Cisco VCS 認証デバイス

導入ガイド

初版：2011 年 5 月

最終更新：2015 年 11 月

Cisco VCS X8.7

デバイス認証について

デバイス認証では、デバイスまたは外部システムから VCS に届く着信要求のクレデンシャルを検証します。既知のユーザまたは信頼できるユーザに対して特定の機能を確保するために使用されます（たとえば、プレゼンス ステータスのパブリッシュ、プロビジョニング データの収集、ISDN ゲートウェイ コールのような有料リソースを使用する能力など）。

VCS 上でデバイス認証が有効になっている場合、その VCS との通信を試みるデバイスはすべて、クレデンシャル（通常はユーザ名とパスワードに基づく）の提示を要求されます。VCS は認証方式に従って、それらのクレデンシャルを検証するか、または他のサービスに検証させて、その結果に従ってメッセージを受け入れるか、または拒否します。

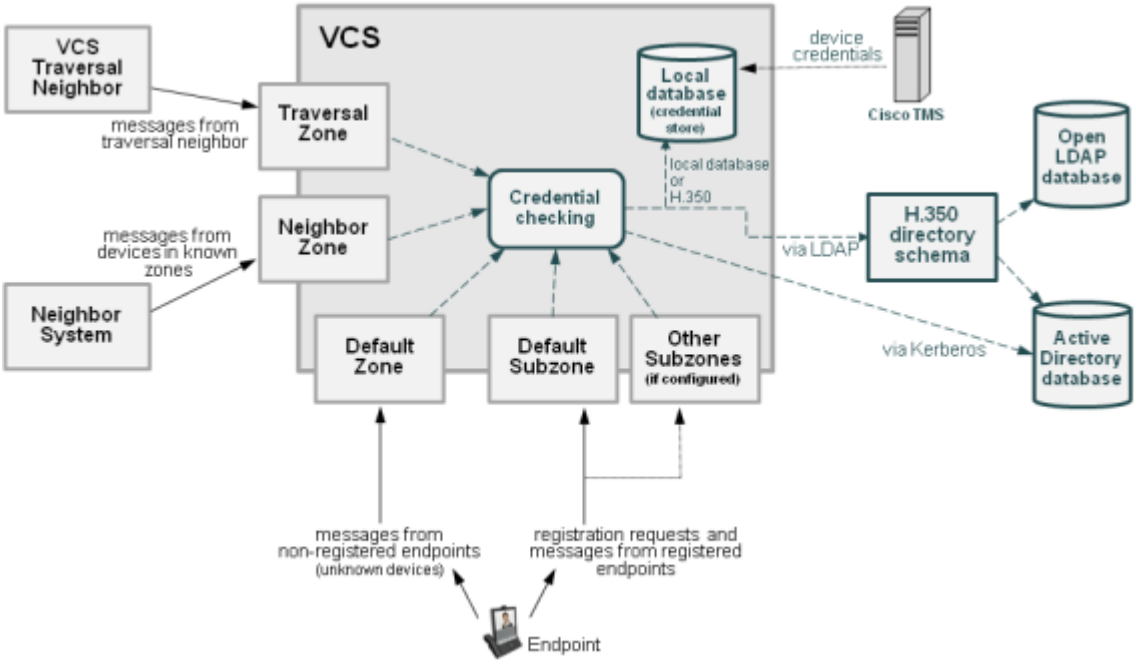
VCS 認証ポリシーは、ゾーンやサブゾーンにそれぞれ独立して設定できます。つまり、認証済みと未認証の両方のデバイスに対して同じ VCS への登録（および通信）を必要に応じて許可することが可能です。後続のコール ルーティングの決定には、デバイスが認証されているかどうかに基づいたさまざまなルールを設定できます。

VCS は、提示されたクレデンシャルを検証するために、最初にユーザ名とパスワードが格納されているオンボックスのローカル データベースと照合します。システムがデバイス プロビジョニングを使用している場合、このローカル データベースには、Cisco TMS から提供されるクレデンシャルとの照合も含まれます。ユーザ名がローカル データベース内で見つからない場合、VCS は、外部の H.350 ディレクトリ サービスにリアルタイムで LDAP 接続して、クレデンシャルの検証を試みることもできます。このディレクトリ サービスが設定されている場合は、Microsoft Active Directory LDAP サーバ用または OpenLDAP サーバ用の H.350 ディレクトリ スキーマが存在する必要があります。

VCS-E は、SIP メッセージのクレデンシャル チェックをトラバーサル ゾーンを介して別の VCS に委任できるように設定することもできます。

デバイスが NTLM チャレンジをサポートしている場合、前述のいずれかの方法とともに、VCS は Kerberos 接続で Active Directory サーバに直接アクセスしてクレデンシャルを検証することもできます。

VCS の各種認証エントリ ポイントおよびクレデンシャルのチェック方法を以下に示します。



ユニファイド コミュニケーションのモバイル デバイスおよびリモート アクセス デバイス

VCS を介して Unified CM に登録するデバイスの認証について、VCS 上で明示的に設定する必要はありません。VCS はホーム Unified CM クラスタに対するそれらのデバイスの認証を自動的に処理します。

認証ポリシー（Authentication policy）

VCS 認証ポリシーの設定

認証ポリシーは、VCS によってゾーン レベルおよびサブゾーン レベルで適用されます。認証ポリシーは、該当ゾーンまたはサブゾーンからの（プロビジョニング、登録、プレゼンス、電話帳、およびコールのための）着信メッセージに対する VCS のチャレンジ方法、つまり、それらのメッセージを拒否するか、認証済みとして扱うか、または VCS 内では未認証として扱うかを制御します。

各ゾーンおよびサブゾーンでは、それぞれの [認証ポリシー（Authentication policy）] を [クレデンシャルを確認する（Check credentials）]、[クレデンシャルを確認しない（Do not check credentials）]、または [認証済みとして扱う（Treat as authenticated）] に設定できます。

- 登録の認証は、デフォルト サブゾーン（または関連する代替サブゾーン）設定で制御されます。
- 最初のプロビジョニング登録要求の認証は、デフォルト ゾーン設定で制御されます。
- コール、プレゼンス、および電話帳要求の認証は、エンドポイントが登録されている場合はデフォルト サブゾーン（または関連する代替サブゾーン）で、エンドポイントが登録されていない場合はデフォルト ゾーンで制御されます。

厳密な認証ポリシーの動作は、メッセージが H.323 メッセージ、ローカル ドメインから受信した SIP メッセージ、非ローカル ドメインから受信した SIP メッセージのいずれであるかによって異なることに注意してください。さまざまな認証ポリシーの動作の詳細な説明については、6 ページの「認証ポリシーの設定オプション」を参照してください。

ゾーンレベルの認証ポリシー

認証ポリシーは、メッセージを受信しているかどうかに基づき、ゾーン タイプごとに選択して設定できます。

- デフォルト ゾーン、ネイバー ゾーン、トラバーサル クライアント ゾーン、トラバーサル サーバ ゾーン、およびユニファイド コミュニケーション トラバーサル ゾーンはすべて、認証ポリシーを設定できます。
- DNS ゾーンと ENUM ゾーンはメッセージを受信しないため、認証ポリシーの設定はありません。

ゾーンの [認証ポリシー（Authentication policy）] を編集するには、[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動し、ゾーンの名前をクリックします。新しいゾーンを作成すると、ポリシーはデフォルトで [クレデンシャルを確認しない（Do not check credentials）] に設定されます。

サブゾーンレベルの認証ポリシー

認証ポリシーは、デフォルト サブゾーンおよびその他の任意の設定済みサブゾーンに対して設定できます。

サブゾーンの [認証ポリシー（Authentication policy）] を設定するには、[設定（Configuration）] > [ローカル ゾーン（Local Zone）] > [サブゾーン（Subzones）] に移動し、[表示/編集（View/Edit）] またはサブゾーンの名前をクリックします。新しいサブゾーンを作成すると、ポリシーはデフォルトで [クレデンシャルを確認しない（Do not check credentials）] に設定されます。

プロビジョニングとデバイスの認証

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、VCS へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

詳細については、13 ページの「デバイス プロビジョニングと認証ポリシー」を参照してください。

プレゼンスとデバイスの認証

プレゼンス サーバは、すでに認証されているプレゼンス PUBLISH メッセージのみ受け入れます。

- VCS によるプレゼンス メッセージの認証は、エンドポイントが登録されている場合にはデフォルト サブゾーン（または関連する代替サブゾーン）上の認証ポリシー設定によって制御され（通常のケース）、エンドポイントが登録されていない場合はデフォルト ゾーン上の認証ポリシー設定によって制御されます。
- 関連する [認証ポリシー（Authentication policy）] は、[クレデンシャルを確認する（Check credentials）] または [認証済みとして扱う（Treat as authenticated）] のいずれかに設定されている必要があります。そうでなければ、PUBLISH メッセージは失敗し、エンドポイントはそれぞれのプレゼンス ステータスをパブリッシュできなくなります。

詳細については、14 ページの「プレゼンスと認証ポリシー」を参照してください。

認証済みデバイスおよび未認証デバイスに対するシステム動作の制御

認証済みデバイスおよび未認証デバイスからのコールおよびその他のメッセージの処理方法は、検索ルール、外部ポリシー サービス、および CPL の設定内容によって異なります。

検索ルール

検索ルールを設定する場合は、[Request must be authenticated（要求は認証が必要）] 属性を使用して、検索ルールが認証済みの検索要求にのみ適用されるのか、またはすべての要求に適用されるのかを指定します。

外部ポリシー サービス

外部ポリシー サービスは、通常、VCS 自体にポリシー ルールを設定するのではなく、外部の集中型サービスによってポリシー決定が管理される導入で使用されます。次の領域でポリシー サービスを使用するように、VCS を設定できます。

- 登録ポリシー
- 検索ルール（ダイヤル プラン）
- コール ポリシー
- ユーザ ポリシー（FindMe）

VCS は、ポリシー サービスを使用するときに、コールまたは登録要求に関する情報を、名前と値のペアで構成される一連のパラメータを使用して POST メッセージでそのサービスに送信します。それらのパラメータには、要求の送信元が認証済みソースかどうかの情報が含まれています。

ポリシー サービスの詳細（CPL の例を含む）については、『*External Policy on VCS Deployment Guide*』を参照してください。

CPL

VCS 上でコール ポリシー ルール ジェネレータを使用している場合、ソースの照合は、認証済みソースに対して実行されます。未認証のソースに対する照合を指定するには、空白フィールドを使用します。（ソースが認証されていない場合、そのソースの値は信頼できません）。

手作業で作成し、アップロードしたローカル CPL を使用してコール ポリシーを管理する場合は、認証済みと未認証のいずれの発信元を調べるかについて CPL を明確にすることを推奨します。

- CPL で未認証の発信元を調べる必要がある場合（たとえば、非認証の発信者をチェックする場合）は、「`unauthenticated-origin`」を使用する必要があります （ただし、未認証のユーザは、自らを好きなように呼ぶことができるため、このフィールドでは、発信者は確認されません）。
- 認証済みの発信元（認証済みデバイスまたは [認証済みとして扱う（Treat as authenticated）] デバイスでのみ可能）をチェックするには、CPL で「`authenticated-origin`」を使用する必要があります。

CPL スクリプトの記述は複雑なため、外部ポリシー サービスを代わりに使用することを推奨します。

認証ポリシーの設定オプション

認証ポリシーの動作は、H.323 メッセージ、ローカル ドメインから受信した SIP メッセージ、および非ローカル ドメインから受信した SIP メッセージであるかによって異なります。

プライマリ認証ポリシーの設定オプションおよびそれぞれに関連付けられている動作は以下のとおりです。

- [クレデンシャルを確認する（Check credentials）]：関連の認証方式を使用してクレデンシャルを確認します。一部のシナリオでは、メッセージはチャレンジされません。以下を参照してください。
- [クレデンシャルを確認しない（Do not check credentials）]：クレデンシャルを確認せずに、メッセージを処理します。
- [認証済みとして扱う（Treat as authenticated）]：クレデンシャルを確認せず、認証済みであるかのようにメッセージを処理します。このオプションは、それぞれの登録メカニズム内で認証をサポートしていないサードパーティ サプライヤからのエンドポイントに対応するために使用できます。一部のシナリオでは、メッセージは許可されても、未認証であるかのように扱われることがあります。以下を参照してください。

