）] : 特定のニーズに基づいて手動でロード バランシングを設定する場合は、このオプションを選択します。このオプションを選択する場合は、[参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdopts.rec ファイルを選択する必要があります。

ステップ 6　[OK] をクリックします。

ステップ 7　Cisco ISE サーバに対応する行をクリックして、そのサーバの securid および sdstatus.12 ファイルをリセットします。

a.　ドロップダウン矢印をクリックし、[securid ファイルのリセット（Reset securid File）] 列と [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] 列の [送信で削除（Remove on Submit）] を選択します。

（注）　[sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] フィールドはユーザのビューから非表示になっています。このフィールドを表示するには、最も内側のフレームで垂直および水平スクロール バーを使用して、下にスクロールし、次に右にスクロールします。

b.　この行で [保存（Save）] をクリックして変更を保存します。

ステップ 8　[保存（Save）] をクリックします。

RSA ID ソースに対する認証制御オプションの設定

Cisco ISE が認証失敗を定義する方法を指定し、ID キャッシングを有効にすることができます。RSA ID ソースでは、「認証失敗」エラーと「ユーザが見つからない」エラーは区別されず、Access-Reject 応答が送信されます。

Cisco ISE が要求の処理およびエラーの報告中にこのようなエラーを処理する方法を定義できます。ID キャッシングによって、Cisco ISE では、Cisco ISE サーバに対して認証に失敗した要求を 2 回めに処理できます。前の認証から取得された結果および属性を、キャッシュで利用できます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）] を選択します。

ステップ 2　[認証制御（Authentication Control）] タブをクリックします。

ステップ 3　次のいずれかを選択します。

- [拒否を「認証失敗」として処理（Treat Rejects as "authentication failed"）] : 拒否された要求を認証失敗として処理する場合は、このオプションを選択します。
- [拒否を「ユーザが見つからない」として処理（Treat Rejects as "user not found"）] : 拒否された要求をユーザが見つからないエラーとして処理する場合は、このオプションを選択します。

ステップ 4　[保存（Save）] をクリックして設定を保存します。

次の作業

1. 認証ポリシーの作成方法については、第 19 章「認証ポリシーの管理」を参照してください。
2. 許可プロファイルおよびポリシーの作成方法については、第 20 章「許可ポリシーおよびプロファイルの管理」を参照してください。

関連項目

- 「RSA ID ソース」（P.14-33）
- 「RSA プロンプトの設定」（P.14-38）
- 「RSA メッセージの設定」（P.14-39）

RSA プロンプトの設定

Cisco ISE では、RSA SecurID サーバに送信された要求の処理中にユーザに表示される RSA プロンプトを設定できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] を選択します。

ステップ 2　[プロンプト（Prompts）] をクリックします。

ステップ 3　RSA プロンプト設定に説明されているように情報を入力します。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

- 「RADIUS トークン ID ソース」（P.14-27）
- 「RSA ID ソースの追加」（P.14-36）
- 「RSA メッセージの設定」（P.14-39）

RSA メッセージの設定

Cisco ISE では、RSA SecurID サーバに送信された要求の処理中にユーザに表示されるメッセージを設定できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] を選択します。

ステップ 2　[プロンプト（Prompts）] をクリックします。

ステップ 3　[メッセージ（Messages）] タブをクリックします。

ステップ 4　RSA メッセージ設定に説明されているように情報を入力します。

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「RADIUS トークン ID ソース」（P.14-27）
- 「RSA ID ソースの追加」（P.14-36）
- 「RSA プロンプトの設定」（P.14-38）

ID ソース順序

ID ソース順序では、Cisco ISE が異なるデータベース内でユーザ クレデンシャルを検索する順序を定義します。Cisco ISE では、次の ID ソースがサポートされています。

- 内部ユーザ
- ゲスト ユーザ
- Active Directory
- LDAP
- RSA
- RADIUS トークン サーバ
- 証明書認証プロファイル

Cisco ISE に接続されているデータベースの複数にユーザ情報が格納されている場合、Cisco ISE がこれらの ID ソースで情報を検索する順序を定義できます。一致が見つかると、Cisco ISE はそれ以降の検索を行いませんが、クレデンシャルを評価し、ユーザに結果を返します。このポリシーは最初の一致ポリシーです。

関連項目

- 「ID ソース順序の作成」（P.14-40）
- 「ID ソース順序の削除」（P.14-40）

ID ソース順序の作成

はじめる前に

Cisco ISE に外部 ID ソースを設定していることを確認します。外部 ID ソースを設定する方法については、「ID ソース順序」（P.14-39）を参照してください。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。ゲスト ポータル認証ソースの設定方法の詳細については、「スポンサーの ID ソース順序の指定」（P.16-8）を参照してください。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）] を選択します。

ステップ 2　ID ソース順序の名前を入力します。任意で説明を入力することもできます。

ステップ 3　認証に証明書認証プロファイルを使用する場合は、[証明書認証プロファイルの選択（Select Certificate Authentication Profile）] チェックボックスをオンにして、証明書認証プロファイルを選択します。

ステップ 4　[選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5　[選択済み（Selected）] リストで、Cisco ISE がデータ ベースを検索する順序にデータ ベースを並べ替えます。

ステップ 6　[高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合は、このオプション ボタンをクリックします。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合は、このオプション ボタンをクリックします。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7　[送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

関連項目

- 「簡易認証ポリシーの設定」（P.19-23）
- 「ルール ベースの認証ポリシーの設定」（P.19-23）

ID ソース順序の削除

ポリシーで使用しなくなる ID ソース順序を削除できます。

はじめる前に

- 削除する ID ソース順序がいずれの認証ポリシーでも使用されていないことを確認してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。

ステップ 2　削除する ID ソース順序の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3　[OK] をクリックして ID ソース順序を削除します。

レポートでの ID ソースの詳細

Cisco ISE は次のものを介して ID ソースに関する情報を提供します。

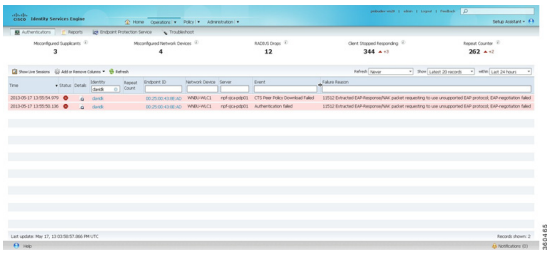
- 「[認証（Authentications）] ダッシュレット」（P.14-41）
- 「ID ソースのレポート」（P.14-42）

[認証（Authentications）] ダッシュレット

[認証（Authentications）] ダッシュレットから、障害の理由などの詳細情報にドリルダウンできます。

図 14-3 に、[認証（Authentications）] ページを示し、詳細にドリルダウンする場合にクリックする必要がある虫眼鏡アイコンを強調表示します。

図 14-3　[認証（Authentications）] ページ



[認証（Authentications）] ページの詳細については、「ライブ認証」（P.25-13）を参照してください。

ID ソースのレポート

Cisco ISE は ID ソースに関する情報を含むさまざまなレポートを提供します。これらのレポートについては、「使用可能なレポート」（P.26-7）を参照してください。

関連項目

- 「レポートの実行および表示」（P.26-2）
- 「レポートのエクスポート」（P.26-2）