Cisco ISE の Active Directory 設定

改訂：2026 年 9 月 22 日

Cisco ISE の Active Directory 設定

Cisco ISE の Active Directory の主な機能

次に、Cisco ISE の Active Directory の主な機能をいくつか示します。

複数参加のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

認証ドメイン

Cisco ISE が Active Directory ドメインに参加している場合、参加ポイントの信頼ドメインを自動的に検出します。ただし、すべてのドメインが認証と認可について Cisco ISE に関連しているとはかぎりません。Cisco ISE では、認証と認可のために信頼ドメインからドメインのサブセットを選択することができます。このドメインのサブセットは、認証ドメインと呼ばれます。ユーザーまたはマシンが配置され、認証するドメインを認証ドメインとして定義することを推奨します。認証ドメインを定義すると、ドメインをブロックしてこれらのドメインでのユーザー認証を制限することによって、セキュリティが強化されます。また、ポリシーおよび認証に関係しないドメインをスキップできるためパフォーマンスが最適化され、Cisco ISE は ID 検索操作をより効率的に実行できるようになります。

ID 書き換え

この機能によって、Cisco ISE は、クライアントまたは証明書から受信するユーザー名を、認証のために Active Directory に送信する前に変更できます。たとえば、ユーザー名 jdoe@amer.acme.com を jdoe@acme.com に書き換えることができます。この機能を使用すると、認証に失敗するユーザー名またはホスト名を修復できます。

また、証明書 ID や不正にプロビジョニングされた証明書のプロセス要求の ID を書き換えることもできます。非証明書ベースの認証のものか証明書内のものかにかかわらず、同一の ID 書き換えルールを受信ユーザー名またはマシン名に適用できます。

あいまいな ID の解決

Cisco ISE が受信したユーザー名またはマシン名があいまいな場合（一意ではない場合）、認証しようとするとユーザーに問題が発生する可能性があります。ユーザーにドメインマークアップがない場合、または複数のドメインに同じユーザー名の ID が複数ある場合に、ID のクラッシュが発生します。たとえば、userA が domain1 に存在し、別の userA が domain2 に存在する場合です。ID 解決設定を使用すると、このようなユーザーの解決範囲を定義できます。UPN や NetBIOS などの修飾名の使用を強く推奨します。修飾名によって、あいまいになる可能性が削減され、遅延を減らすことでパフォーマンスが向上します。

セキュリティ ID に基づいたグループメンバーシップ評価

ISE は、グループ メンバーシップ評価の最適化にセキュリティ ID（SID）を使用します。SID は、グループを評価する効率（スピード）、ドメインが停止している場合やユーザーがドメインのグループ メンバーである場合の遅延に対する復元性という 2 つの理由から有用です。グループを削除して、元と同じ名前で新規グループを作成する場合は、SID を更新して、新規作成したグループに新しい SID を割り当てる必要があります。

ユーザー名ベースの認証テスト（テスト ユーザー）

テスト認証は、エンドユーザーの認証および許可に関する問題のトラブルシューティングに最適です。テストユーザー機能を使用して、Active Directory 認証をテストできます。テストでは、結果とともに管理者ポータルに表示されるグループと属性の詳細（承認情報）が返されます。

診断ツール

診断ツールを使用すると、一般的な接続問題について Active Directory 環境を自動的にテストおよび診断することができます。このツールは、次の情報を提供します。

- テストを実行する Cisco ISE ノード
- Active Directory との接続
- ドメインの詳細なステータス
- Cisco ISE-DNS サーバの接続に関する詳細なステータス

ツールは、実行するテストごとに詳細なレポートを提供します。

証明書認証プロファイル

- 証明書のすべてのサブジェクトまたは代替名属性（Active Directory の場合のみ）のオプション：このオプションを使用すると、ログのユーザー名として Active Directory UPN を使用し、ユーザー名の検索に証明書内のすべてのサブジェクト名および代替名を試行できます。このオプションは、ID ソースとして Active Directory を選択した場合にのみ使用できます。
- ID のあいまいさの解決のみのオプション：このオプションを使用すると、EAP-TLS 認証の ID 問題を解決できます。TLS 証明書の複数の ID を持つことができます。ユーザー名があいまいな場合（たとえば、2 つの jdoe が取得される場合やクライアント証明書が Active Directory にある場合）、Cisco ISE はバイナリ比較を使用してあいまいさを排除することができます。

ノードビュー

このページを使用して、Cisco ISE 展開内の各ノードの参加ポイントのステータスを表示できます。ノード ビューは、読み取り専用ページで、ステータスのみを表示します。このページは、参加、脱退、またはテストのオプションはサポートしません。ただし、各参加ポイントには、これらの操作を実行できる主要な参加ポイント ページへのリンクが示されています。このページには、最新の診断ステータスおよび診断ツールへのリンクも表示されます。

レポートとアラーム

Cisco ISE は、ダッシュボードに、Active Directory 関連のアクティビティのモニタリングおよびトラブルシューティングを実行する新しい AD コネクタ操作レポートおよびアラームを提供しています。

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DC、GC、DC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。また、このページでは、暗号の無効化などのトラブルシューティング オプションも提供します。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 ガイダンスに従って使用する必要があります。

Active Directory と Cisco ISE の統合の前提条件

この項では、Cisco ISE と統合する Active Directory を設定するために必要な手動での作業手順について説明します。ただしほとんどの場合、Cisco ISE が Active Directory を自動的に設定するようにできます。次に、Cisco ISE と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- Cisco ISE でのネットワーク管理者またはシステム管理者の権限があることを確認します。
- Cisco ISE サーバーと Active Directory 間の時間を同期するために Network Time Protocol（NTP）サーバー設定を使用します。Cisco ISE CLI で NTP を設定できます。
- Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。特定の参加ポイントから他のドメインを照会する場合は、参加ポイントと、アクセスする必要があるユーザー情報およびマシン情報があるその他のドメインの間に信頼関係が確立されていることを確認します。信頼関係が確立されていない場合は、信頼できないドメインへの別の参加ポイントを作成する必要があります。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。
- Cisco ISE の参加先ドメインでは、少なくとも 1 つのグローバル カタログ サーバーが動作し、Cisco ISE からアクセス可能である必要があります。

（注） Cisco ISE CLI を Active Directory と統合する場合、AD パスワードに特殊文字「!」を含めることはできません。パスワードにこの文字が含まれていると、「事前認証に失敗しました（Pre-Authentication Failed）」というエラーメッセージが表示され、統合が失敗します。この制約事項は、CLI ベースの統合にのみ適用されます。GUI 統合にはこの制限はありません。

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	脱退処理	Cisco ISE マシンアカウント
参加操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがあるかどうかの確認） • ドメインに Cisco ISE 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（Cisco ISE マシンアカウント パスワード、SPN、dnsHostname など）	脱退操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがあるかどうかの確認） • ドメインから Cisco ISE マシンアカウントを削除する権限 強制脱退（パスワードなしの脱退）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 接続と通信する ISE マシンアカウントには、次の権限が必要です。 • パスワードを変更する。 • 認証されるユーザーおよびマシンに対応するユーザーおよびマシンオブジェクトを読み取る権限 • 情報を取得するために Active Directory をクエリする権限（信頼ドメイン、代替の UPN サフィックスなど） • tokenGroups 属性を読み取る権限 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 Cisco ISE アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。 複数の参加操作が実行される場合、参加ごとに複数のマシン アカウントが Cisco ISE 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 Cisco ISE に保存されません。新規作成された Cisco ISE マシンアカウントのログイン情報のみが保存されます。

Microsoft Active Directory のセキュリティポリシー「**ネットワーク アクセス：SAM へのリモートの呼び出しを許可するクライアントを制限する**」が改訂されました。このため、Cisco ISE は 15 日ごとにマシンアカウントのパスワードを更新できない場合があります。マシンアカウントのパスワードが更新されない場合、Cisco ISE は Microsoft Active Directory を介してユーザーを認証しません。このイベントを通知するために、Cisco ISE ダッシュボードに [AD：ISE アカウントパスワードの更新に失敗（AD: ISE account password update failed）] アラームが表示されます。

（注） この問題は、Windows Server 2016 Active Directory 以降および Windows 10 バージョン 1607 の制限により発生します。この制限を克服するには、Windows Server 2016 Active Directory 以降または Windows 10 バージョン 1607 を Cisco ISE と統合する場合、レジストリ：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam のレジストリ値を non-zero から空白に設定して、すべてにアクセスを提供する必要があります。これにより、Cisco ISE がそのマシンのアカウントパスワードを更新できるようになります。

セキュリティポリシーにより、ユーザーはローカル セキュリティ アカウント マネージャ（SAM）データベース内と Microsoft Active Directory 内のユーザーとグループを列挙できます。Cisco ISE がマシンアカウントのパスワードを更新できるようにするには、Microsoft Active Directory の設定が正しいことを確認します。影響を受ける Windows オペレーティングシステムと Windows Server のバージョン、ネットワークにおけるこのセキュリティポリシーの意味、必要な変更の詳細については、こちらのドキュメントを参照してください。