以下の表に、ゾーン レベルおよびサブゾーン レベルで適用されている場合のポリシーの動作、およびメッセージ プロトコルによる違いの要約を示します。

ゾーンレベルの認証ポリシー

認証ポリシーは、メッセージを受信しているかどうかに基づき、ゾーン タイプごとに選択して設定できます。

- デフォルト ゾーン、ネイバー ゾーン、トラバーサル クライアント ゾーン、トラバーサル サーバ ゾーン、およびユニファイド コミュニケーション トラバーサル ゾーンはすべて、認証ポリシーを設定できます。
- DNS ゾーンと ENUM ゾーンはメッセージを受信しないため、認証ポリシーの設定はありません。

ゾーンの [認証ポリシー（Authentication policy）] を編集するには、[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動し、ゾーンの名前をクリックします。新しいゾーンを作成すると、ポリシーはデフォルトで [クレデンシャルを確認しない（Do not check credentials）] に設定されます。

以下の表に示されているように、H.323 メッセージと SIP メッセージの動作は異なります。

H.323

ポリシー	動作
クレデンシャルを確認する	メッセージは、メッセージ内のいずれかのクレデンシャルを認証データベースで確認できるかどうかによって、認証済みまたは未認証として分類されます。 クレデンシャルが提供されていない場合、メッセージは常に未認証として分類されます。
クレデンシャルを確認しない	メッセージのクレデンシャルはチェックされず、すべてのメッセージが未認証として分類されます。
認証済みとして扱う	メッセージのクレデンシャルはチェックされず、すべてのメッセージが認証済みとして分類されます。

SIP

ゾーン レベルでの SIP メッセージの動作は、[**SIP 認証信頼モード（SIP authentication trust mode）**] の設定によって異なります。つまり、VCS が受信メッセージに含まれている P-Asserted-Identity ヘッダーと呼ばれる既存の認証済みインジケータを信頼するかどうか、およびメッセージをローカル ドメイン（VCS が信頼するドメイン）から受信したか、非ローカル ドメインから受信したかによって異なります。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
クレデンシャルを確認する	オフ	メッセージは認証をチャレンジされます。 認証に失敗したメッセージは拒否されます。 認証に合格したメッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。
	オン	既存の P-Asserted-Identity ヘッダーがあるメッセージは、追加のチャレンジなしに認証済みとして分類されます。P-Asserted-Identity ヘッダーは変更されずに渡されます（発信者の Asserted ID を保持）。 既存の P-Asserted-Identity ヘッダーがないメッセージはチャレンジされます。認証に合格すると、メッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。認証に失敗すると、メッセージは拒否されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。
クレデンシャルを確認しない	オフ	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。
	オン	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
認証済みとして扱う	オフ	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーは削除され、VCS の発信者 ID を含む新しいヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。
	オン	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーがあるメッセージは変更されずに渡されます。既存の P-Asserted-Identity ヘッダーがないメッセージにはヘッダーが挿入されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。

サブゾーンレベルの認証ポリシー

認証ポリシーは、デフォルト サブゾーンおよびその他の任意の設定済みサブゾーンに対して設定できます。

サブゾーンの [認証ポリシー（Authentication policy）] を設定するには、[設定（Configuration）] > [ローカル ゾーン（Local Zone）] > [サブゾーン（Subzones）] に移動し、[表示/編集（View/Edit）] またはサブゾーンの名前をクリックします。新しいサブゾーンを作成すると、ポリシーはデフォルトで [クレデンシャルを確認しない（Do not check credentials）] に設定されます。

以下の表に示されているように、H.323 メッセージと SIP メッセージの動作は異なります。

H.323

ポリシー	動作
クレデンシャルを確認する	メッセージは、メッセージ内のいずれかのクレデンシャルを認証データベースで確認できるかどうかによって、認証済みまたは未認証として分類されます。認証に合格したメッセージは認証済みとして分類されます。 クレデンシャルが提供されていない場合、メッセージは常に未認証として分類されます。 未認証の登録要求は拒否されます。
クレデンシャルを確認しない	メッセージのクレデンシャルはチェックされず、すべてのメッセージが未認証として分類されます。
認証済みとして扱う	メッセージのクレデンシャルはチェックされず、すべてのメッセージが認証済みとして分類されます。

SIP

SIP メッセージの動作は、メッセージをローカル ドメイン（VCS が信頼するドメイン）から受信したか、非ローカル ドメインから受信したかによって異なります。

ポリシー	ローカル ドメイン内	ローカル ドメインの外
クレデンシャルを確認する	メッセージは認証をチャレンジされ、合格したメッセージは認証済みとして分類されます。 認証に失敗したメッセージ（登録要求を含む）は拒否されます。	非ローカル ドメインから受信した SIP メッセージはすべて、サブゾーンの [認証ポリシー（Authentication policy）] の設定に関係なく、同じ方法で処理されます。 メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。
クレデンシャルを確認しない	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。	
認証済みとして扱う	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。	

SIP 認証信頼

デバイス認証を使用するように設定されている VCS では、着信の SIP 登録要求および INVITE 要求が認証されます。その後、VCS からネイバー ゾーン（別の VCS など）に要求が転送されると、受信システムでもその要求が認証されます。このシナリオでは、すべてのホップでメッセージを認証する必要があります。

デバイスのクレデンシャルが（最初のホップで）一度だけ認証され、ネットワーク内の SIP メッセージの数が減るように簡素化する場合は、[認証信頼モード（Authentication trust mode）] の設定を使用するようにネイバー ゾーンを設定できます。

この設定は、ゾーンの認証ポリシーと組み合わせて使用されて、該当ゾーンから受信した事前認証済みの SIP メッセージが信頼されているかどうか、その後、VCS 内で認証済みまたは未認証として扱われるかを制御します。事前認証済みの SIP 要求は、*RFC 3325*.で定義されている SIP メッセージ ヘッダー内の P-Asserted-Identity フィールドの存在によって識別されます。

[認証信頼モード（Authentication trust mode）] の設定は次のとおりです。

- [オン（On）]：事前認証済みメッセージは追加のチャレンジなしに信頼され、その後、VCS 内では認証済みとして扱われます。未認証メッセージは、[認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] に設定されている場合はチャレンジされます。

- [オフ（Off）]：既存の認証済みインジケータ（P-Asserted-Identity ヘッダー）はすべてメッセージから削除されます。ローカル ドメインからのメッセージは、[認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] に設定されている場合はチャレンジされます。

（注）

- 認証信頼は、ネイバー ゾーンが信頼できる SIP サーバのネットワークの一部である場合のみ有効にすることを推奨します。
- 認証信頼は、トラバーサル サーバ ゾーンとトラバーサル クライアント ゾーンの間では自動的に暗示されます。

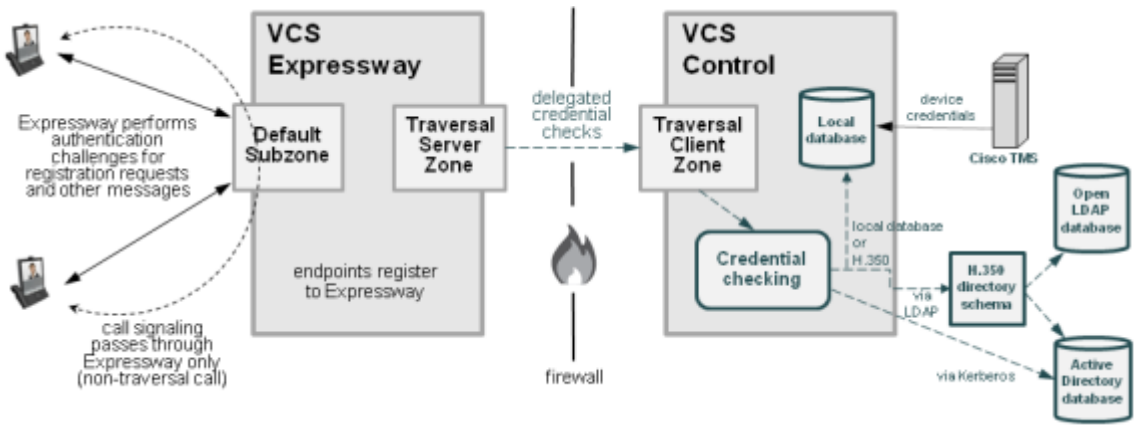
委任クレデンシャル チェックの設定（SIP のみ）

デフォルトでは、VCS は、認証チャレンジを実行している同一 VCS 上で、関連のクレデンシャル チェック メカニズム（ローカル データベース、Active Directory サービス、または LDAP 経由の H.350 ディレクトリ）を使用します。

また、SIP メッセージのクレデンシャル チェックをトラバーサル ゾーンから別の VCS（通常は VCS-C）に委任するために、認証チャレンジを実行する VCS を設定することもできます。委任クレデンシャル チェックは、デバイスを VCS Expressway に登録できるようにする（その結果、たとえば、トラバーサル ライセンスがなくてもコールが可能になる）が、セキュリティ上の理由で、認証システム（Active Directory サーバなど）との通信はすべて、企業の内部で実行したい導入で役立ちます。

- SIP Digest メッセージと NTLM メッセージの両方のクレデンシャル チェックを委任できます。
- メッセージはすべて、ローカルで定義された SIP ドメイン向けである必要があります。必要に応じて、ドメインごとに異なるトラバーサル クライアントにクレデンシャル チェックを委任できます。

次の図は、着信 SIP メッセージ（コール、登録など）が VCS Expressway でどのようにチャレンジされるか、それらのチャレンジに応じて提示されるクレデンシャルのチェックが VCS Control にどのように委任されるかを示しています。



委任クレデンシャル チェック用のビデオ通信ネットワークの設定

VCS Expressway と VCS Control の両方で複数の構成手順が関係している場合、委任クレデンシャル チェック用のビデオ ネットワークをセットアップします。

一連のローカル SIP ドメインなど、この構成の大部分はすでに終了している可能性がありますが、以下のセクションに、必要なすべての構成要件の一覧を示します。

VCS Expressway と VCS Control

VCS Control と VCS Expressway 間には、セキュアなトラバーサル ゾーン接続が必要です。

- VCS Control および VCS Expressway は*ユニファイド コミュニケーション トラバーサル*タイプのゾーンに設定する必要があります。これは自動的に適切なトラバーサル ゾーン（VCS Control 上で選択されたときは、トラバーサル クライアント ゾーン、VCS-E 上で選択されたときは、トラバーサル サーバ ゾーン）を設定します。そのゾーンは、**[TLS 検証モード（TLS verify mode）]** が *[オン（On）]* かつ **[メディア暗号化モード（Media encryption mode）]** が *[強制暗号化（Force encrypted）* の状態で SIP TLS を使用します。
- 両方の VCS が相互のサーバ証明書を信頼する必要があります。各 VCS がクライアントとサーバの両方として機能する際、各 VCS の証明書がクライアントとしてもサーバとしても有効であることを確認する必要があります。
- H.323 または暗号化されていない接続も必要な場合、トラバーサル ゾーンの個別のペアを設定する必要があります。

VCS Control

1. SIP ドメインを設定します（[設定（Configuration）] > [ドメイン（Domains）]。

   これは、委任された認証チェックを受信するすべてのドメインで設定する必要があります。
2. 関連するメカニズム認証（ローカル データベース、Active Directory サービス、または LDAP 経由の H.350 ディレクトリ）を設定します。
3. [委任クレデンシャル チェック（Delegated credential checking）] を有効にします（[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]）。
4. トラバーサル クライアント ゾーンが [委任クレデンシャル チェックを受け入れる（Accept delegated credential checks）] に設定されていることを確認します。

VCS Expressway

1. SIP ドメインを設定します（[設定（Configuration）] > [ドメイン（Domains）]。

   これは、認証チェックの委任先となるすべてのドメインで設定する必要があります。
2. ドメインごとに、クレデンシャル チェックの委任時に経由するトラバーサル ゾーンを選択します。
3. NTLM および Active Directory サービスの認証が必要な場合は、[NTLM プロトコル チャレンジ（NTLM protocol challenges）]（[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）]）が [自動（Auto）] に設定されていることを確認します。
4. [SIP] ページ（[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]）で [委任クレデンシャル チェック（Delegated credential checking）] を有効にします。
5. 関連ゾーンとサブゾーンの認証ポリシーが [クレデンシャルを確認する（Check credentials）] に設定されていることを確認します。

それでも、[クレデンシャルを確認する（Check credentials）] に設定されているゾーンまたはサブゾーンに届く H.323 メッセージは、そのローカル VCS 上の関連メカニズム（ローカル データベースや H.350 ディレクトリなど）によってクレデンシャルをチェックされ、委任はされません。

6. ダイヤル プランの一部として必要な場合は、SIP コール シグナリング メッセージを関連のトラバーサル クライアント ゾーンに転送する検索ルールを設定します。

   VCS Control への認証メッセージの委任をサポートするための固有の検索ルールは必要ありません。

VCS Expressway で行われる認証チャレンジのクレデンシャル チェックは、トラバーサル ゾーンを介して VCS Control に委任される必要があります。

クレデンシャル チェック サービスのテスト

クレデンシャル チェックを委任されている VCS がメッセージを受信して、関連の認証チェックを実行できるかどうか確認するには、以下の手順を実行します。

1. [設定（Configuration）] > [ドメイン（Domains）] に移動します。
2. 関連するドメインを選択します。
3. [クレデンシャル チェック サービスのテスト（Test credential checking service）].をクリックします。

   [結果（Results）] セクションが表示され、受信 VCS にトラバーサル ゾーン経由で到達できるかどうか、また、NTLM と SIP の両方のダイジェスト タイプのチャレンジのクレデンシャル チェックを実行できるかどうかが示されます。

   ビデオ ネットワークで NTLM 認証を使用していない場合、受信 VCS には Active Directory サービスへの接続が設定されていないため、NTLM のチェックは失敗します。

TURN サービス

TURN サービスが VCS Expressway で有効になっていて、TURN サーバの要求のクレデンシャル チェックも委任する場合は、以下の手順を実行します。

1. [設定（Configuration）] > [トラバーサル（Traversal）] > [TURN] を選択します。
2. [委任クレデンシャル チェック（Delegated credential checking）] を [オン（On）] に設定します。
3. [認証レルム（Authentication realm）] の場合は、一連の設定済み SIP ドメインから選択して、クレデンシャル チェックの委任時に経由するトラバーサル ゾーンを決めます。

その他の情報

- VCS Control と VCS Expressway のシステム クロックは、互いに 100 秒以内の範囲にある必要があります。すべての VCS が共通の NTP サーバを使用するように設定することをお勧めします。
- VCS Expressway は、引き続き特定のドメインに対して「ローカル」で委任されていない認証を実行できます。この認証が必要な場合は、以下の点を確認してください。

- 該当ドメインの [委任クレデンシャル チェックのためのトラバーサル ゾーン（Traversal zone for delegated credential checking）] が [委任しない（Do not delegate）] に設定されている。
- VCS Expressway に関連の認証メカニズムが設定されている。

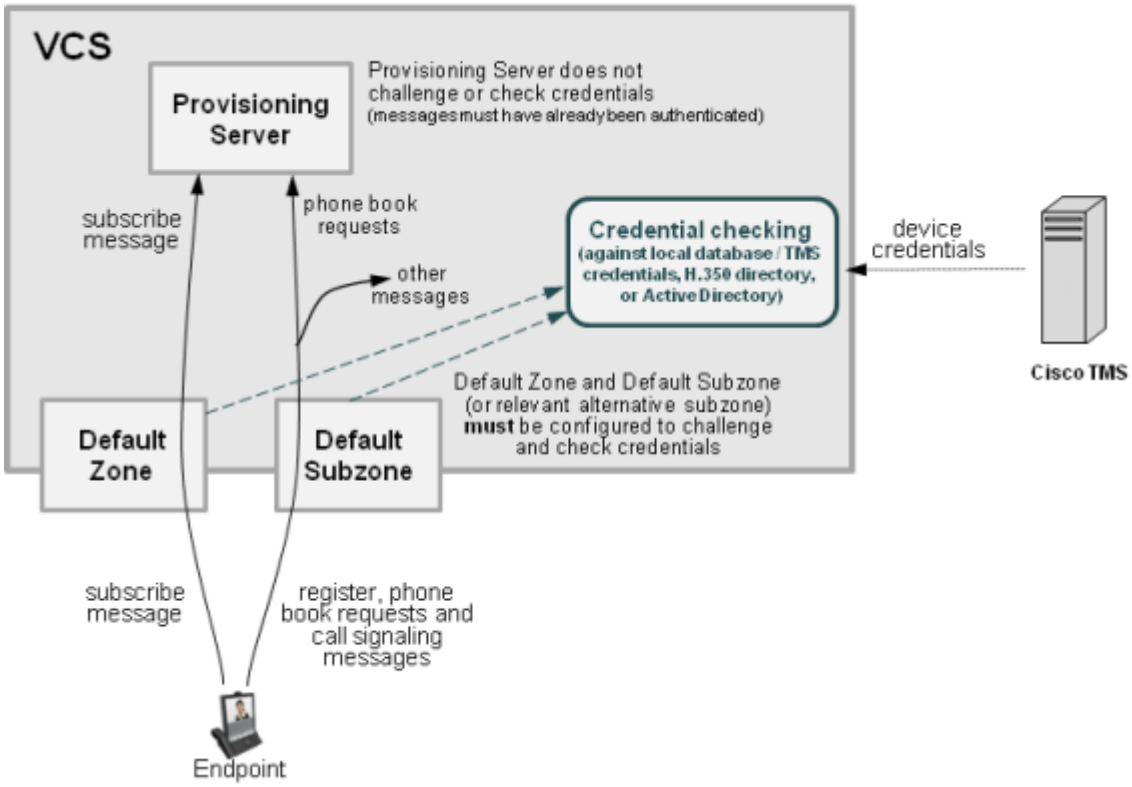
- VCS Control は引き続き通常の方法で認証を実行でき、VCS Expressway のために委任クレデンシャル チェックサービスを提供できます。次の点に注意してください。
  - VCS Control の [NTLM プロトコル チャレンジ（NTLM protocol challenges）] の設定は、VCS Control 自体が認証チャレンジを行っている場合のみ適用されます。
  - VCS Control 上のトラバーサル クライアントの認証ポリシーの設定は、VCS Control によって受信される委任クレデンシャル チェックの要求には無効です。

  委任クレデンシャル チェックを有効にしても、他のメッセージのルーティングには影響を及ぼしません。既存のトランスフォームや検索ルールなどを修正する必要はありません。

デバイス プロビジョニングと認証ポリシー

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、VCS へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

次の図に、エンドポイントからプロビジョニング サーバまでのプロビジョニング メッセージのフローおよびクレデンシャル チェック プロセスを示します。



VCS には、適切なデバイス認証設定が行われている必要があります。そうでなければ、プロビジョニング関連のメッセージは拒否されます。

- （サブスクライブ メッセージ）の初期プロビジョニングの認証は、デフォルト ゾーンの認証ポリシーの設定によって制御されます（デバイスがまだ登録されていないので、デフォルト ゾーンが使用されます）。

  デフォルト ゾーンおよびトラバーサル クライアント ゾーンの認証ポリシーは、[クレデンシャルを確認する（Check credentials）] または [認証済みとして扱う（Treat as authenticated）] のいずれかに設定されている必要があります。そうでなければ、プロビジョニング要求は失敗します。

- 後続メッセージ（登録要求、電話帳要求、コール シグナリング メッセージを含む）の認証は、エンドポイントが登録されている場合（通常のケース）は、デフォルト サブゾーン（または関連する代替サブゾーン）の認証ポリシーの設定によって制御され、エンドポイントが登録されていない場合は、デフォルト ゾーンの認証ポリシーの設定によって制御されます。

  関連する認証ポリシーは、[クレデンシャルを確認する（Check credentials）] または [認証済みとして扱う（Treat as authenticated）] のいずれかに設定されている必要があります。そうでなければ、電話帳要求は失敗します。

いずれの場合でも、VCS は、設定されている認証方式に従って、適切なクレデンシャル ストアとの認証チェックを実行します。VCS がローカル データベースを使用している場合は、Cisco TMS によって提供されるクレデンシャルもすべて含まれます。

一般的なプロビジョニング設定の詳細については、『*Cisco TMS Provisioning Extension Deployment Guide*』を参照してください。

VCS Starter Pack Express

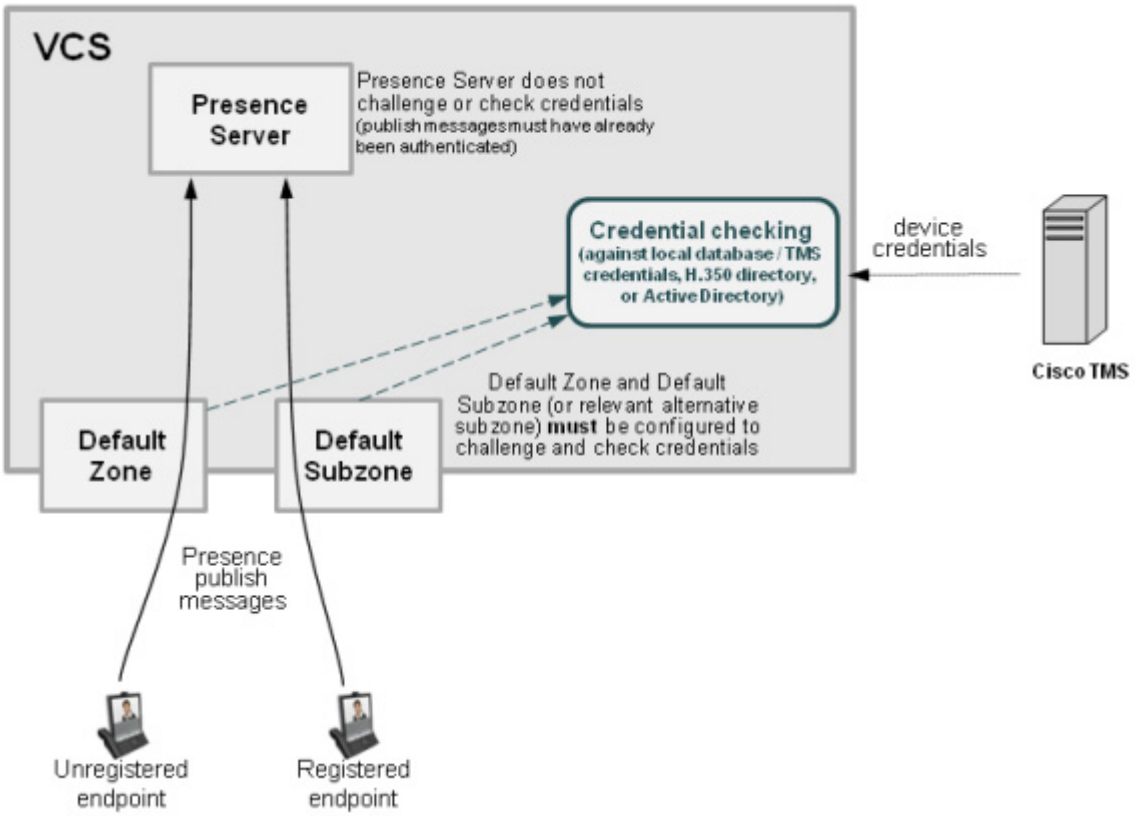
VCS Starter Pack Express 上のプロビジョニング サーバは、Cisco TMS プロビジョニングを使用する場合と同じ方法で動作するため、プロビジョニング要求をチャレンジしません。VCS によって要求が（ゾーンまたはサブゾーン エントリ ポイントで）すでに認証されている場合にのみ、デバイスをプロビジョニングします。