通信用に開放する必要があ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	注記
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバー/AD ドメイン コントローラ	×	—
MSRPC	445	ドメイン コントローラ	対応	—
Kerberos（TCP/UDP）	88	ドメイン コントローラ	あり（Kerberos）	MS AD/KDC
LDAP（TCP/UDP）	389	ドメイン コントローラ	対応	—
LDAP（GC）	3268	グローバル カタログ サーバー	対応	—
NTP	123	NTP サーバー/ドメイン コントローラ	×	—
IPC	80	展開内の他の ISE ノード	あり（RBAC クレデンシャルを使用）	—

DNS サーバー

DNS サーバーを設定する場合は、次の前提条件に注意してください。

- Cisco ISE に設定されている DNS サーバーで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS 再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバーで Active Directory レコードを解決することをお勧めします。

- すべての DNS サーバーで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。
- パフォーマンスを向上させるために、SRV 応答にサーバー IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバーを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

Active Directory 参加ポイントの追加と参加ポイントへの Cisco ISE ノードの参加

始める前に

Cisco ISE ノードが、NTP サーバー、DNS サーバー、ドメインコントローラ、グローバルカタログサーバーが配置されているネットワークと通信できることを確認します。ドメイン診断ツールを実行して、これらのパラメータをチェックできます。

Active Directory と、パッシブ ID ワーク センターのエージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

Active Directory と統合する際に IPv6 を使用する場合は、関連する ISE ノードで IPv6 アドレスが設定されていることを確認する必要があります。

Google Chrome ブラウザを使用し、広告ブロックソフトウェアを有効にしている場合は、広告ブロッカーを無効にする必要があります。このタスクには、広告ブロッカーの影響を受ける Cisco ISE GUI 要素が含まれています。または、Google Chrome シークレットブラウザでこのタスクを実行できます。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 [追加（Add）] をクリックして、[Active Directory 参加ポイント名（Active Directory Join Point Name）] の設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、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 ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックするか、または左側のナビゲーションペインから新しい Active Directory 参加ポイントをクリックします。展開の参加/脱退テーブルに、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が表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE ノードをドメインに参加させるには、使用するアカウントのユーザー名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE ノードを追加するために異なるユーザー名とパスワードが必要な場合は、Cisco ISE ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザー名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。

参加操作に使用するユーザーは、ドメイン自体に存在する必要があります。ユーザーが異なるドメインまたはサブドメインに存在する場合、ユーザー名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意） [組織ユニットの指定（Specify Organizational Unit）] チェックボックスをオンにします。

このチェックボックスは、Cisco ISE ノードのマシンアカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE は、指定された組織ユニットの下にマシンアカウントを作成するか、またはマシンアカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジ リターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシンアカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [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、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します。

参加ポイントを設定する際は、次の点に注意してください。

- 複数の参加ポイントを使用する場合、代替 UPN サフィックスが単一の参加ポイントまたはドメインに対してのみ設定されている場合、アイデンティティ ルックアップはその参加ポイントまたはドメインでのみ実行されます。このような場合、認証が失敗する可能性があります。回避策として、すべての参加ポイントまたはドメインに代替 UPN サフィックスを設定できます。

- ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DC の数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。展開用のドメインコントローラのテスト済みスケール制限の詳細については、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。
- 参加が完了すると、Cisco ISE によりその AD グループと対応するセキュリティ識別子（SID）が更新されます。Cisco ISE は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。
- DNS サービス（SRV）レコードが欠落している（参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE を参加させることができない可能性があります。
- 指定されたメンテナンスウィンドウの後に AD に再参加することを推奨します。これにより、AD キャッシュが最新の更新内容で更新されます。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントからユーザーとマシンを認証する必要がない場合は、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場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE ノードがすでに参加している場合は、Active Directory ドメインから切断されます。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。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE ホスト名を変更する場合にも推奨されます。

始める前に

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。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 作成した Active Directory 参加ポイント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。展開の参加/脱退テーブルが、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とともに表示されます。

ステップ 3 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 4 Active Directory のユーザー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 データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE マシン アカウントが削除されます。

（注）
Active Directory データベースから Cisco ISE マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 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。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

認証ドメインの設定

Cisco ISE が参加しているドメインは、信頼関係を持つ他のドメインに対して可視性があります。デフォルトでは、Cisco ISE はこれらすべての信頼ドメインに対する認証を許可するように設定されます。認証ドメインのサブセットに対して、Active Directory 展開との相互作用を制限できます。ドメイン認証を設定することにより、接続ポイントごとに特定のドメインを選択して、選択され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、接続ポイントから信頼されたすべてのドメインではなく、選択されたドメインのユーザーのみを認証するように Cisco ISE に指示するため、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（着信したユーザー名または ID に一致するアカウントの検索）が制限されるため、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、着信したユーザー名または ID にドメイン マークアップ（プレフィクスまたはサフィックス）が含まれていない場合に特に重要です。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。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID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 **Active Directory** の参加ポイントをクリックします。

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

表に、信頼ドメインのリストが表示されます。デフォルトでは、Cisco ISE 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 4 指定したドメインのみを許可するには、[認証にすべての Active Directory ドメインを使用する（Use all Active Directory domains for authentication）] チェックボックスをオフにします。

ステップ 5 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、[選択対象の有効化（Enable Selected）] をクリックします。[認証（Authenticate）] カラムで、このドメインのステータスが [はい（Yes）] に変わります。

また、選択したドメインを無効にすることもできます。

ステップ 6 [使用できないドメインを表示（Show Unusable Domains）] をクリックして、使用できないドメインのリストを表示します。使用できないドメインは、単方向の信頼や選択的な認証などの理由により、Cisco ISE が認証に使用できないドメインです。

次のタスク

Active Directory ユーザー グループを設定します。

サポートされるセキュリティグループタイプ

Cisco ISE では、次のセキュリティグループタイプがサポートされます。

- ユニバーサル
- グローバル
- 組み込み

  組み込みグループには、ドメインで一意のセキュリティ ID（SID）がありません。これを解決するために、Cisco ISE はグループが属する SID にドメイン名を使用してプレフィクスを付けます。

Cisco ISE は、AD 属性の tokenGroups を使用して、ユーザーのグループ メンバーシップを評価します。Cisco ISE マシン アカウントには、tokenGroups 属性を読み取るためのアクセス許可が必要です。この属性には、ユーザーがメンバーである可能性がある最初の約 1015 グループを含めることができます（実際の数は Active Directory 設定によって異なり、Active Directory を再設定することで増やすことができます）。ユーザーが所属するグループの数がこれを超える場合、Cisco ISE はポリシー ルールで最初の 1015 までを使用します。

Active Directory ユーザーグループの設定

Active Directory ユーザー グループを許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。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかの操作を行います。

a) **[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）]** の順に選択し、既存のグループを選択します。

b) **[追加（Add）] > [グループの追加（Add Group）]** の順に選択し、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザー インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザー グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

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 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

（注）
グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

次のタスク

Active Directory のユーザー属性を設定します。

Active Directory ユーザーとマシンの属性の設定

許可ポリシーの条件で使用できるように Active Directory ユーザーとマシンの属性を設定する必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] >** [Active Directory] の順に移動します。

ステップ 2 [属性（Attributes）] タブをクリックします。

ステップ 3 **[追加（Add）] > [属性の追加（Add Attribute）]** を選択して属性を手動で追加するか、**[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。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザー認証に IPv4 または IPv6 アドレスを使用して AD を設定できます。

ステップ 4 ディレクトリからの属性の追加を選択した場合、ユーザーの名前を [サンプル ユーザー（Sample User）] フィールドまたは [マシン アカウント（Machine Account）] 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ー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 **administrator** を入力します。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。

（注）
ユーザー名の例を入力する場合、Cisco ISE が接続されているアクティブな Active Directory ドメインからユーザーを選択します。マシン属性を取得するマシンの例を選択する場合、マシン名のプレフィックスとして「host/」を追加するか、SAM$ 形式を使用してください。たとえば、host/myhost を使用します。属性の取得時に表示される値の例は説明のみを目的としており、保存されません。

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 属性を手動で追加する場合は、新しい属性の名前を入力します。

ステップ 7 [保存（Save）] をクリックします。

Active Directory 認証のためのユーザーテスト

Active Directory からユーザー認証を検証するには、[ユーザーのテスト（Test User）] ツールを使用できます。グループおよび属性を取得して調査することもできます。単一の参加ポイントまたはスコープのテストを実行できます。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 次のオプションのいずれかを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）] > [すべての参加ポイントのユーザーをテスト（Test User for All Join Points）]** の順に選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE ノードを選択し、[ユーザーのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザー（またはホスト）のユーザー名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE ノードを選択します。

ステップ 6 Active Directory からグループおよび属性を取得するには、[グループを取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェック ボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順（認証、参照、グループおよび属性の取得）を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE に警告メッセージが表示されます。

Active Directory の複数参加設定のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

同じフォレストに複数回参加できます。つまり、必要に応じて、同じフォレスト内の複数のドメインに参加できます。

Cisco ISE は、単方向の信頼があるドメインに参加できます。このオプションで、単方向の信頼によって生じる権限の問題を回避できます。いずれかの信頼ドメインに参加できるため、両方のドメインを確認できます。