プレゼンスと認証ポリシー

プレゼンス サーバは、すでに認証されているプレゼンス PUBLISH メッセージのみ受け入れます。

- VCS によるプレゼンス メッセージの認証は、エンドポイントが登録されている場合にはデフォルト サブゾーン（または関連する代替サブゾーン）上の認証ポリシー設定によって制御され（通常のケース）、エンドポイントが登録されていない場合はデフォルト ゾーン上の認証ポリシー設定によって制御されます。
- 関連する [認証ポリシー（Authentication policy）] は、[クレデンシャルを確認する（Check credentials）] または [認証済みとして扱う（Treat as authenticated）] のいずれかに設定されている必要があります。そうでなければ、PUBLISH メッセージは失敗し、エンドポイントはそれぞれのプレゼンス ステータスをパブリッシュできなくなります。

次の図に、エンドポイントからプレゼンス サーバまでのプレゼンス メッセージのフローを示します。



いずれの場合でも、VCS は、設定されている認証方式に従って、適切なクレデンシャル ストアとの認証チェックを実行します。VCS がローカル データベースを使用している場合は、Cisco TMS によって提供されるクレデンシャルもすべて含まれます。

階層型ダイヤル プランと認証ポリシー

階層型ダイヤル プラン（ディレクトリ VCS）の導入とデバイス認証

ディレクトリ VCS による階層的なダイヤル プランを持つビデオ ネットワークに認証を導入する場合、次の条件では認証の問題が発生する可能性があります。

- ネットワーク内のいずれかの VCS が、そのネットワーク内にある他の VCS とは異なる認証データベースを使用している場合
- いずれかの VCS のデフォルト ゾーン上でクレデンシャル チェックが有効になっている場合（Cisco TMSPE を使用するときなどに必要）
- ディレクトリ VCS またはシグナリング パス内の他の VCS がコール ルーティング パスの外で自分を最適化できる場合

これらの導入では、各 VCS が、ネットワーク内の他のすべての VCS との間でネイバー ゾーンを設定される必要があります。各ゾーンで、[認証ポリシー（Authentication policy）] が [クレデンシャルを確認しない（Do not check credentials）] に設定されている必要があります （これらのネイバー ゾーンに検索ルールは必要ありません。これらのゾーンは、VCS 間のメッセージを信頼するためのメカニズムのみを提供します）。

この設定が必要なのは、そうしなければ、SIP RE-INVITE（最適なコール ルーティングを実現するために VCS 間で直接送信されるメッセージ）などの一部のメッセージがデフォルト ゾーンから届いたものとして分類されてしまうからです。その場合、VCS はメッセージの認証を試みますが、認証データベースに必要なクレデンシャルが存在しないことにより、認証に失敗する可能性があります。したがって、メッセージが拒否され、コールがドロップされる可能性があります。しかし、ノード VCS にネイバー ゾーン関係が設定されている場合、このメッセージはネイバー ゾーン経由で届いたものとして識別され、VCS はクレデンシャル チェックを実行せず（このネイバー ゾーンが [クレデンシャルを確認しない（Do not check credentials）] に設定されているため）、メッセージが受け入れられます。

複数の地域/サブネットワーク ディレクトリ VCS による導入

複数の地域サブネットワークにセグメント化され、それぞれに独自のディレクトリ VCS が存在する導入の場合、ネットワーク全体にわたって各 VCS とすべての VCS との間にネイバー ゾーンをセットアップすることは実行不可能です（または推奨されません）。

このシナリオでは、各サブネットワークを前述の説明に従って設定する必要があります（つまり、同一のディレクトリ VCS によって管理される各 VCS の間にネイバー ゾーンをセットアップします）。その後、ディレクトリ VCS 間のネイバー ゾーンを、それらがディレクトリ VCS 間のサブネットワークにまたがるコール時にコール シグナリング パス内にとどまるように設定します。手順は次のとおりです。

1. ディレクトリ VCS 上で、[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動し、他のディレクトリ VCS に関連するゾーンをクリックします。
2. [ゾーンの編集（Edit zones）] ページで、[詳細設定（Advanced）] セクションまで下にスクロールし、[ゾーン プロファイル（Zone profile）] を [カスタム（Custom）] に設定します。
3. [コール シグナリング ルーティング モード（Call signaling routed mode）] を [常時（Always）] に設定します。
4. [保存（Save）] をクリックします。
5. 「もう一方」のディレクトリ VCS 上の対応するゾーン定義に対してこの手順を繰り返します。その後、このプロセス全体を、他のすべてのディレクトリ VCS 間のゾーン設定にも繰り返し実行します。

注：[コール数（Calls）] ページのディレクトリ VCS のプライマリの [コール シグナリング ルーティング モード（Call signaling routed mode）] の設定は変更しないでください。

これは、各ディレクトリ VCS がサブネットワーク間で伝送されるコールのコール シグナリング パスに留まることを意味します。各サブネットワーク内で完結するコールについては、これまでどおり、各ディレクトリ VCS がコール シグナリング パスの外で自分を最適化できます。

また、各ディレクトリ VCSに、各サブネットワーク間で伝送されるコールを処理するのに十分なコール ライセンス（トラバーサルおよび非トラバーサル）があることを確認する必要があります。

認証ポリシーの実際の設定

VCS Control

次の表に、VCS-C で認証ポリシーを設定する際の実用的なガイドラインを示します。

認証ポイント	ガイドライン
デフォルト ゾーン	[クレデンシャルを確認する（Check credentials）] を使用します。
デフォルト サブゾーン	[クレデンシャルを確認する（Check credentials）] を使用します。
特定のローカル サブゾーン	既知のローカル サブネットの場合は、クレデンシャルを使用してすべてのローカル エンドポイントを設定しないように、[認証済みとして扱う（Treat as authenticated）] を使用します。 これは実用的なソリューションではありますが、[認証済みとして扱う（Treat as authenticated）] のサブゾーンは使用せず、すべてのエンドポイントに適切かつ一意のクレデンシャルを設定し、[クレデンシャルを確認する（Check credentials）] を使用することを推奨します。
その他のサブゾーン	[クレデンシャルを確認する（Check credentials）] を使用します。
トラバーサル ゾーン	[クレデンシャルを確認する（Check credentials）] を使用します。VCS Expressway からの要求のクレデンシャルは常に確認します。
ネイバー ゾーン	[クレデンシャルを確認しない（Do not check credentials）] を使用し、[SIP 認証信頼モード（SIP authentication trust mode）] を [オン（On）] に設定します。

VCS Expressway

VCS Expressway の認証ポリシーは、理想としては、VCS Control の場合と同じガイドラインに厳密に従うことが推奨されます。しかし、AD への直接アクセスまたは H.350 アクセスが必要な場合、多くのセキュリティ ポリシーでは、DMZ 内のデバイスがそれらのリソースへアクセスすることを許可しません。そのため、実用面からは、認証を VCS Control にまかせてしまうことが推奨されます。SIP デバイスの場合は委任クレデンシャル チェックを使用できるため、SIP デバイスを VCS Expressway に登録できますが、それらのデバイスは VCS Control に設定されているデバイス認証メカニズムを使用して認証されます。

登録の許可リストおよび拒否リストを使用して、VCS Expressway に登録可能なものを制限することもできます。認証されたユーザのみが発信コールを行えるようにするには、すべてのコール要求が VCS Control にルーティングされ、そこで認証可能な要求のみが転送されるようにする必要があります。

インフラストラクチャ デバイス

インフラストラクチャ製品（MCU など）が専用のサブゾーン（認証ポリシーが [認証済みとして扱う（Treat as authenticated）] に設定されている）に登録されるように、VCS を設定することを推奨します。

認証方式

VCS の認証方式の設定

VCS では、認証クレデンシャルの検証方法として 3 種類の方式がサポートされています。

- オンボックスのローカル データベースと照合（Cisco TMS から提供されるすべてのクレデンシャルを含む）
- 外部の H.350 ディレクトリ サービスへの LDAP 接続を使用
- Kerberos 接続を使用した Active Directory サーバへの直接アクセス（NTLM チャレンジのみ）

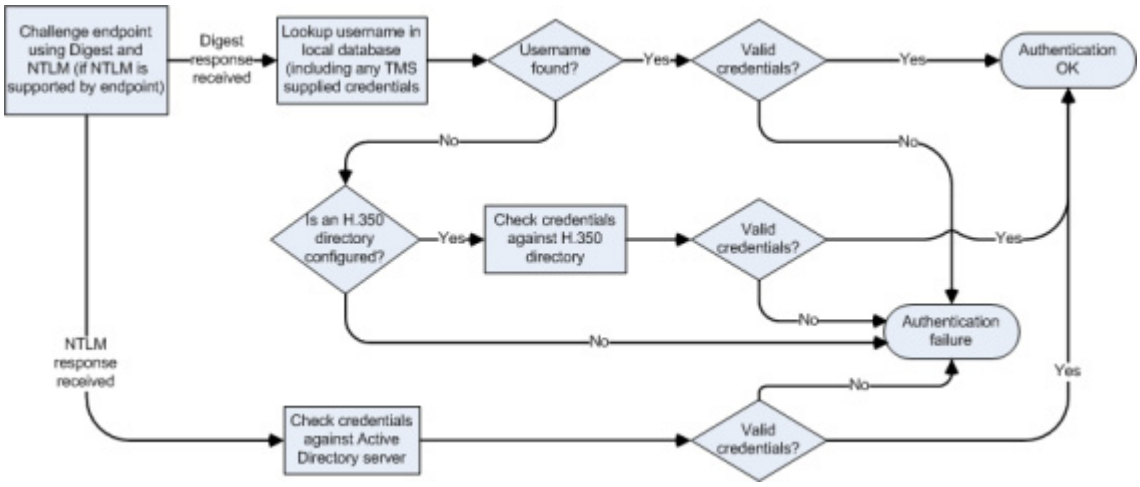
VCS は、提示されたクレデンシャルを検証するために、最初にユーザ名とパスワードが格納されているオンボックスのローカル データベースと照合します。システムがデバイス プロビジョニングを使用している場合、このローカル データベースには、Cisco TMS から提供されるクレデンシャルとの照合も含まれます。ユーザ名がローカル データベース内で見つからない場合、VCS は、外部の H.350 ディレクトリ サービスにリアルタイムで LDAP 接続して、クレデンシャルの検証を試みることもできます。このディレクトリ サービスが設定されている場合は、Microsoft Active Directory LDAP サーバ用または OpenLDAP サーバ用の H.350 ディレクトリ スキーマが存在する必要があります。

デバイスが NTLM チャレンジをサポートしている場合、前述のいずれかの方法とともに、VCS は Kerberos 接続で Active Directory サーバに直接アクセスしてクレデンシャルを検証することもできます。Kerberos による Active Directory の直接認証方式は、限られた範囲のエンドポイントでのみサポートされます（このマニュアルの執筆時点では、Cisco Jabber for iPad と Jabber Video のみ）。この認証方式が使用される場合、他の非サポートのエンドポイントデバイスは、残りの 2 つの認証方式のいずれかを使用して認証を継続します。

VCS は、常に標準のダイジェスト チャレンジでエンドポイントをチャレンジします。また、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が有効になっている場合に、エンドポイントでの NTLM サポートを認識した VCS は NTLM チャレンジも送信します。

エンドポイントが両方のチャレンジを受信した場合、ダイジェスト チャレンジと NTLM チャレンジのどちらに応答するかはエンドポイントが判断します。このマニュアルの執筆時点では、サポートされているすべてのエンドポイントが、ダイジェスト チャレンジに優先して NTLM チャレンジに応答します。

次の図に、クレデンシャルの認証時に VCS がたどるプロセスを示します。



H.323 デバイスの認証では、リプレイ アタックを防ぐために、正確なタイムスタンプが重要な役割を果たします。そのため、H.323 デバイスとのデバイス認証を使用する場合は、VCS とエンドポイントの両方が NTP サーバを使用してシステム時刻を同期している必要があります。

認証メカニズム

認証プロセスでは、ユーザ名とパスワードベースのチャレンジ/レスポンス方式を使用して、デバイスのクレデンシャルがチェックされます。

VCS にクレデンシャルを提供するために、デバイスによって実際に使用されるメカニズムは、使用しているプロトコルによって異なります。

- **H.323**：必要なクレデンシャルはすべて着信要求に含まれています （VCS は、通信する H.323 ネットワーク デバイスの ID を認証するための *ITU H.235 仕様*に対応しています）。
- **SIP**：クレデンシャルは初期要求には含まれていません。代わりに、VCS はクレデンシャルを要求している送信者にチャレンジを送り返します。ただし、SIP メッセージが（たとえば、前のホップ上の別の VCS によって）すでに認証されている場合、認証済みであることを示す情報がその SIP メッセージに挿入されることがあります。VCS が前段階で実行された認証を信頼するかどうかは、ゾーンの [SIP 認証信頼（SIP authentication trust）] の設定を設定することで制御できます。

VCS がトラバーサル サーバとして機能している場合、各トラバーサル クライアントの認証クレデンチャルが、選択したデータベースに入力されていることを確認する必要があります。

認証に使用されるエンドポイントのクレデンシャル

たとえば、登録を試みたときに、関連するサブゾーンの [認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] に設定されている場合に、VCS と認証する必要がある場合は、エンドポイントがその VCS にユーザ名とパスワードを提供する必要があります。

H.323 を使用しているシスコのエンドポイントの場合、ユーザ名は一般的にエンドポイントの [認証 ID（Authentication ID）] で、SIP を使用しているシスコのエンドポイントの場合は、一般的にエンドポイントの {認証名（Authentication username）] です。

エンドポイントのクレデンシャルの設定方法の詳細については、関連するエンドポイントのマニュアルを参照してください。

ローカル データベースを使用するための認証の設定

ローカル認証データベースは、VCS システムの一部として組み込まれているため、固有の接続設定は必要ありません。ユーザ アカウントの認証クレデンシャルを保存するために使用されます。各クレデンシャルのセットは**名前**と**パスワード**で構成されます。

ローカル データベース内のクレデンシャルは、デバイス（SIP および H.323）、トラバーサル クライアント、および TURN クライアントの認証に使用できます。

ローカル データベースへのクレデンシャルの追加

デバイス クレデンシャルのセットを入力するには、次の手順を実行します。

1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [ローカル データベース（Local Database）] に移動し、[新規（New）] をクリックします。
2. デバイスのクレデンシャルを表す**名前**と**パスワード**を入力します。
3. [クレデンシャルの作成（Create credential）] をクリックします。

2 台以上のデバイスで同じクレデンシャルを使用することができます。

Cisco TMS 内で管理されるクレデンシャル（デバイス プロビジョニング用）

VCS が TMS Provisioning Extension サービスを使用している場合、ユーザ サービスから提供されたクレデンシャルは、手動で設定されたエントリとともに、ローカル認証データベースに保存されます。[ソース（Source）] カラムで、ユーザ アカウント名が **TMS** から提供されたものか、**ローカル** エントリであるかを識別できます。編集できるのは、**ローカル** エントリのみです。

ローカル データベース内に Cisco TMS のクレデンシャルを組み込むことで、VCS は Cisco TMS 内で使用されている同一のクレデンシャルのセットと照合して（プロビジョニング要求だけではなく）すべてのメッセージを認証できます。

H.350 ディレクトリ認証と組み合わせたローカル データベース認証

VCS は、ローカル データベースと H.350 ディレクトリの両方を使用するように設定できます。

H.350 ディレクトリが設定されている場合、VCS は、提示されたダイジェスト クレデンシャルを検証する際は常に、最初にローカル データベースと照合してから、H.350 ディレクトリと照合します。

Active Directory（直接）認証と組み合わせたローカル データベース認証

Active Directory（直接）認証が設定されていて、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が [自動（Auto）] に設定されている場合、NTLM をサポートするデバイスに NTLM 認証チャレンジが提供されます。

- NTLM チャレンジは標準のダイジェスト チャレンジに加えて提供されます。
- NTLM をサポートするエンドポイントは、ダイジェスト チャレンジに優先して NTLM チャレンジに応答します。VCS は、その NTLM 応答の認証を試みます。

Starter Pack

Starter Pack オプション キーがインストールされると、ローカル認証データベースに、事前に設定された一連の認証クレデンシャルが組み込まれます。TURN サーバを Starter Pack と組み合わせて正しく動作させるには、ローカル認証データベース内の **StarterPackTURNUser** エントリを削除したり、変更したりしないでください。

Starter Pack でプロビジョニングされたデバイスをサポートするために必要な他のすべてのクレデンシャルは、ユーザ アカウントごとに手動で追加する必要があります。

LDAP 経由の H.350 ディレクトリ サービス ルックアップの使用

[H.350 デバイス認証設定（Device authentication H.350 configuration）] ページ（[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [H.350 ディレクトリ サービス（H.350 directory service）]）は、LDAP を介した H.350 ディレクトリ サービスへの接続を設定するために使用します。H.350 ディレクトリ サービス検索は、任意のエンドポイント（SIP および H.323）を認証するために使用できます。

H.350 ディレクトリの認証と登録プロセス

VCS が H.350 ディレクトリ サービスを使用して登録要求を認証している場合のプロセスは以下のとおりです。

1. エンドポイントから VCS にユーザ名と認証クレデンシャル、および登録対象のエイリアスが提示されます。
2. 次に、VCS が [登録用エイリアスのソース（Source of aliases for registration）] の設定に基づき、そのエンドポイントとの登録を許可するエイリアスを決定します。H.323 エンドポイントの場合、この設定を使用して、エンドポイントから提示されたエイリアスを H.350ディレクトリ内のエイリアスでオーバーライドするか、またはそれらのエイリアスをエンドポイントのエイリアスに加えて使用することができます。SIP エンドポイントの場合、この設定を使用して、エンドポイントの AOR が H.350 ディレクトリのものと一致しない場合に登録を拒否できます。次のオプションがあります。
   - [H.350 ディレクトリ（H.350 directory）]：SIP 登録の場合、エンドポイントから提示される AOR は、エンドポイントのユーザ名用の H.350 ディレクトリに含まれているならば登録されます。

     H.323 の登録の場合

- エンドポイントから提示される少なくとも 1 つのエイリアスが、そのエンドポイントのユーザ名用の H.350 ディレクトリに含まれている必要があります。提示されたエイリアスがどれも含まれていない場合、登録はできません。
- エンドポイントは、H.350 ディレクトリに含まれているすべてのエイリアス（最大 20）に登録されます。エンドポイントから提示された、H.350 ディレクトリに含まれていないエイリアスは登録されません。
- H.350 ディレクトリにエイリアスが 1 つも含まれていない場合、エンドポイントは提示したすべてのエイリアスに登録されます。
- エンドポイントからエイリアスが提示されない場合、そのユーザ名用の H.350 ディレクトリに含まれているすべてのエイリアスに登録されます。

- [複合（Combined）]：エンドポイントのユーザ名用の H.350 ディレクトリに含まれているエイリアスに加えて、エンドポイントから提示されたエイリアスが使用されます。つまり、エンドポイントから提示されたエイリアスが H.350 ディレクトリに存在しない場合、そのエイリアスに登録できる点を除き、[H.350 ディレクトリ（H.350 directory）] の場合と同じです。
- [エンドポイント（Endpoint）]：エンドポイントから提示されたエイリアスが使用されます。H.350 ディレクトリにあるエイリアスは無視されます。エンドポイントからエイリアスが提示されない場合、登録はできません。

デフォルトは、[H.350 ディレクトリ（H.350 directory）] です。

認証ポリシーが [クレデンシャルを確認しない（Do not check credentials）] または [認証済みとして扱う（Treat as authenticated）] に設定されている場合、[登録用エイリアスのソース（Source of aliases for registration）] の設定は無視され、エンドポイントから提示されたエイリアスが使用されます。

LDAP サーバ ディレクトリの設定

LDAP サーバ上の H.350 ディレクトリは、*ITU H.350 仕様*を実装するように設定する必要があります。H.350 ディレクトリには、VCS が通信するデバイスのクレデンシャル、および VCS に登録されるエンドポイントのエイリアスを保存する必要があります。

1. 必要な H.350 スキーマを VCS からダウンロードして（[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [H.350 ディレクトリ スキーマ（H.350 directory schemas）]）、LDAP サーバにインストールします。
2. VCS に登録されるエンドポイントのエイリアスを指定して、ディレクトリを設定します。

LDAP サーバ設定の設定

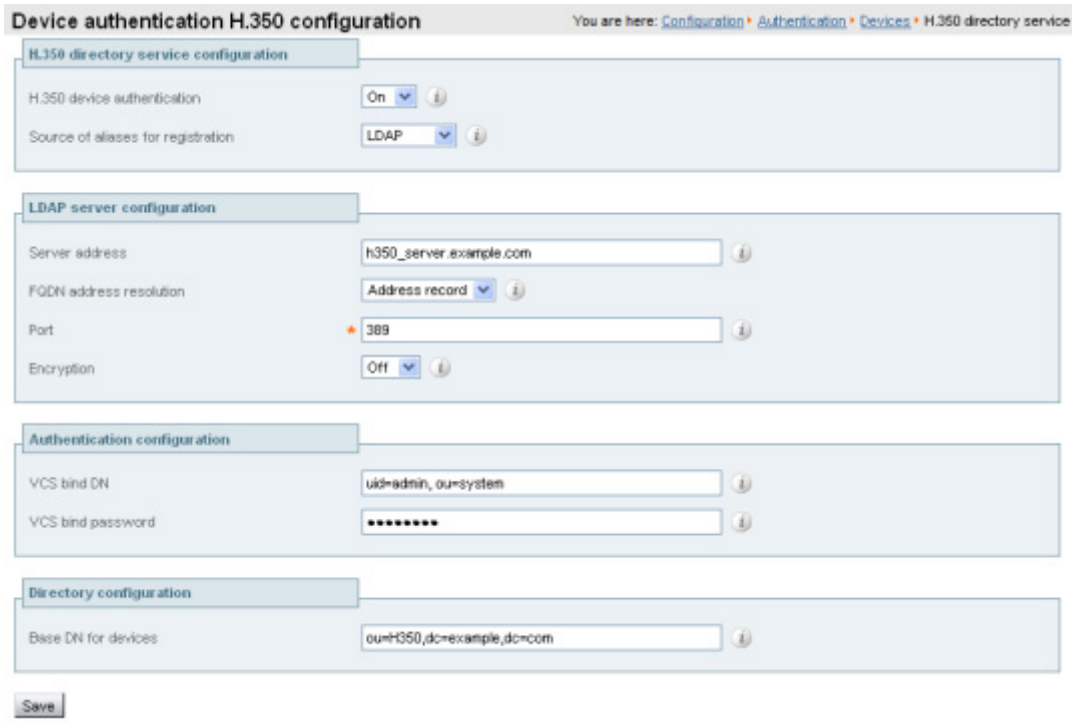
1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [H.350 ディレクトリ サービス（H.350 directory service）] に移動します。
2. フィールドを次のように設定します。