- [参加ポイント（Join Point）]：Cisco ISE では、Active Directory ドメインへの個別参加は、参加ポイントと呼ばれます。Active Directory の参加ポイントは、Cisco ISE の ID ストアであり、認証ポリシーで使用できます。属性およびグループの関連ディクショナリがあり、許可条件で使用できます。
- [スコープ（Scope）]：グループ化された Active Directory の参加ポイントのサブセットは、スコープと呼ばれます。単一参加ポイントの代わりに、認証結果として認証ポリシーでスコープを使用できます。スコープは、複数の参加ポイントに対してユーザーを認証するために使用されます。各参加ポイントに複数のルールを使用する代わりにスコープを使用すると、単一のルールで同じポリシーを作成することができ、Cisco ISE で要求の処理やパフォーマンスの向上にかかる時間を短縮できます。参加ポイントには、複数のスコープが含まれる場合があります。スコープは、ID ソース順序に含まれる場合があります。スコープには関連するディクショナリがないため、許可ポリシー条件にスコープを使用することはできません。

  新しい Cisco ISE のインストールを実行する場合、デフォルトでスコープは存在しません。これは、ノー スコープ モードと呼ばれます。スコープを追加すると、Cisco ISE はマルチスコープ モードになります。必要に応じて、ノー スコープ モードに戻すことができます。すべての参加ポイントは [Active Directory] フォルダに移動されます。

  - Initial_Scope は、ノー スコープ モードで追加された Active Directory 参加ポイントの格納に使用される暗黙のスコープです。マルチスコープ モードを有効にすると、すべての Active Directory 参加ポイントが自動作成された Initial_Scope に移動します。Initial_Scope の名前を変更できます。
  - All_AD_Instances は組み込み型の疑似スコープで、Active Directory 設定には表示されません。これは、認証結果としてポリシーおよび ID 順序にのみ示されます。Cisco ISE で設定されたすべての Active Directory 参加ポイントを選択する場合は、このスコープを選択できます。

ID ソース順序と認証ポリシーの範囲と参加ポイント

Cisco ISE では、複数の Active Directory の参加ポイントを定義できます。各参加ポイントは、異なる Active Directory ドメインへの接続を表します。各参加ポイントは、個別の ID ストアとして、認証ポリシー、認可ポリシーおよび ID 順序で使用できます。参加ポイントはグループ化してスコープを形成できます。スコープは認証ポリシーで、認証結果として、および ID ソース順序で使用できます。

各参加ポイントを完全に独立したポリシー グループとして処理する場合は、認証ポリシーの結果として、または ID ソース順序で、個々の参加ポイントを選択できます。たとえば、Cisco ISE 導入環境で、独自のネットワーク デバイスを持つ独立したグループがサポートされるマルチテナント シナリオでは、ネットワーク デバイス グループを Active Directory ドメインの選択に使用できます。

ただし、Active Directory ドメインが、ドメイン間に信頼がない同じ企業の一部と見なされる場合は、スコープを使用して、接続されていない複数の Active Directory ドメインを結合し、共通の認証ポリシーを作成することができます。これにより、異なる ID ストアによって表されるすべての参加ポイントを認証ポリシーで定義する必要がなくなるため、各ドメインのためのルールが重複することを回避できます。使用される実際の参加ポイントは、認可ポリシーによって使用される認証 ID ストアに含まれます。

ユーザー名が同じで、複数のドメインに複数の ID がある場合、ID のあいまいさが発生します。たとえば、ドメインマークアップのないユーザー名が一意ではなく、Cisco ISE が EAP-TLS などのパスワードのないプロトコルを使用するように設定されている場合、適切なユーザーを検索する他の基準がないため、Cisco ISE はあいまいな ID エラーで認証に失敗します。このようなあいまいな ID が出現した場合、認証ポリシー ルールで特定のスコープや参加ポイントを使用するか、ID ソース順序を使用できます。たとえば、特定のネットワーク デバイス グループのユーザーが特定の Active Directory スコープまたは単一の参加ポイントを使用するようにして、検索スコープを制限することができます。同様に、ID が @some.domain で終了する場合は特定の Active Directory の参加ポイントを使用するなどのルールを作成できます。このことは、適切な参加ポイントで認証が行われるようにするのに役立ちます。

Active Directory 参加ポイントを追加する新しい範囲の作成

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID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 [スコープモード（Scope Mode）] をクリックします。
Initial_Scope と呼ばれるデフォルトのスコープが作成され、現在のすべての参加ポイントがこのスコープに配置されます。

ステップ 3 より多くのスコープを作成するには、[追加（Add）] をクリックします。

ステップ 4 新しいスコープの名前と説明を入力します。

ステップ 5 **[送信（Submit）]** をクリックします。

読み取り専用ドメイン コントローラ

次の操作が読み取り専用ドメインコントローラでサポートされます。

- Kerberos ユーザー認証
- ユーザー ルックアップ
- 属性およびグループの取得

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ーとマシンの認証、Active Directory ユーザー パスワードの変更などの機能をサポートしています。

次の表に、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 *1 : 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 およびパスワード ベースの Protected Extensible Authentication Protocol（PEAP）	MS-CHAPv2 および EAP-GTC の内部方式で EAP-FAST と PEAP を使用するパスワード変更機能を備えたユーザーとマシンの認証
Password Authentication Protocol（PAP）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol Version 1（MS-CHAPv1）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）	ユーザーおよびマシン認証
Extensible Authentication Protocol-Generic Token Card（EAP-GTC）	ユーザーおよびマシン認証
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security（EAP-FAST-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Lightweight Extensible Authentication Protocol（LEAP）	ユーザー認証

Active Directory ユーザー認証プロセスフロー

ユーザーの認証またはクエリ時に、Cisco ISE は次の点をチェックします。

- MS-CHAP および PAP 認証では、ユーザーが無効かどうか、ロックアウトされているかどうか、期限切れかどうか、またはログイン時間外かどうかを確認します。これらの条件のいずれかが true の場合、認証が失敗します。
- EAP-TLS 認証では、ユーザーが無効かどうか、ロックアウトされているかどうかを確認します。これらの条件のいずれかが一致する場合、認証が失敗します。

サポートされるユーザー名の形式

次に、サポートされるユーザー名のタイプを示します。

- SAM（例：jdoe）
- NetBIOS プレフィクス付きの SAM（例：ACME\jdoe）
- UPN（例：jdoe@acme.com）
- Alt UPN（例：john.doe@acme.co.uk）
- サブツリー（例：johndoe@finance.acme.com）
- SAM マシン（例：laptop$）
- NetBIOS プレフィクス付きのマシン（例：ACME\laptop$）
- FQDN DNS マシン（例：host/laptop.acme.com）
- ホスト名のみのマシン（例：host/laptop）

Active Directory のパスワードベース認証

Password Authentication Protocol（PAP）と Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、パスワードベース認証です。MS-CHAP クレデンシャルは、MS-RPC によってのみ認証できます。Cisco ISE では PAP 認証に 2 つのオプション（MS-RPC および Kerberos）があります。MS-RPC も Kerberos も同様にセキュアなオプションです。PAP 認証の MS-RPC はデフォルトであり、次の理由から推奨されるオプションです。

- MS-CHAP との一貫性の確保。
- より明確なエラーレポートの提供。
- Active Directory とのより効率的な通信。MS-RPC の場合、Cisco ISE は参加しているドメインのみからドメイン コントローラに認証要求を送信し、そのドメイン コントローラが要求を処理します。

Kerberos の場合、Cisco ISE は、参加しているドメインからユーザーのアカウント ドメインまで Kerberos のリフェラルに従う必要があります（つまり、Cisco ISE は参加しているドメインからユーザーのアカウント ドメインへの信頼パスにあるすべてのドメインと通信する必要があります）。

Cisco ISE は、ユーザー名の形式を確認し、ドメイン マネージャを呼び出して適切な接続を検索します。アカウント ドメインのドメイン コントローラが検出されたら、Cisco ISE はそれに対してユーザーを認証しようとします。パスワードが一致すると、ユーザーにネットワークへのアクセス権が付与されます。

パスワードベースのマシン認証は、マシン名がホスト/プレフィクス形式であることを除き、ユーザーベース認証によく似ています。この形式（DNS ネームスペース）では、Cisco ISE はそのまま認証することはできません。認証する前に、NetBIOS のプレフィクスが付いた SAM 形式に変換します。

証明書ベースの認証の 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ー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。Active Directory 上のユーザーまたはマシン 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、バイナリ比較の実行に使用します。

証明書認証プロファイルは、証明書の取得に使用する Active Directory のユーザーを検索するためにユーザー名を取得するフィールド（たとえば、サブジェクト代替名（SAN）または一般名）を決定します。Cisco ISE は、証明書を取得した後、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、ユーザーまたはマシン認証に合格します。

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。従来のユーザー名とパスワードの方法で認証する代わりに、Cisco ISE はクライアントから受信した証明書をサーバー内の証明書と比較してユーザーの信頼性を確認します。

始める前に

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。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID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）] > [追加（Add）]** の順に移動します。