H.350 デバイス認証（H.350 device authentication）	[オン（On）] を選択します。	H.350 ディレクトリは他の認証メカニズムと組み合わせて使用できます。
登録用エイリアスのソース（Source of aliases for registration）	エイリアスの確認および登録方法を決定します。	各設定の詳細については、前述の「**H.350 ディレクトリの認証と登録プロセス**」を参照してください。 [登録用エイリアスのソース（Source of aliases for registration）] が [H.350 ディレクトリ（H.350 directory）] の場合、MCU は特別なケースとして扱われます。MCU は提示されたエイリアスに登録され、H.350 ディレクトリ内のエイリアスは無視されます（このため、MCU で、会議用のエイリアスを付加的に登録することもできます）。
サーバ アドレス（Server address）	LDAP サーバの IP アドレスまたは FQDN（あるいは、DNS **ドメイン名**も設定されている場合はサーバ アドレス）。	LDAP サーバには、H.350 スキーマがインストールされている必要があります。 TLS を使用する場合、ここに入力するアドレスは、LDAP サーバから提示される証明書に含まれる CN（コモン ネーム）と一致している必要があります。
FQDN アドレス解決（FQDN address resolution）	LDAP **サーバ アドレス**が FQDN として指定されている場合の解決方法を定義します。 [アドレス レコード（Address record）]：DNS A レコードまたは AAAA レコード ルックアップ。 [SRV レコード（SRV record）]：DNS SRV レコード ルックアップ。 **注：**SRV レコードを使用する場合は、レコードが LDAP の標準ポートを使用していることを確認してください。`_ldap._tcp.<domain>` は 389 を使用し、`_ldaps._tcp.<domain>` は 636 を使用する必要があります。VCS は LDAP 用の他のポート番号をサポートしていません。	DNS SRV ルックアップにより、VCS は複数のリモート H.350 ディレクトリ サーバに対してデバイスを認証することができます。このため、H.350 ディレクトリ サーバへの到達可能性の問題が発生した時にシームレスな冗長メカニズムが得られます。 SRV ルックアップは、**暗号化**が有効かどうかに応じて、_ldap._tcp レコードまたは _ldaps._tcp レコードのいずれかに対して実行されます。複数のサーバが返された場合、各 SRV レコードのプライオリティとウェイトによって、サーバが使用される順序が決まります。
ポート（Port）	LDAPサーバの IP ポート	非セキュア接続は *389*、セキュア接続は *636* を使用します。

暗号化（Encryption）	LDAP サーバへの接続がトランスポート層セキュリティ（TLS）を使用して暗号化するかどうかを決定します。 [TLS]：LDAP サーバへの接続に TLS 暗号化を使用します。 [オフ（Off）]：暗号化は使用されません。	TLS が有効になっている場合、LDAP サーバの証明書は、VCS の信頼済み CA 証明書ファイル内の認証局によって署名されている必要があります。 [TLS 用の CA 証明書ファイルをアップロード（Upload a CA certificate file for TLS）]（[関連タスク（Related tasks）] セクション内）をクリックし、[信頼できる CA 証明書（Trusted CA certificate）] ページに移動します。
バインド DN（Bind DN）	LDAP サーバにバインドするときに VCS で使用されるユーザ識別名。	例、uid=admin、ou=system
バインド パスワード（Bind Password）	LDAP サーバにバインドするときに VCS で使用されるパスワード。	
デバイスのベース DN（Base DN for devices）	クレデンシャル情報を検索する LDAP サーバのディレクトリの領域。これは、H.350 オブジェクトが存在する LDAP ディレクトリ内の識別名（DN）として指定する必要があります。	例：ou=H350、dc=example、dc=com

3. [保存（Save）] をクリックします。

指定した LDAP サーバへの接続の現在のステータスがページの下部に表示されます。



他の認証メカニズムを使用した H.350 ディレクトリの使用

H.350 ディレクトリ認証と組み合わせたローカル データベース認証

VCS は、ローカル データベースと H.350 ディレクトリの両方を使用するように設定できます。

H.350 ディレクトリが設定されている場合、VCS は、提示されたダイジェスト クレデンシャルを検証する際は常に、最初にローカル データベースと照合してから、H.350 ディレクトリと照合します。

Active Directory（直接）認証と組み合わせた H.350 ディレクトリ サービス認証

Active Directory（直接）認証が設定されていて、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が [自動（Auto）] に設定されている場合、NTLM をサポートするデバイスに NTLM 認証チャレンジが提供されます。NTLM をサポートしないデバイスは標準のダイジェスト チャレンジを受信し続けます。

Active Directory データベース（直接）の使用

Active Directory データベース（直接）認証は、NTLM プロトコル チャレンジを使用し、Kerberos 接続で Active Directory サーバに直接アクセスしてクレデンシャルを認証します。

Active Directory データベース（直接）認証は、ローカル データベースおよび H.350 ディレクトリ サービス認証と同時に有効にできます。これは、NTLM 認証が一部のエンドポイントでしかサポートされていないためです。そのため、たとえば、Jabber Video に対しては Active Directory（直接）サーバ方式を使用し、NTLM をサポートしない他のデバイスに対してはローカル データベースまたは H.350 ディレクトリ サービス認証を使用することができます。

Active Directory（直接）認証が設定されていて、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が [自動（Auto）] に設定されている場合、NTLM をサポートするデバイスに NTLM 認証チャレンジが提供されます。NTLM をサポートしないデバイスは標準のダイジェスト チャレンジを受信し続けます。

設定の前提条件

Active Directory

- VCS がドメインに対して参加と離脱を行うために使用する、「アカウント オペレータ」または「管理者」のアクセス権限を持つ AD ユーザ アカウントのユーザ名およびパスワードを用意する必要があります。
- この方式で認証されるすべてのデバイスのエントリが Active Directory サーバ内に存在している必要があります。各エントリには、パスワードが関連付けられている必要があります。
- （すべてのドメインの）デバイス エントリは、VCS がドメインに参加するために使用するユーザ アカウントからアクセスできる必要があります。VCS がフォレストを構成するドメイン内に存在し、そのフォレスト内のドメイン間に信頼が存在する場合、他のドメインに対してデバイスを認証するための適切な権限がユーザ アカウントに与えられていれば、VCS は異なるドメインのデバイス エントリを認証できます。

Kerberos キー発行局

KDC（Kerberos キー発行局）サーバは、タイム サーバと同期されている必要があります。

DNS サーバ

DNS 名または DNS SRV 名を使用して AD サーバが識別される場合は、関連する詳細情報が DNS サーバに設定されている必要があります。（AD サーバの指定に DNS/DNS SRV を使用しない場合であっても、DNS サーバを使用するように VCS が設定されている必要があることに注意してください）。

VCS

- VCS は、DNS サーバを使用するように設定する必要があります（[システム（System）] > [DNS]）。
  - VCS の [システム ホスト名（System host name）]（[システム（System）] > [DNS]）は 15 文字以内で指定する必要があります。

    （Microsoft NetBIOS 名は 15 文字に制限されます）。
  - クラスタの一部の場合は、各 Cisco VCS ピアに一意の [システム ホスト名（System host name）] が設定されていることを確認します。
- NTP サーバ（[システム（System）] > [時刻（Time）]）が構成されていて、アクティブであることを確認します。
- 接続で TLS 暗号化を使用する場合は、有効な CA 証明書、秘密キー、およびサーバ証明書を VCS にアップロードする必要があります。
- VCS は、関連するゾーンおよびサブゾーンの認証をチャレンジするように設定する必要があります。
  - デフォルト ゾーン（[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] を選択して、[デフォルト ゾーン（Default Zone）] を選択）では、[認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] に設定されている必要があります これにより、プロビジョニング要求（および登録されていないデバイスからのコール要求）が確実にチャレンジされます。
  - デフォルト サブゾーン（[設定（Configuration）] > [ローカル ゾーン（Local Zone）] > [デフォルト サブゾーン（Default Subzone）]）（または関連するサブゾーン）では、[認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] に設定されている必要があります。これにより、登録されたデバイスからの登録要求、プレゼンス要求、電話帳要求、およびコール要求が確実にチャレンジされます。

クレデンシャルを確認するための認証ポリシーを設定すると、プロビジョニング要求、登録要求、プレゼンス要求、電話帳要求、およびコール要求を VCS に送信するすべてのデバイスに影響を及ぼします。

エンドポイント

Jabber Video が動作する PC では、AD サーバの設定と一致する設定を使用する必要があります。

Active Directory サービス（ADS）への接続の設定

[Active Directory サービス（Active Directory Service）] ページ（[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）]）は、Jabber Video エンドポイント（バージョン 4.2 以降）のデバイス認証を行うための Active Directory サービスへの接続を設定するために使用します。

Active Directory サービスの設定の設定

Active Directory（直接）を設定し、AD ドメインに参加するには、次の手順を実行します。

1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）] に移動します。
2. フィールドを次のように設定します。

Active Directory サービスへの接続（Connect to Active Directory Service）	[オン（On）] を選択します。	[Active Directory サービスへの接続（Connect to Active Directory Service）] を [オフ（Off）] にしても、VCS は AD ドメインから離脱しません。
NTLM プロトコル チャレンジ（NTLM protocol challenges）	SIP 経由でデバイスを認証するときに、VCS が（ダイジェスト チャレンジに加えて）NTLM プロトコル チャレンジを送信するかどうかを制御します。 [自動（Auto）]：VCS は、デバイス タイプに基づいて、NTLM チャレンジを送信するかどうかを決定します。 [オフ（Off）]：NTLM チャレンジは送信されません。 [オン（On）]：NTLM チャレンジは常に送信されます。 デフォルトは [自動（Auto）] です。	通常は [自動（Auto）] に設定する必要があります。 既存の認証メカニズムから ADS に移行している場合、AD サーバへの接続を設定している間は [オフ（Off）] を選択します。その後、接続がアクティブになり、この認証メカニズムに切り替える準備ができたら、[自動（Auto）] を選択します。 [オン（On）] は絶対に使用しないでください。[オン（On）] にすると、NTLM をサポートしていないデバイスにも NTLM チャレンジが送信されるため、デバイスがクラッシュしたり、動作がおかしくなったりすることがあります。 VCS は NTLM チャレンジを送信するために、Active Directory サービスに接続する必要があります。