ステップ 2 証明書認証プロファイルの名前と説明（任意）を入力します。

ステップ 3 ドロップダウン リストから ID ストアを選択します。

基本証明書のチェックは ID ソースを必要としません。証明書にバイナリ比較チェックが必要な場合は、ID ソースを選択する必要があります。ID ソースとして Active Directory を選択した場合は、サブジェクト名、一般名、およびサブジェクト代替名（すべての値）を使用してユーザーを検索できます。

ステップ 4 [Certificate Attribute] または [Any Subject or Alternative Name Attributes in the Certificate] から **[Use Identity From]** を選択します。これは、ログで検索のために使用されます。

[証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] を選択すると、Active Directory UPN がログ用のユーザー名として使用され、証明書のすべてのサブジェクト名および代替名がユーザーの検索に試行されます。このオプションは、ID ソースとして Active Directory を選択した場合にのみ使用できます。

ステップ 5 **クライアント証明書を ID ストアの証明書と照合する**場合に選択します。この場合、ID ソース（LDAP または Active Directory）を選択する必要があります。[Active Directory] を選択した場合は、ID のあいまいさを解決するためにのみ証明書を照合することを選択できます。

- [なし（Never）]：このオプションは、バイナリ比較を実行しません。
- [ID のあいまいさを解決する目的のみ（Only to resolve identity ambiguity）]：このオプションは、あいまいさが見つかった場合にのみ、クライアント証明書と Active Directory のアカウントの証明書とのバイナリ比較を実行します。たとえば、複数の Active Directory アカウントが証明書の識別名に一致することがあります。
- [常にバイナリ比較を実行する（Always perform binary comparison）]：このオプションは、クライアント証明書と ID ストア（Active Directory または LDAP）内のアカウントの証明書とのバイナリ比較を常に実行します。

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。

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設定の変更

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。詳細については、Active Directory 参加ポイントの追加と参加ポイントへの Cisco ISE ノードの参加 （7 ページ）を参照してください。

Windows Server 2025 でのセキュリティホットパッチの要件：Windows Server 2025 を実行しているドメインコントローラを使用する場合は、Windows セキュリティホットパッチ KB5068861（またはこれに取って変わるそれ以降の累積更新）をインストールする必要があります。このホットパッチがインストールされていない場合、Cisco ISE は Active Directory ドメインに参加できません。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

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

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 必要に応じて、次のオプションを変更します。

- **[パスワードの変更を有効にする（Enable password change）]**

  Cisco ISE リリース 3.3 パッチ 12 以降では、ドメインコントローラでの手動設定なしで Windows Server 2025 Active Directory ドメインに参加できます。ただし、Windows Server 2025 のデフォルトのセキュリティ設定では、ドメインコントローラは、EAP-MS-CHAPv2 または EAP-GTC を介して開始されたユーザーパスワード変更要求を拒否します。そのため、Cisco ISE の [パスワード変更の有効化（Enable Password Change）] 設定は、デフォルトでは無効になっています。

- [マシン認証の有効化（Enable Machine Authentication）]
- [マシンアクセス制限（MAR）の有効化（Enable Machine Access Restrictions (MARs)）]

ステップ 5 [ダイヤルインチェックを有効にする（Enable dial-in check）] チェックボックスをオンにして、マシン認証中またはクエリ中にユーザーのダイヤルインアクセス権を確認します。ダイヤルインアクセス権が拒否された場合、認証チェックの結果は拒否になります。

ステップ 6 認証中またはクエリ中にサーバーからユーザーにコールバックするようにするには、[ダイヤルインクライアントのコールバック チェックを有効にする（Enable callback check for dial-in clients）] チェックボックスをオンにします。サーバーによって使用されるIPアドレスまたは電話番号は、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。ダイヤルインアクセス権が拒否された場合、認証チェックの結果は拒否になります。

ステップ 7 プレーン テキスト認証に Kerberos を使用する場合は、[プレーン テキスト認証に Kerberos を使用（Use Kerberos for Plain Text Authentications）] チェックボックスをオンにします。デフォルトの推奨オプションは MS-RPC です。

（注）
AD で保護されたアカウントの認証を許可するには、このチェックボックスをオンにします。

Active Directory インスタンスに対する承認

ここでは、Cisco ISE が Active Directory に対するユーザーまたはマシンの承認に使用するメカニズムについて説明します。

認証ポリシーで使用する Active Directory 属性およびグループの取得

Cisco ISE は、許可ポリシー ルールで使用するために Active Directory からユーザーまたはマシンの属性およびグループを取得します。これらの属性は Cisco ISE ポリシーで使用され、ユーザーまたはマシンの承認レベルを決定します。Cisco ISE は、認証が成功した後にユーザーおよびマシンの 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、外部 ID ストア内のグループを使用してユーザーまたはコンピュータに権限を割り当てることがあります（たとえば、ユーザーをスポンサー グループにマップします）。Active Directory のグループメンバーシップにおける次の制限事項に注意してください。

- ポリシールールの条件は、ユーザーまたはコンピュータのプライマリグループ、ユーザーまたはコンピュータが直接メンバーであるグループ、または間接的（ネストされた）グループのいずれかを参照します。
- ユーザーまたはコンピュータのアカウント ドメイン外のドメイン ローカル グループはサポートされません。

（注）

- Active Directory 属性の値 msRadiusFramedIPAddress を IP アドレスとして使用できます。この IP アドレスは、許可プロファイルのネットワーク アクセス サーバー（NAS）に送信できます。msRADIUSFramedIPAddress 属性は IPv4 アドレスだけをサポートします。ユーザー認証では、ユーザーに対し取得された msRadiusFramedIPAddress 属性値が IP アドレス形式に変換されます。
- Cisco ISE では、SASL（Simple Authentication and Security Layer）LDAP フレームが 128 KiB に制限されます。エラー 40286 を回避するために、Active Directory の `userCertificate` 属性の合計サイズが常に約 126 KiB 未満になるようにしてください。回避策として、[クライアント証明書をIDストアの証明書と照合（Match Client Certificate Against Certificate In Identity Store）] を [しない（Never）] か [IDのあいまいさを解決する目的のみ（Only to resolve identity ambiguity）] に設定して [証明書認証プロファイル（Certificate Authentication Profile）] を変更します。

属性およびグループは、参加ポイントごとに取得され、管理されます。これらは許可ポリシーで使用されます（まず参加ポイントを選択し、次に属性を選択します）。許可のスコープごとに属性またはグループを定義することはできませんが、認証ポリシーでスコープを使用できます。認証ポリシーでスコープを使用する場合、ユーザーは 1 つの参加ポイントで認証されますが、ユーザーのアカウント ドメインへの信頼できるパスがある別の参加ポイント経由で属性またはグループを取得することができます。認証ドメインを使用して、1 つの範囲内にある 2 つの参加ポイントで認証ドメインが重複しないようにすることができます。

マルチ参加ポイント設定の許可プロセス時に、Cisco ISE は、特定のユーザーが見つかるまで、認証ポリシーに記載されている順序で参加ポイントを検索します。ユーザーが見つかると、参加ポイント内のユーザーに割り当てられた属性とグループが、認証ポリシーを評価するために使用されます。

複数参加ポイント設定で、各参加ポイントからの同じ ID に対して個別に認証が成功する場合、ID ソース順序 "All_AD_Join_Points" に対して認証が行われると、この認証は失敗します。

複数参加ポイント設定で、各参加ポイントからの同じ ID に対して個別に Active Directory グループ取得が成功する場合、Active Directory グループ取得は次の場合に失敗します。

- 異なる参加ポイントが認証と承認に使用される。
- 認証でバイナリ比較なしの EAP-TLS が使用されていて（[Certificate Authentication Profile] で [Match Client Certificate Against Certificate In Identity Store] が [Never] に設定されている）、一致認証ルールの前に、異なる参加ポイントを持つ不一致認証ルールがある。
- 認証でバイナリ比較なしの EAP-TLS が使用されていて（[Certificate Authentication Profile] で [Match Client Certificate Against Certificate In Identity Store] が [Never] に設定されている）、マシンアクセス制限（MAR）が、現在の一致認証ルールの参加ポイントとは別の MAR 期間内の参加ポイントを使用してエンドポイントで有効になっている。

（注）

複数参加ポイント設定で、Active Directory グループ取得は各参加ポイントに対して個別に成功しますが、"All_AD_Join_Points" を含む ID ソース順序で認証ルールが設定されている場合は失敗します。承認と認証に異なる参加ポイントが使用されている場合も、Active Directory グループ取得は失敗します。

使用可能な Active Directory グループの最大数については、Microsoft のドキュメントの制限を参照してください。

ルールに、/、!、@、\、#、$、%、^、&、*、(、)、_、+、または~のような特殊文字を使用したActive Directoryグループ名が含まれる場合、許可ポリシーは失敗します。

管理者ユーザー名に$という文字が含まれている場合、Active Directoryを介した管理者ユーザーのログインが失敗することがあります。

明示的なUPNの使用

ユーザー情報とActive Directoryのユーザープリンシパル名（UPN）属性を照合する場合の不確実性を減らすため、明示的なUPNを使用するようにActive Directoryを設定する必要があります。2人のユーザーが同じ値*sAMAccountName*を使用した場合、暗示的なUPNを使用すると、あいまいな結果が生成されます。

Active Directoryで明示的なUPNを設定するには、[高度な調整（Advanced Tuning）]ページを開いて、属性*REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN*を1に設定します。

ブール属性のサポート

Cisco ISEは、Active DirectoryおよびLDAP IDストアからのブール属性の取得をサポートしています。

Active DirectoryまたはLDAPのディレクトリ属性を設定する際に、ブール属性を設定できます。これらの属性は、Active Directoryまたは LDAPによる認証時に取得されます。

ブール属性は、ポリシー ルール条件の設定に使用できます。

ブール属性値は、文字列型としてActive DirectoryまたはLDAPサーバーから取得されます。Cisco ISEは、次のブール属性値をサポートしています。

ブール属性	サポートされる値
[はい（True）]	t、T、true、TRUE、True、1
いいえ（False）	f、F、false、FALSE、False、0

（注） 属性置換はブール属性ではサポートされません。

文字列型としてブール属性（たとえば、msTSAllowLogon）を設定すると、Active DirectoryまたはLDAPサーバーの属性のブール値はCisco ISEの文字列属性に設定されます。属性タイプをブール型に変更したり、ブール型として属性を手動で追加できます。

認証ポリシーのディクショナリ属性

認可ポリシーは、ディクショナリ属性に基づく条件によって決定されます。Active Directoryの各参加ポイントには、属性およびグループを含む関連ディクショナリがあります。

ディクショナリ	属性	説明
Network Access	AD-User-Join-Point	この属性は、参加ポイントがユーザ認証に使用されたことを示します。

ディクショナリ	属性	説明
Network Access	AD-Host-Join-Point	この属性は、参加ポイントがマシン認証に使用されたことを示します。
Network Access	AD-User-DNS-Domain	この属性は、ドメイン DNS 修飾名がユーザ認証に使用されたことを示します。
Network Access	AD-Host-DNS-Domain	この属性は、ドメイン DNS 修飾名がマシン認証に使用されたことを示します。
Network Access	MachineAuthenticationIdentityStore	この属性は、ID ストアがマシン認証に使用されたことを示します。
Network Access	WasMachineAuthenticated	この属性は、ユーザのマシンが認証済みかどうかを示します。
参加ポイント	ExternalGroups	この属性は、ユーザが属する Active Directory グループを示します。
参加ポイント	IdentityAccessRestricted	この属性は、ユーザアカウントが無効になっていること、またはログイン時間外でアクセス権が付与されていないことを示します。
参加ポイント	<ATTR name>	この属性は、ユーザの Active Directory 属性を示します。

ID 書き換え

ID 書き換えは、外部 Active Directory システムに渡される前に ID を操作するよう Cisco ISE に指示する拡張機能です。ID を必要な形式（任意のドメイン プレフィクスやサフィックスまたはその他の追加マークアップを含むまたは除く）に変更するためのルールを作成できます。

ID 書き換えルールは、サブジェクト検索、認証クエリー、許可クエリーなどの操作のために、クライアントから受信したユーザー名またはホスト名に対して Active Directory に渡される前に適用されます。Cisco ISE は条件のトークンを照合し、最初の 1 つが一致するとポリシーの処理を停止して、結果に応じて ID 文字列を書き換えます。

書き換え時、角カッコ [ ] で囲まれている（[IDENTITY] など）内容はすべて、評価側では評価されず、代わりに文字列内のその場所に一致する文字列が付加される変数です。角カッコなしはすべて、ルールの評価側と書き換え側の両方で、固定文字列として評価されます。

次に、ユーザーによって入力された ID が ACME\jdoe であるとした場合の ID 書き換えの例を示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

結果は jdoe です。このルールは、ACME プレフィクスを持つすべてのユーザー名を削除するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]@ACME.com** に書き換えます。

  結果は jdoe@ACME.com です。このルールは、形式をプレフィクス表記からサフィックス表記に、または NetBIOS 形式から UPN 形式に変更するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**ACME2\[IDENTITY]** に書き換えます。

  結果は ACME2\jdoe です。このルールは、特定のプレフィクスを持つすべてのユーザー名を代替プレフィクスに変更するよう Cisco ISE に指示します。

- ID が **[ACME]\jdoe.USA** と一致する場合、**[IDENTITY]@[ACME].com** に書き換えます。

  結果は jdoe\ACME.com です。このルールは、ドットの後の領域を削除するよう Cisco ISE に指示します。この場合は国名で、正しいドメインに置き換えられます。

- ID が **E=[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。これは、ID が証明書から取得され、フィールドが電子メール アドレスで、Active Directory がサブジェクトで検索するように設定されている場合に作成可能なルールの例です。このルールは、「E=」を削除するように Cisco ISE に指示します。

- ID が **E=[EMAIL],[DN]** と一致する場合、**[DN]** に書き換えます。

  このルールは、証明書サブジェクトを、E= jdoe@acme.com、CN=jdoe、DC=acme、DC=com から単なる DN、CN=jdoe、DC=acme、DC=com に変換します。これは、ID が証明書サブジェクトから取得され、Active Directory が DN でユーザー検索するように設定されている場合に作成可能なルールの例です。このルールは、電子メール プレフィクスを削除し、DN を生成するよう Cisco ISE に指示します。

次に、ID 書き換えルールを記述する際によくある間違いを示します。

- ID が **[DOMAIN]\[IDENTITY]** と一致する場合、**[IDENTITY]@DOMAIN.com** に書き換えます。

  結果は jdoe@DOMAIN.com です。このルールは、ルールの書き換え側の角カッコ [ ] に [DOMAIN] がありません。

- ID が **DOMAIN\[IDENTITY]** と一致する場合、**[IDENTITY]@[DOMAIN].com** に書き換えます。

  この場合も、結果は jdoe@DOMAIN.com です。このルールは、ルールの評価側の角カッコ [ ] に [DOMAIN] がありません。

ID 書き換えルールは、常に、Active Directory 参加ポイントのコンテキスト内で適用されます。認証ポリシーの結果としてスコープが選択されている場合でも、書き換えルールは、各 Active Directory 参加ポイントに適用されます。EAP-TLS が使用されている場合、これらの書き換えルールは、証明書から取得される ID にも適用されます。

ID 書き換えの有効化

この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

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 [ID 書き換え（Identity Rewrite）] セクションで、ユーザー名を変更する書き換えルールを適用するかどうかを選択します。

ステップ 4 一致条件および書き換え結果を入力します。表示されるデフォルト ルールを削除し、要件に応じてルールを入力できます。Cisco ISE は順番にポリシーを処理し、要求ユーザー名に一致する最初の条件が適用されます。一致トークン（角カッコ内に含まれるテキスト）を使用して、元のユーザー名の要素を結果に転送できます。いずれのルールにも一致しない場合、識別名は変更されません。[テスト開始（Launch Test）] ボタンをクリックして、書き換え処理をプレビューできます。

ID 解決設定

一部のタイプの ID には、プレフィクスまたはサフィックスのようなドメイン マークアップが含まれます。たとえば、ACME\jdoe などの NetBIOS ID では、「ACME」がドメイン マークアップのプレフィクスで、同様に jdoe@acme.com などの UPN ID では、「acme.com」がドメイン マークアップのサフィックスです。ドメイン プレフィクスは、組織内の Active Directory ドメインの NetBIOS（NTLM）名に一致し、ドメイン サフィックスは、組織内の Active Directory ドメインの DNS 名または代替 UPN サフィックスに一致する必要があります。たとえば、gmail.com は Active Directory ドメインの DNS 名ではないため、jdoe@gmail.com はドメイン マークアップなしとして処理されます。

ID 解決設定では、Active Directory 展開に一致するように、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を指定できます。これらの設定を使用して、ドメイン マークアップのないユーザー名およびホスト名の認証を調整できます。Cisco ISE でユーザーのドメインを認識できない場合、すべての認証ドメインでユーザーを検索するように設定できます。ユーザーが 1 つのドメインで見つかった場合でも、Cisco ISE は ID のあいまいさがないことを確実にするために、すべての応答を待ちます。この処理は、ドメインの数、ネットワークの遅延、負荷などに応じて、時間がかかる場合があります。

ID 解決の問題の回避

認証時に、ユーザーおよびホストに完全修飾名（つまり、ドメイン マークアップが含まれている名前）を使用することを強く推奨します。たとえば、ユーザーの UPN と NetBIOS 名、およびホストの FQDN SPN です。これは、複数の Active Directory アカウントが受信ユーザー名と一致する（たとえば、jdoe が jdoe@emea.acme.com および jdoe@amer.acme.com と一致する）など、あいまいエラーが頻繁に生じる場合に特に重要です。場合によっては、完全修飾名を使用することが、問題を解決する唯一の方法になります。また、ユーザーに一意のパスワードが設定されていることを保証するだけで十分な場合もあります。したがって、一意の ID を最初から使用すると、効率が向上し、パスワード ロックアウトの問題が減少します。

ID 解決設定の構成

この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE ノードを参加させる必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

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 [ID解決（Identity Resolution）] セクションで、ユーザー名またはマシン名の ID 解決についての次の設定を定義します。この設定によって、ユーザーの検索と認証を詳細に制御できます。