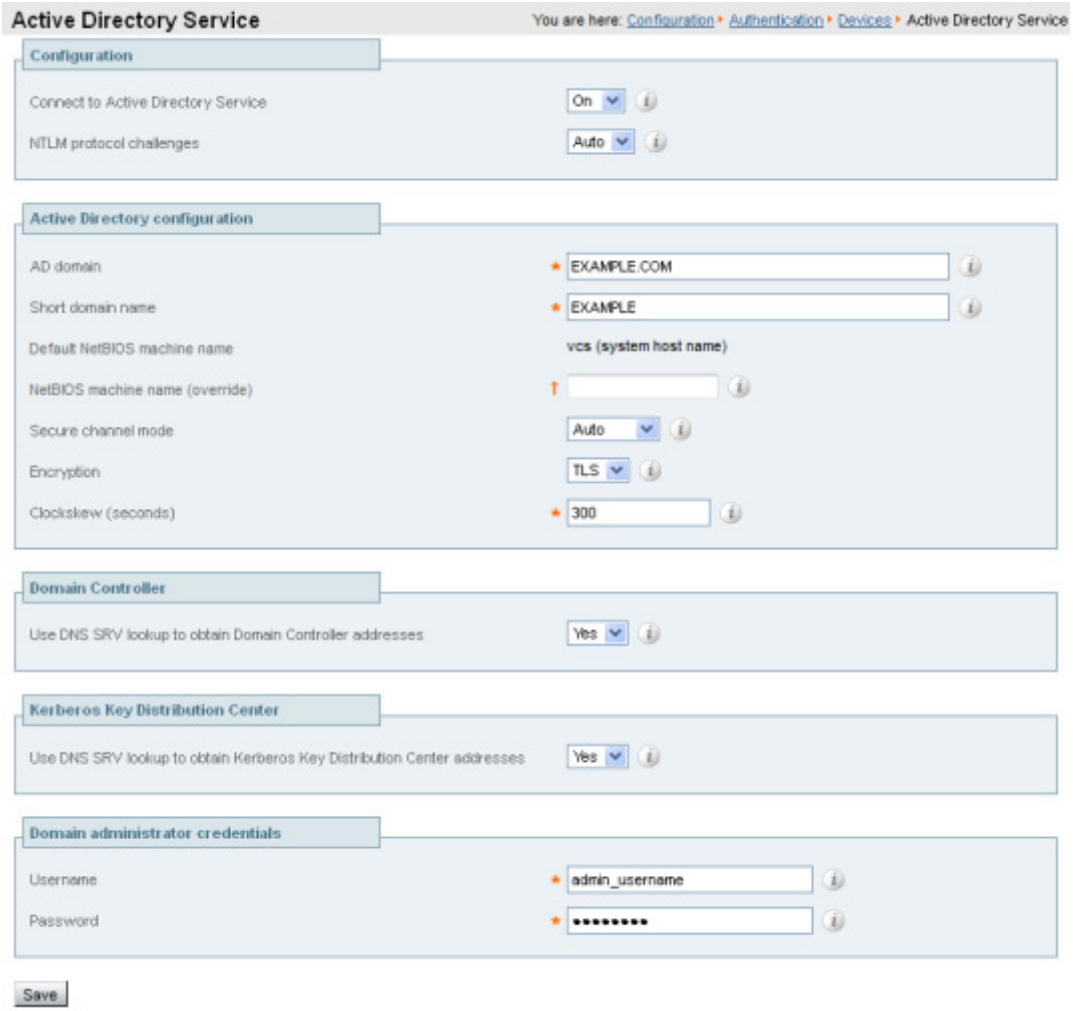
AD ドメイン（AD domain）	これは、VCS が参加する AD ドメインの完全修飾ドメイン名（FQDN）である必要があります。EXAMPLE.COM のように大文字で入力する必要があります。	一般的に、ドメインは Kerberos サーバの DNS 名と同一です。 大文字での入力は、Active Directory に大文字と小文字の区別の問題があるために適用されています。
短いドメイン名（Short domain name）	VCS が AD ドメインに参加するときに使用する短いドメイン名です。	これは NetBIOS ドメイン名とも呼ばれています。
NetBIOS マシン名（NetBIOS machine name）（オーバーライド）	デフォルトでは、[システム ホスト名（System host name）] が AD ドメインに参加するときの NetBIOS マシン名として使用されます。必要に応じて、別の名前を入力して、デフォルト名をオーバーライドできます。	[システム ホスト名（System host name）] が 15 文字を超えている場合は、オーバーライドを指定する必要があります。
セキュア チャネル モード（Secure channel mode）	VCS から AD ドメイン コントローラに送信されたデータがセキュア チャネル経由で送信されているかどうかを示します。 [自動（Auto）]：ドメイン コントローラの設定に自動的に適合します。 [有効（Enabled）]：常にセキュア チャネルの使用を試みます。 [無効（Disabled）]：セキュア チャネルを使用しません。 デフォルトは [自動（Auto）] です。	[自動（Auto）] を使用することを推奨します。
暗号化（Encryption）	Active Directory サービスへの LDAP 接続に使用する暗号化を設定します。 [オフ（Off）]：暗号化は使用されません。 [TLS]：TLS 暗号化が使用されます。 デフォルトは、[TLS] です。	暗号化を [TLS] に設定する場合は、有効な CA 証明書、秘密キー、およびサーバ証明書を VCS にアップロードする必要があります。 [TLS 用の CA 証明書ファイルをアップロード（Upload a CA certificate file for TLS）]（[関連タスク（Related tasks）] セクション内）をクリックし、[信頼できる CA 証明書（Trusted CA certificate）] ページに移動します。
クロック スキュー（Clock skew）	Kerberos メッセージが無効だとみなされる前に、VCS と KDC 間で許可される最大のクロック スキュー（秒単位）。 デフォルトは 300 秒です。	これは、KDC のクロック スキューの設定と一致している必要があります。 VCS と KDC がタイム サーバに同期されていることを確認してください。

DNS SRV 検索を使用してドメイン コントローラのアドレスを取得する（Use DNS SRV lookup to obtain Domain Controller addresses）	[はい（Yes）] が推奨の設定です。VCS は、**AD ドメイン**の DNS SRV ルックアップを使用して、AD ドメイン コントローラのアドレスの詳細を取得します。 ルックアップでアドレスを得られない場合は、このフィールドを [いいえ（No）] に設定し、表示される [アドレス 1（Address 1）] フィールドにプライマリ ドメイン コントローラの IP アドレスを入力します。	
DNS SRV 検索を使用して Kerberos キー配布センターのアドレスを取得する（Use DNS SRV lookup to obtain Kerberos Key Distribution Center addresses）	[はい（Yes）] が推奨の設定です。VCS は、**AD ドメイン**の DNS SRV ルックアップを使用して、Kerberos キー発行局サーバのアドレスの詳細を取得します。 ルックアップでアドレスを得られない場合は、このフィールドを [いいえ（No）] に設定し、表示される [アドレス 1（Address 1）] フィールドにプライマリ キー発行局サーバの IP アドレスを入力します。通常、[ポート 1（Port 1）] にはデフォルト値の 88 をそのまま使用できます。	一般的に、KDC アドレスはドメイン コントローラ アドレスと同一です。
ユーザ名（Username）およびパスワード（Password）	AD ドメイン管理者のユーザ名とパスワード。パスワードは大文字と小文字が区別されます。	ドメインに参加する場合にのみ、ドメイン管理者のクレデンシャルが必要です。VCS はドメインに一度だけ参加すればよく、その後は必要に応じて接続を有効または無効にできます。

3. [保存（Save）] をクリックして設定を保存し、AD ドメインに参加します。

   VCS が AD ドメインに参加します。エラー メッセージが表示された場合は、次を確認してください。

   - このページの設定（ユーザ名とパスワードを含む）
   - VCS の CA 証明書、秘密キー、およびサーバ証明書
   - [Active Directory サービス（Active Directory Service）] ページの下部にある [ステータス（Status）] 領域。AD ドメインへの接続ステータスに関する詳細を確認できます。



次の点に注意してください。

- ドメイン管理者のユーザ名とパスワードは VCS には保存されません。これらは AD ドメインに参加する（または離脱する）場合のみ必要になります。
- VCS は AD ドメインに一度だけ参加すればよく、Active Directory サービスへの接続が無効になり、再び有効にする場合でも、もう一度参加する必要はありません。参加が再び必要になるのは、VCS がドメインを離脱した場合、あるいは別のドメインに参加する必要があるときだけです。

プライマリ以外のドメイン コントローラと Kerberos キー発行局サーバの追加（任意）

この手順は、**AD ドメイン**の DNS SRV ルックアップを使用してドメイン コントローラ サーバと Kerberos キー発行局サーバのアドレスの詳細を取得していない場合にのみ必要です。

1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）] に移動します。
2. 追加のドメイン コントローラ サーバのアドレスを最大で 4 つまで入力します（合計で最大 5 つ）。

3. 追加の Kerberos キー発行局サーバのアドレスおよびポート番号を最大で 4 組まで入力します（合計で最大 5 組）。
4. [保存（Save）] をクリックします。
5. VCS がクラスタの一部である場合は、マスター ピア上で入力した設定が残りの各ピアに複製されていることを確認します。

クラスタ化 VCS システム

クラスタ化されたシステムでは、各 VCS が AD ドメインに別々に参加する必要があります。手順は次のとおりです。

マスター ピア上で、次の手順を実行します。

1. 前述の手順に従って、Active Directory（直接）を設定し、AD ドメインに参加します。
2. 作業を続ける前に、マスター ピアが AD ドメインに正常に参加したことを確認してください。

残りの各ピア上で、次の手順をそれぞれ実行します。

1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）] に移動します。
2. マスター ピア上で入力した設定が現在のピアに複製されていることを確認します。
3. AD ドメイン管理者の [ユーザ名（Username）] と [パスワード（Password）] を入力します。
   （これらのクレデンシャルは VCS によって保存されないため、毎回入力する必要があります）。
4. [保存（Save）] をクリックします。

   VCS が AD ドメインに参加します。エラー メッセージが表示された場合は、次を確認してください。

   - このページの設定（ユーザ名とパスワードを含む）
   - VCS の CA 証明書、秘密キー、およびサーバ証明書（CA 証明書情報はクラスタ ピア間で複製されません）

NTLM 認証チャレンジの有効化

Active Directory の詳細が設定され、VCS が AD ドメインに参加したら、Jabber Video（4.2 以降）を NTLM 認証チャレンジでチャレンジするように VCS を設定できます。

1. [設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）] に移動します。
2. [NTLM プロトコル チャレンジ（NTLM protocol challenges）] が [自動（Auto）] に設定されていることを確認します。

   [オン（On）] は絶対に使用しないでください。[オン（On）] にすると、NTLM をサポートしていないデバイスにも NTLM チャレンジが送信されるため、デバイスがクラッシュしたり、動作がおかしくなったりすることがあります。
3. 必要に応じて [保存（Save）] をクリックします。

4. VCS がクラスタの一部である場合は、マスター ピア上で入力した設定変更が残りの各ピアに複製されていることを確認します。

Jabber Video の設定および Active Directory データベース（直接）認証のテスト

プロビジョニングまたは VCS 認証を使用してすでに認証に成功している Jabber Video の設定を使用することを推奨します。そうすることで、Jabber Video の詳細設定（[内部サーバ（Internal Server）]、[外部サーバ（External Server）]、および [SIP ドメイン（SIP domain）] のエントリ）が正しく設定されます。

1. Jabber Video にサインインします。
2. [ユーザ名（Username）] フィールドで、`<AD Short Domain Name>\username` を設定します

   （このフィールドでは、大文字と小文字は区別されません）。
3. [パスワード（Password）] フィールドに、Active Directory データベースに設定されている選択したユーザのパスワードを入力します。
4. [サインイン（Sign In）] をクリックします。

登録に成功すれば、VCS への Jabber Video のプロビジョニングおよび登録の認証が、Active Directory データベース（直接）認証を使用して機能することが確認されたことになります。

ポート

AD システムとの通信に使用されるポートの一覧については、36 ページの「デバイス認証ポートのリファレンス」を参照してください。

外部システムによる認証

[アウトバウンド接続クレデンシャル（Outbound connection credentials）] ページ（[設定（Configuration）] > [認証（Authentication）] > [アウトバウンド接続クレデンシャル（Outbound connection credentials）]）は、外部システムとの認証が必要な場合に VCS が常に使用するユーザ名とパスワードを設定するために使用します。

たとえば、VCS がエンドポイントから他の VCS に招待を転送している場合、その別のシステムで認証が有効になっているために、ローカル VCS がユーザ名とパスワードをそのシステムに提供する必要があることがあります。

これらの設定はトラバーサル クライアント ゾーンでは使用されません。接続前に、トラバーサル サーバと常に認証する必要があるトラバーサル クライアントでは、トラバーサル クライアント ゾーンごとに接続のクレデンシャルを設定します。

付録 1： トラブルシューティング

ここでは、認証に関する問題のトラブルシューティングおよび解決に役立つ情報を示します。

ローカル データベースのトラブルシューティング

固有のトラブルシューティングはありません。

H.350 ディレクトリ サービスのトラブルシューティング

固有のトラブルシューティングはありません。

Active Directory（直接）のトラブルシューティング

パスワードの確認

デバイス固有のエントリである場合は、パスワードがアクティブになっていて、期限切れになっていないことを確認します。

ユーザ ログインである場合は、ユーザが別のアプリケーションでそのユーザ名とパスワードを使用できることを確認します。

Jabber Video が認証に失敗する

NTLM バージョンの不一致

Active Directory（直接）モードを使用するには、Jabber Video を実行している PC が、AD サーバと適合する適切な設定を使用している必要があります。確認（および必要に応じて変更）する場合は、「Jabber Video PC および AD サーバの互換性の設定」を参照してください。

ユーザ名が長すぎる

Jabber Video ユーザ名は、20 文字以下にする必要があります。ユーザ名の長さが 20 文字を超えると、Active Directory の制限によって名前が切り詰められてしまうため、ログインに失敗します。

Netlogon ログ エラー コード：NTreasonCodes

AD 直接認証の診断ログには、失敗時に NT から提供される理由コードの値が返されます。このログには、「NTreasonCode=" <value>" 」が含まれています。これらの値については、http://technet.microsoft.com/en-us/library/cc776964%28v=ws.10%29.aspx [英語] に文書化されています。次に要約を示します。