最初に、マークアップなしの ID に対する設定を行います。このような場合、次のオプションのいずれかを選択できます。

- [要求を拒否する（Reject the request）]：このオプションを使用すると、SAM 名などのドメインマークアップがないユーザーの認証は失敗します。このことは、複数参加ドメインで、Cisco ISE がすべての参加グローバル カタログの ID を検索する必要があることによって、安全性が低下する可能性がある場合に役立ちます。このオプションによって、ドメイン マークアップを含むユーザー名を使用することがユーザーに対して強制されます。
- [結合されたフォレストの「認証ドメイン」のみで検索する（Only search in the “Authentication Domains” from the joined forest）]：このオプションを使用すると、認証ドメインのセクションで指定した、結合ポイントのフォレスト内のドメイン内のみで ID が検索されます。これはデフォルトオプションです。
- [すべての「認証ドメイン」セクションで検索する（Search in all the “Authentication Domains” sections）]：このオプションを使用すると、すべての信頼できるフォレストのすべての認証ドメイン内で ID が検索されます。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。

Cisco ISE で認証ドメインがどのように設定されているかに基づいて選択します。特定の認証ドメインのみを選択した場合は、それらのドメインのみが検索されます（「結合されたフォレスト」と「すべてのフォレスト」のいずれを選択した場合も）。

2 番目の設定は、Cisco ISE が [認証ドメイン（Authentication Domains）] セクションで指定された設定に準拠するために必要となるすべてのグローバルカタログ（GC）と通信できない場合に使用します。このような場合、次のオプションのいずれかを選択できます。

- [使用可能なドメインで続行する（Proceed with available domains）]：このオプションを使用すると、使用可能ないずれかのドメインで一致が見つかった場合に認証が続行されます。
- [要求をドロップする（Drop the request）]：このオプションを使用すると、ID 解決で到達不能または使用できないドメインが検出された場合に認証要求がドロップされます。

サンプルシナリオ

ここでは、Cisco ISE と Active Directory の設定フローに関するいくつかの基本的なシナリオについて説明します。

企業買収

シナリオ

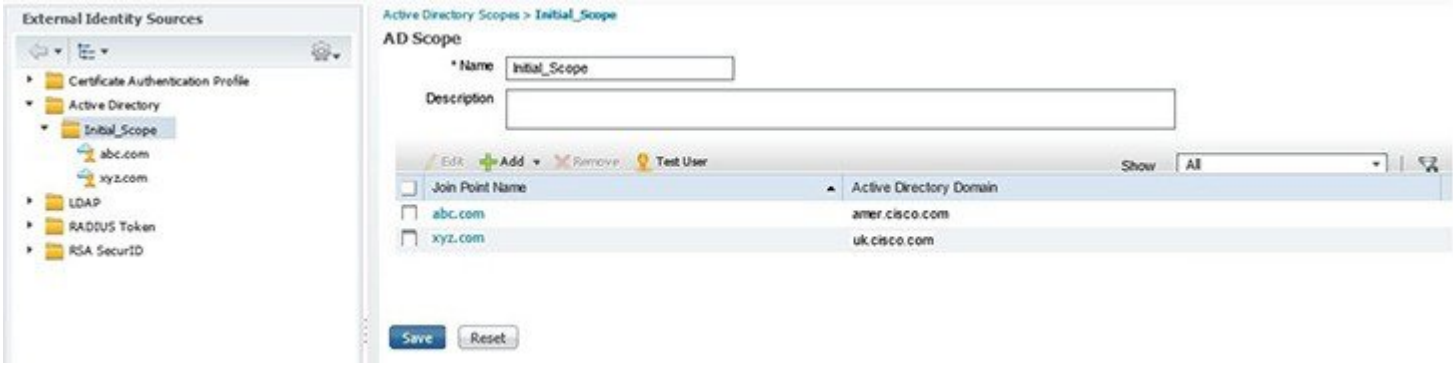
企業 abc.com が、企業 xyz.com を買収または合併しました。abc.com の管理者として、abc.com および xyz.com の両方のユーザーが同じ物理ネットワークにアクセスできる統合されたネットワーク認証インフラストラクチャを実現しようと考えています。

必要な設定

abc.com の単一の Active Directory 参加ポイントがすでに設定されています。信頼できない Active Directory インフラストラクチャを追加するには、次の操作を実行します。

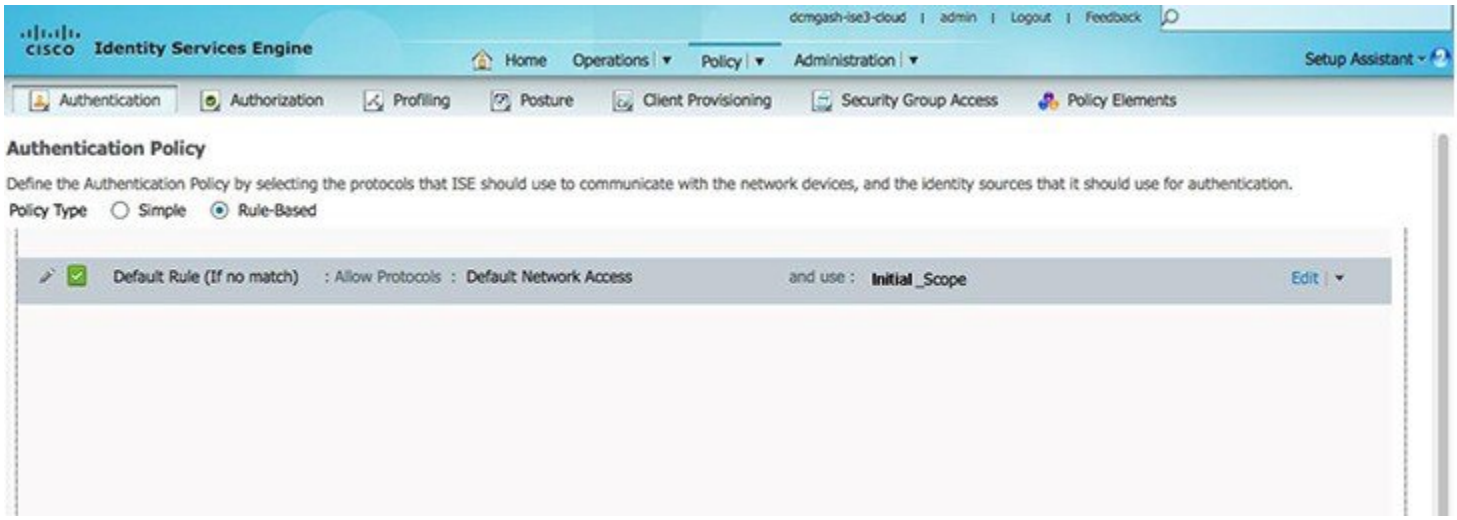
1. スコープ モードにして Initial_Scope を追加します。
2. xyz.com の新しい参加ポイントを追加します。

   図 *1 : Initial_Scope* 内に作成された参加ポイント



3. 認証ポリシーを設定し、すべての認証の結果として Initial_Scope を選択します。

図 *2 :* 認証ポリシーの結果として選択された ***Initial_Scope***



上記の設定を実行することによって、いずれかの会社の Active Directory のユーザーを検索するように Cisco ISE を設定するためのスコープを作成しました。スコープを使用することで、ネットワークで、複数の Active Directory インフラストラクチャに対して、それらが完全に切断されている場合や相互に信頼していない場合にも、認証を実行できます。

マルチテナント

シナリオ

マルチテナントのシナリオでは、複数の顧客（CompanyA、CompanyB、およびCompanyC）の設定を定義する必要があります。各お客様に対して、次のことを行う必要があります。

- 独立したネットワーク デバイス グループを定義します。
- ID トラフィックが効率的にスキャンできるスコープを定義します。
- 独立した Active Directory の参加ポイントを設定し、参加します。
- Active Directory の ID トラフィックがこれらのデバイス グループからこれらの Active Directory の参加ポイントに送られるような認証および認可ポリシーを定義します。

必要な設定

必要なすべての機能を提供するには、次の操作を実行します。

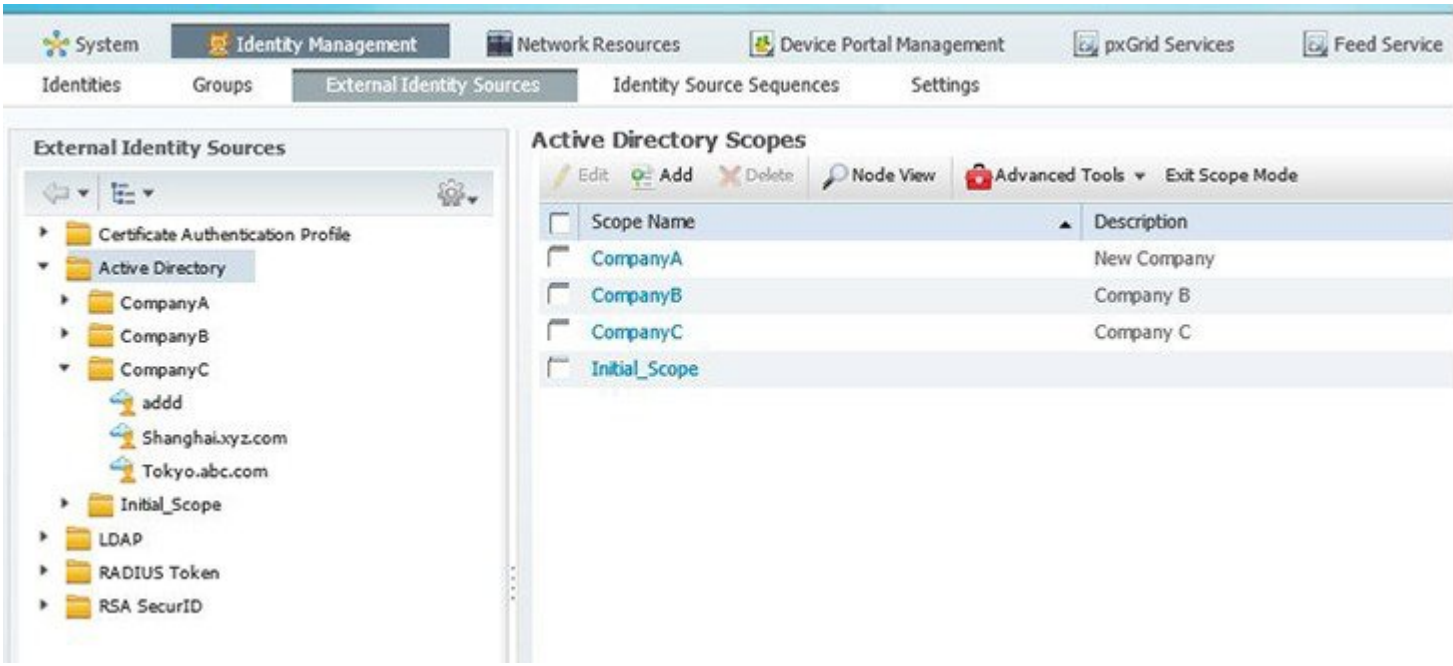
1. CompanyA、CompanyB、CompanyC のようなネットワーク デバイス グループ（NDG）タイプを定義し、各社のネットワーク デバイスを追加します。

図 *3*：各会社のネットワーク デバイス グループの定義

2. 各会社のスコープを定義します。各会社のスコープ内に複数の Active Directory の参加ポイントを定義します。

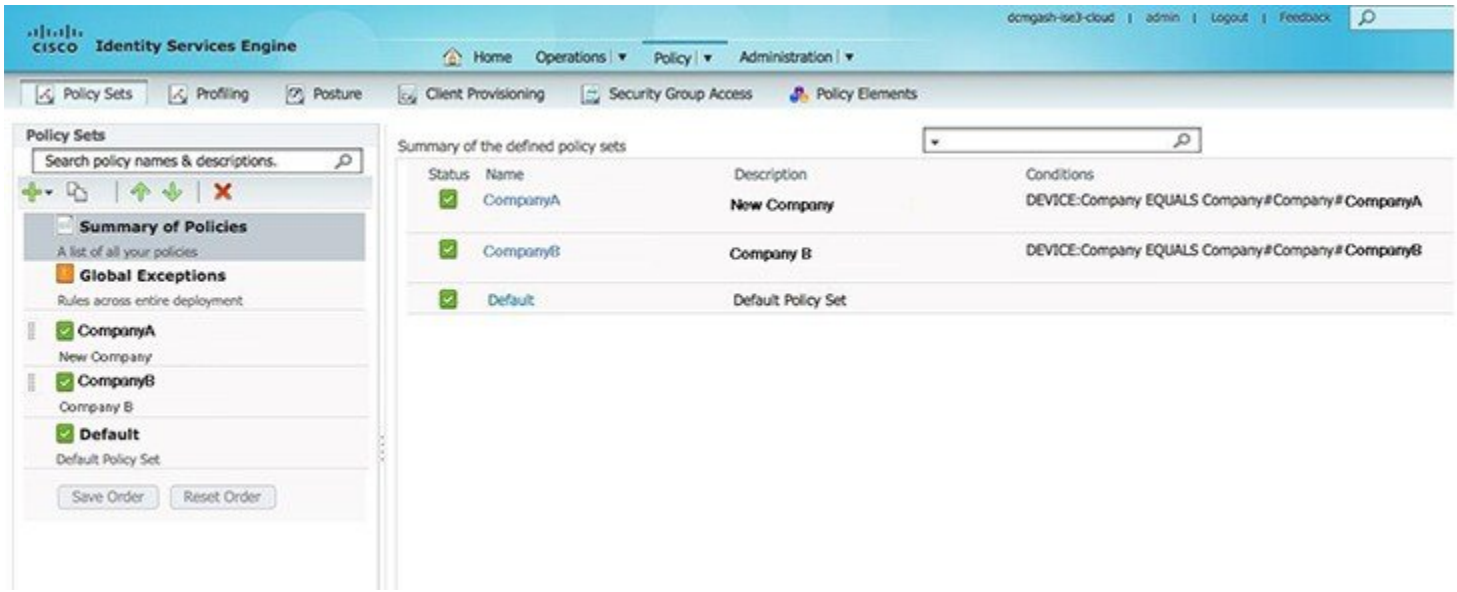
   すべての会社のドメインが信頼できる場合、必要な参加ポイントは1つのみです。ただし、この例では、信頼できないドメインが多数あるため、複数の参加ポイントが必要になります。

図 *4*：各会社の範囲と参加ポイントの定義



3. ポリシーセットを設定し、会社の認証のために、会社の NDG を Active Directory のスコープに結び付けます。各会社では独自のポリシーも必要となるため、会社独自のポリシー グループで認可ポリシーを定義できます。

図 *5:* ポリシーセットの設定



373708

トラブルシューティング ツール

Cisco ISE には、Active Directory のエラーを診断およびトラブルシューティングするツールが複数備えられています。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE によって Active Directory が使用される場合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。

Cisco ISE が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE 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ことを確認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、ユーザー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したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE ノードを選択します。

Cisco ISE ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory のアラームとレポート

Cisco ISE は、Active Directory に関連するアクティビティをモニターリングし、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を提供します。

アラーム

Active Directory のエラーと問題に対して、次のアラームがトリガーされます。

- 構成済みネーム サーバーが使用不可（Configured nameserver not available）
- 参加しているドメインが使用不可（Joined domain is unavailable）
- 認証ドメインが使用不可（Authentication domain is unavailable）
- Active Directory フォレストが使用不可（Active Directory forest is unavailable）
- AD コネクタを再起動する必要があります（AD Connector had to be restarted）
- AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）
- AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）

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監視できます。

- RADIUS 認証レポート：このレポートには、Active Directory の認証と許可の詳細な手順が表示されます。このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[エンドポイントとユーザー（Endpoints and Users）]** > **[RADIUS 認証（RADIUS Authentications）]** にあります。

- AD コネクタ操作レポート：AD コネクタ操作レポートには、AD コネクタが実行するバックグラウンド操作（Cisco ISE サーバーパスワードの更新、ケルベロスチケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など）のログが表示されます。Active Directory の障害が発生した場合は、考えられる原因を特定するために、このレポートで詳細を確認できます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [AD コネクタ操作（AD Connector Operations）]** にあります。

あいまいな ID エラーの検索

1 つのフォレスト内に同じ名前の ID が複数出現することがあります。Multi-Join シナリオ、特に、Active Directory ドメインに複数の無関係の会社があり、ユーザー名を相互に制御していない場合に、このことがよく発生します。SAM 名を使用すると、名前が競合する可能性も高まります。NetBIOS プレフィクスでさえ、フォレストごとに一意ではありません。UPN が適切に機能していても代替 UPN は競合する可能性があります。このようなすべてのシナリオで、あいまいな ID エラーが発生します。

[オペレーション（Operations）] タブの下の [認証（Authentications）] ページを使用して、次の属性を検索できます。次の属性は、あいまい ID エラーが発生した場合に、実際に使用されている ID を理解し、制御するために役立ちます。

- AD-Candidate-Identities：あいまいな ID が最初に検出されると、この属性が検出された ID を示します。ID があいまいである理由の特定に役立ちます。
- AD-Resolved-Identities：ID が検出されて、認証、get-groups、get-attributes などの操作で使用された後、この属性は検出された ID で更新されます。ID のクラッシュ時にはこれが複数になる場合があります。
- AD-Resolved-Providers：この属性は、ID が検出された Active Directory の参加ポイントを示します。

ノードの Active Directory 参加の表示

特定の Cisco ISE ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** の順に移動します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

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。展開でポリシー サービス ペルソナを担当する Cisco ISE ノードでこのオプションを有効にする必要があります。Active Directory のデバッグ ログを有効にすると、ISE のパフォーマンスに影響する場合があります。

手順

ステップ 1 Cisco ISE GUI で、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）]** の順に移動します。

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] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 [保存（Save）] をクリックします。

Active Directory ログファイルの入手

可能性がある問題をトラブルシューティングするには、Active Directory のデバッグ ログをダウンロードし、表示します。

始める前に

Active Directory のデバッグ ロギングを有効にする必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [ログのダウンロード（Download Logs）]** の順に移動します。

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。

Active Directory の高度な調整

高度な調整機能により、シスコのサポート担当者の管理下で、サポート操作に使用されるノード固有の設定が可能となり、システムのさらに深いレベルでパラメータを調整できるようになります。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。ガイダンスに従って使用する必要があります。

AD コネクタの内部操作

ドメイン検出アルゴリズム

Cisco ISE は、次の 3 つのフェーズでドメイン検出を実行します。

1. 参加しているドメインのクエリー：フォレストのドメイン、および参加しているドメインに対して外部的に信頼できるドメインを検出します。
2. フォレスト内のルート ドメインのクエリー：フォレストで信頼を確立します。
3. 信頼できるフォレスト内のルート ドメインのクエリー：信頼できるフォレストからドメインを検出します。

さらに、Cisco ISE は DNS ドメイン名（UPN サフィックス）、代替の UPN サフィックスおよび NTLM ドメイン名を検出します。

デフォルト ドメインの検出頻度は、2 時間ごとです。[高度な調整（Advanced Tuning）] ページからこの値を変更できますが、シスコのサポート担当者に相談してください。

ドメインコントローラ検出

AD コネクタは、次のように特定ドメインのドメインコントローラ（DC）を選択します。

1. DNS SRV クエリー（サイトにスコープされていない）を実行し、ドメインで完全なドメイン コントローラ リストを取得します。
2. IP アドレスのない DNS SRV の DNS 解決を実行します。
3. SRV レコードの優先順位に従って CLDAP ping 要求をドメイン コントローラに送信し、応答がある場合は最初の応答のみを処理します。CLDAP 応答には、DC サイトとクライアント サイト（Cisco ISE マシンが割り当てられたサイトなど）が含まれます。
4. DC サイトとクライアント サイトが同じ場合、応答の送信元（DC）が選択されます。
5. DC サイトとクライアント サイトが同じでない場合、AD コネクタは、検出されたクライアント サイトにスコープされた DNS SRV クエリーを実行し、クライアント サイトを使用するドメイン コントローラのリストを取得し、これらのドメイン コントローラに CLDAP ping 要求を送信し、応答がある場合は最初の応答のみを処理します。応答の送信元（DC）が選択されます。サイトを使用するクライアント サイトに DC がない場合や、現在使用できる DC がサイトにない場合は、手順 2 で検出された DC が選択されます。

Active Directory サイトを作成および使用することで、Cisco ISE が使用するドメイン コントローラに影響を与える場合があります。サイトの作成および使用方法については、Microsoft Active Directory のマニュアルを参照してください。

Cisco ISE は、ドメインごとに優先 DC のリストも定義できます。DC のリストは、DNS SRV クエリーの前に選択の優先順位が付けられます。ただし、この優先 DC のリストは除外リストではありません。優先 DC が使用できない場合は、その他の DC が選択されます。優先 DC のリストは、次の場合に作成できます。

- SRV レコードが不良か、存在しないか、設定されていない場合。
- サイト関連が間違っているか、存在しないか、サイトを使用できない場合。
- DNS 設定が間違っているか、編集できない場合。

ドメインコントローラのフェールオーバー

ドメインコントローラ（DC）のフェールオーバーは、次の条件によってトリガーされます。

- AD コネクタは、現在選択している DC が LDAP、RPC、または Kerberos の通信試行時に使用できなくなった場合に検出します。DC はダウンしているかネットワーク接続されていないために使用できない可能性があります。このような場合、AD コネクタは DC の選択を開始し、新しく選択した DC にフェールオーバーします。
- DC が起動していて CLDAP ping に応答しますが、AD コネクタはいくつかの理由で DC と通信できません。たとえば、RPC ポートがブロックされている場合、DC は破損複製状態になっているか、適切に使用停止されていません。このような場合、AD コネクタは、ブラックリストを使用する DC の選択（「不良」DC はブラック リストに置かれます）を開始して、選択した DC との通信を試します。ブラックリストを使用して選択した DC とブラックリストのどちらもキャッシュされません。

DNS フェールオーバー

最大 3 つの DNS サーバーと 1 つのドメイン サフィックスを設定できます。Cisco ISE で Active Directory の ID ストア順序を使用している場合、すべての DNS サーバーが、使用するすべての Active Directory DNS ドメインの正引きおよび逆引き DNS クエリーに応答できるようにする必要があります。DNS のフェールオーバーは、最初の DNS がダウンしているときにのみ発生します。フェールオーバー DNS には最初の DNS と同じレコーダが必要です。DNS サーバーがクエリーの解決に失敗する場合、DNS クライアントは別の DNS サーバーを試行しません。デフォルトでは、DNS サーバーはクエリーを 2 回再試行し、3 秒でクエリーをタイムアウトします。

ID アルゴリズムの解決

ID に関しては、パスワードが入力されているかどうか、任意のドメイン マークアップが ID に存在するかどうかに関係なく、ID のタイプに基づいて、さまざまなアルゴリズムがユーザーまたはマシン オブジェクトの検索に使用されます。

次に、Cisco ISE がさまざまな ID タイプの解決に使用するさまざまなアルゴリズムを示します。

（注） ID が設定済みの ID リライト ルールに従って書き換えられている場合、ID 解決は書き換えられた ID に適用されます。

SAM 名の解決

- ID が SAM 名（ドメイン マークアップのないユーザー名またはマシン名）の場合、Cisco ISE は各参加ポイントのフォレストを（1 回）検索して ID を探します。一意に一致した場合、Cisco ISE はドメインまたは一意の名前を特定し、AAA フローに進みます。
- SAM 名が一意ではなく、Cisco ISE が EAP-TLS などのパスワードのないプロトコルを使用するように設定されている場合、適切なユーザーを検索する他の基準がないため、Cisco ISE は「あいまいな ID」エラーで認証に失敗します。ただし、ユーザー証明書が Active Directory に存在する場合、Cisco ISE はバイナリ比較を使用して ID を解決します。
- PAP などのパスワードベースのプロトコル、または MSCHAP を使用するように Cisco ISE が設定されている場合、Cisco ISE は引き続きパスワードを確認します。一意に一致した場合、Cisco ISE は AAA フローに進みます。ただし、パスワードが同じアカウントが複数ある場合、Cisco ISE は「あいまいな ID」エラーで認証に失敗します。

ユーザー名の競合を回避する必要があります。これにより、効率およびセキュリティが向上するだけでなく、アカウントがロックされることも防止されます。たとえば、パスワードが異なる 2 つの「Chris」が存在し、Cisco ISE は SAM 名の「Chris」のみを受信するとします。このシナリオでは、Cisco ISE は正しいアカウントを特定する前に、SAM 名が「Chris」である両方のアカウントを試行し続けます。このような場合、Active Directory は間違ったパスワードの試行によっていずれかのアカウントをロックする可能性があります。このため、一意のユーザー名またはドメイン マークアップ付きのユーザー名を使用するようにしてください。また、各 Active Directory ドメインに特定のネットワーク デバイスを使用する場合、ID 書き換えを使用して SAM 名を認定できます。

UPN の解決

- ID が UPN 場合、Cisco ISE は各フォレストのグローバル カタログを検索して、その UPN ID との一致を確認します。一意に一致した場合、Cisco ISE は AAA フローに進みます。同じ UPN の参加ポイントが複数あり、パスワードが入力されていないか、適切なアカウントの特定に役立たない場合、Cisco ISE は「あいまいな ID」エラーで認証に失敗します。
- また、Cisco ISE は、UPN である ID にユーザーのメール属性の照合も許可します。つまり、「identity=matching UPN or email」を検索します。一部のユーザーは、実際の基盤となる UPN ではなく、電子メール名を使用して（多くの場合、証明書経由で）ログインします。このことは、ID が電子メール アドレスと同じ形式の場合に、暗黙的に行われます。

マシン ID の解決

- マシン認証の場合、Cisco ISE は、ホスト/プレフィクスを持つ ID を使用して、一致する servicePrincipalName 属性がないかフォレストを検索します。完全修飾ドメイン サフィックス（host/machine.domain.com など）が ID で指定されている場合、Cisco ISE はそのドメインが存在するフォレストを検索します。ID がホスト/マシン形式の場合、Cisco ISE はサービス プリンシパル名がないかすべてのフォレストを検索します。一致が複数ある場合、Cisco ISE は「あいまいな ID」エラーで認証に失敗します。
- マシンが別の ID 形式（machine@domain.com、ACME\laptop$、または laptop$ など）の場合、Cisco ISE は通常の UPN、NetBIOS、または SAM の解決アルゴリズムを使用します。

NetBIOS ID の解決

ID に NetBIOS ドメイン プレフィクス（ACME\jdoe など）がある場合、Cisco ISE は NetBIOS ドメインがないかフォレストを検索します。検出されたら、検出されたドメインで指定の SAM 名（この例では「jdoe」）を検索します。NetBIOS ドメインは、1 つのフォレストにおいても必ずしも一意ではないため、検索によって同じ名前の NetBIOS ドメインが複数検出される場合があります。このような場合にパスワードが入力されていると、適切な ID を検索するために、そのパスワードが使用されます。それでもあいまいな場合やパスワードが入力されていない場合、Cisco ISE は「あいまいな ID」エラーで認証に失敗します。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。