ログ コード	説明
0x0	ログイン成功
0xC0000022	ドメイン コントローラがアクセスを拒否しています（ドメインへの参加を再試行してください）

ログ コード	説明
0xC0000064	指定されたユーザが存在しません（ユーザ名が存在しません）
0xC000006A	現在のパスワードとして入力された値が正しくありません（名前は正しいですが、パスワードが間違っています）
0xC000006C	パスワード ポリシーに適合しません
0xC000006D	ユーザ名に誤りがあるため、ログインの試行は無効です
0xC000006E	ユーザ アカウント制限により、ログインに失敗しました
0xC000006F	ユーザ アカウントに時間帯の制限が設定されており、この時間にログインすることはできません（ユーザが曜日または時刻の制限範囲外でログインしようとしました）
0xC0000070	ユーザには制限が設定されており、このソース ワークステーションからはログインできません
0xC0000071	ユーザ アカウントのパスワードの有効期限が切れています
0xC0000072	ユーザ アカウントが現在無効になっています
0xC000009A	システム リソースが不足しています
0xC0000133	DC と他のコンピュータとの間でクロックの同期が極端にずれています
0xc000015b	このマシンでは、要求されたログイン タイプ（ログイン権限）がユーザに付与されていません
0xC0000193	ユーザのアカウントの有効期限が切れています。
0xC0000224	ユーザはログインする前に自分のパスワードを変更する必要があります
0xC0000234	ユーザ アカウントが自動的にロックされました（ユーザは現在ロックアウトされています）

ビデオ エンドポイントで AD 直接認証によるログインに失敗した後、PC にログインできない

許容されるログインの失敗回数が AD 認証で制限されている場合、エンドポイントからのログインの失敗は、AD を使用して認証を行う他のすべてのデバイスの認証に影響を与えます。

デバイス プロビジョニング（TMSPE モード）とプレゼンス

プロビジョニング用の SUBSCRIBE が拒否される/プロビジョニングされたエンドポイントがサイン　インできない

- デフォルト ゾーンで [認証ポリシー（Authentication policy）] が [クレデンシャルを確認する（Check credentials）] または [認証済みとして扱う（Treat as authenticated）] に設定されていることを確認します。

[認証ポリシー（Authentication policy）] が [クレデンシャルを確認しない（Do not check credentials）] の場合、プロビジョニング用の SUBSCRIBE と Jabber Video のサインインは失敗します。

認証が [クレデンシャルを確認する（Check credentials）] に設定されている場合は（推奨）、適切なユーザ名とパスワードが、関連するクレデンシャル データベースに設定されている必要があります。

- アカウント ユーザ名、認証クレデンシャル名、および Jabber Video サインイン ユーザ名がすべて一致していることを確認します（X7.1 以降では、ユーザ名の大文字と小文字は区別されません）。

Jabber Video サインイン ユーザ名と認証クレデンシャル名が一致しない場合、最初のサブスクライブは未許可として拒否されます。

Jabber Video サインイン ユーザ名とアカウント ユーザ名が一致しない場合、サブスクライブは認証されますが、「Reason: rejected; Content length: 0」の通知が送信されます。

電話帳検索でエントリが返ってこない

デフォルト サブゾーンで [認証ポリシー（Authentication policy）] が [クレデンシャルを確認しない（Do not check credentials）] に設定されている場合、電話帳検索要求は拒否されます。

- デフォルト サブゾーンの認証を [クレデンシャルを確認する（Check credentials）] に設定し、適切なユーザ名とパスワードを関連するクレデンシャル データベースに設定することを推奨します。

プレゼンスの更新に失敗した

デフォルト サブゾーンで [認証ポリシー（Authentication policy）] が [クレデンシャルを確認しない（Do not check credentials）] に設定されている場合、Jabber Video に「プレゼンスの更新に失敗しました（Failed to update Presence）」というメッセージが表示されます。

- デフォルト サブゾーンの認証を [クレデンシャルを確認する（Check credentials）] に設定し、適切なユーザ名とパスワードを関連するクレデンシャル データベースに設定することを推奨します。

付録 2：追加情報

デバイス認証ポートのリファレンス

H.350 ディレクトリ サービス

次の表に、VCS と H.350 サーバ間でデバイス認証に使用されるポートを示します。これらのポートは、[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [H.350 ディレクトリ サービス（H.350 directory service）] から設定できます。

目的	VCS ポート	接続先ポート
H.350 LDAP サーバ	TCP の一時的なポート	TCP/389 または TCP/636

Active Directory（直接）

次の表に、VCS と AD システム間でデバイス認証に使用されるポートを示します。これらのポートは、[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）] から設定できます。

目的	VCS ポート	接続先ポート
Kerberos キー発行局	UDP の一時的なポート	88 UDP
Kerberos	TCP の一時的なポート	88 TCP
ドメイン コントローラ（CLDAP）を備えた VCS	UDP の一時的なポート	389 UDP
ドメイン コントローラ（LDAP）を備えた VCS	TCP の一時的なポート	389 / 636 TCP
ドメイン コントローラ（Microsoft-DS）を使用したクライアント クレデンシャル認証。VCS は最初にポート 445 を試しますが、到達できない場合はポート 139 を試します。	TCP の一時的なポート	445 / 139 TCP

TLS の証明書

TLS 経由でサーバに接続する VCS の場合、VCS にインストールされた信頼できる CA 証明書で、サーバのサーバ証明書を承認できる必要があります。

詳細については、『*VCS を使用した証明書の作成と利用の導入ガイド（Certificate Creation and Use with VCS Deployment Guide）*』を参照してください。

VCS クラスタでの使用

Active Directory（直接）

すべての認証設定はクラスタ ピア間で複製されますが、DNS サーバは VCS ピアごとに独立して設定できます。各ピアが DNS サーバを参照し、AD サーバや Kerberos KDC などの必要な DNS アドレスと DNS SRV アドレスを検索できることを確認してください。

各ピアは AD サーバに個別に接続しているので、ドメインに対する参加または離脱は、クラスタのすべてのピアに対して実行される必要があります。

IT の要求書

H.350 ディレクトリ サービス：IT の要求書（H.350 ディレクトリ サービスへの LDAP アクセスの場合）

宛先：IT 部門

次の詳細情報についてご記入ください。ビデオ エンドポイント コールを認証する際に H.350 ディレクトリ サービス サーバへの LDAP アクセスを使用するために必要な VCS の設定項目です。

LDAP サーバ IP またはドメイン	
LDAP アクセス用の IP ポート	389 / 636 /その他：
暗号化（Encryption）	[オフ（Off）] / [TLS]
H.350 LDAP サーバにバインドするときに使用されるユーザ名の識別名（例：uid=、ou=）	
H.350 LDAP サーバにバインドするときに使用するパスワード	
H.350 LDAP サーバに接続するときに使用する識別名（例：ou=、dc=）	

Active Directory（直接）：IT の要求書（Active Directory サーバへのアクセスの場合）

宛先：IT 部門

次の詳細情報についてご記入ください。ビデオ エンドポイント コールを認証する際に Active Directory サーバへアクセスするために必要な VCS の設定項目です。

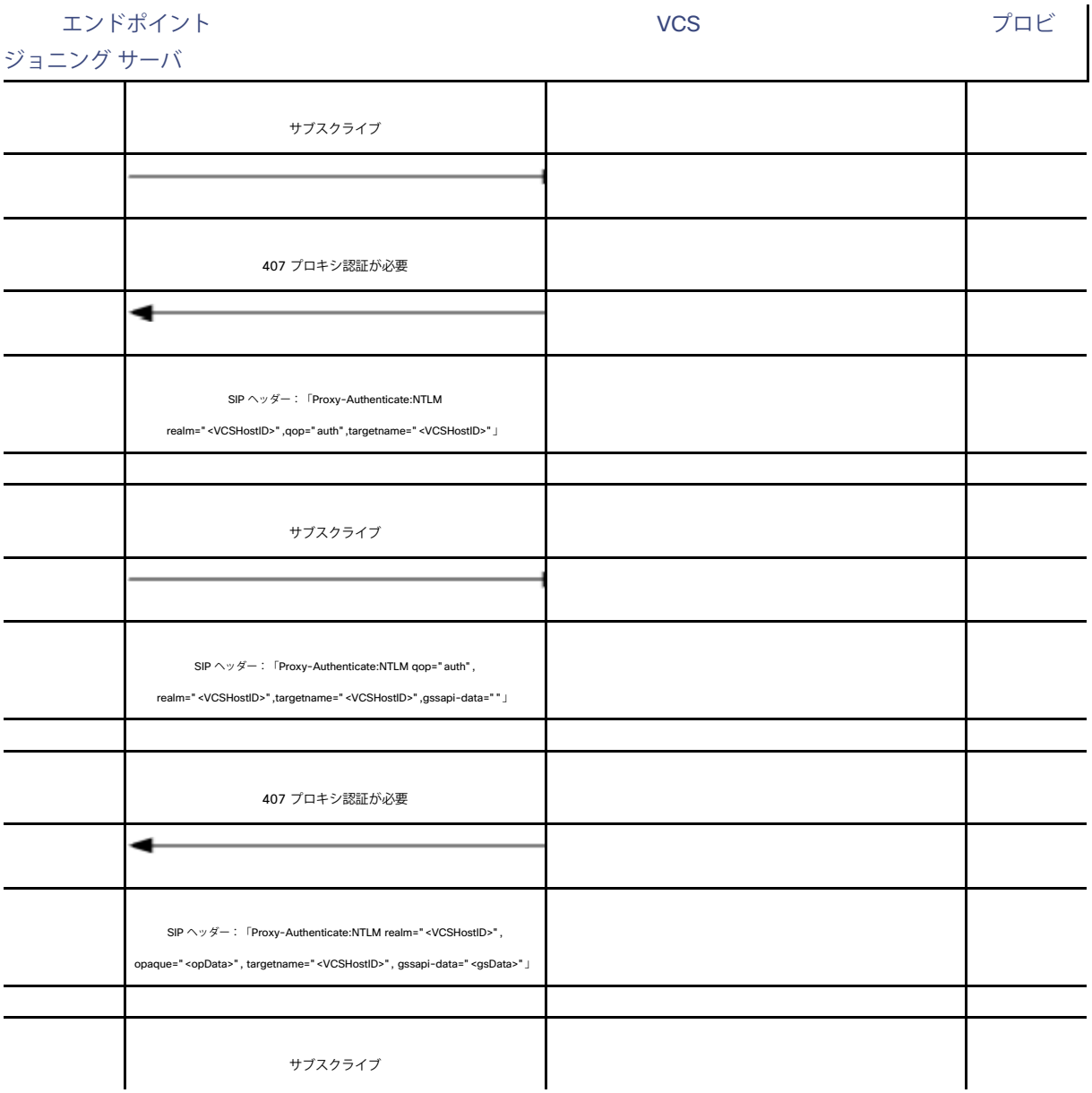
Active Directory ドメイン（FQDN）	
Active Directory の短いドメイン名（NetBIOS ドメイン名）	
VCS と AD ドメイン コントローラの間にセキュア チャネルは必要か	はい/いいえ
VCS と AD サーバの間に TLS 暗号化は必要か 証明書の場所はどこか	はい/いいえ 証明書ファイルへのパス：
VCS と Kerberos キー発行局の間に 300（5 分）以外のクロック スキュー値は必要か	300（デフォルト）/その他
VCS と AD ドメイン コントローラの間で適切な認証プロトコルを特定するために、SPNEGO（Simple and Protected GSSAPI Negotiation Mechanism）が使用されるか	はい/いいえ
ドメイン コントローラ サーバ これらは、以下に対する DNS SRV ルックアップで使用できるか **_ldap._tcp.dc._msdcs.<Domain>** できない場合は、DC サーバの IP を指定してください。	はい/いいえ 1. 2. 3. 4. 5.
Kerberos キー発行局サーバ これらは、以下に対する DNS SRV ルックアップで使用できるか **_kerberos._udp.<Domain>** および **_kerberos._tcp.<Domain>** できない場合は、KDC サーバの IP を指定してください。	はい/いいえ 1. 2. 3. 4. 5.
管理者ユーザ名（VCS をドメインに参加させるために使用）	
管理者パスワード（VCS をドメインに参加させるために使用）	

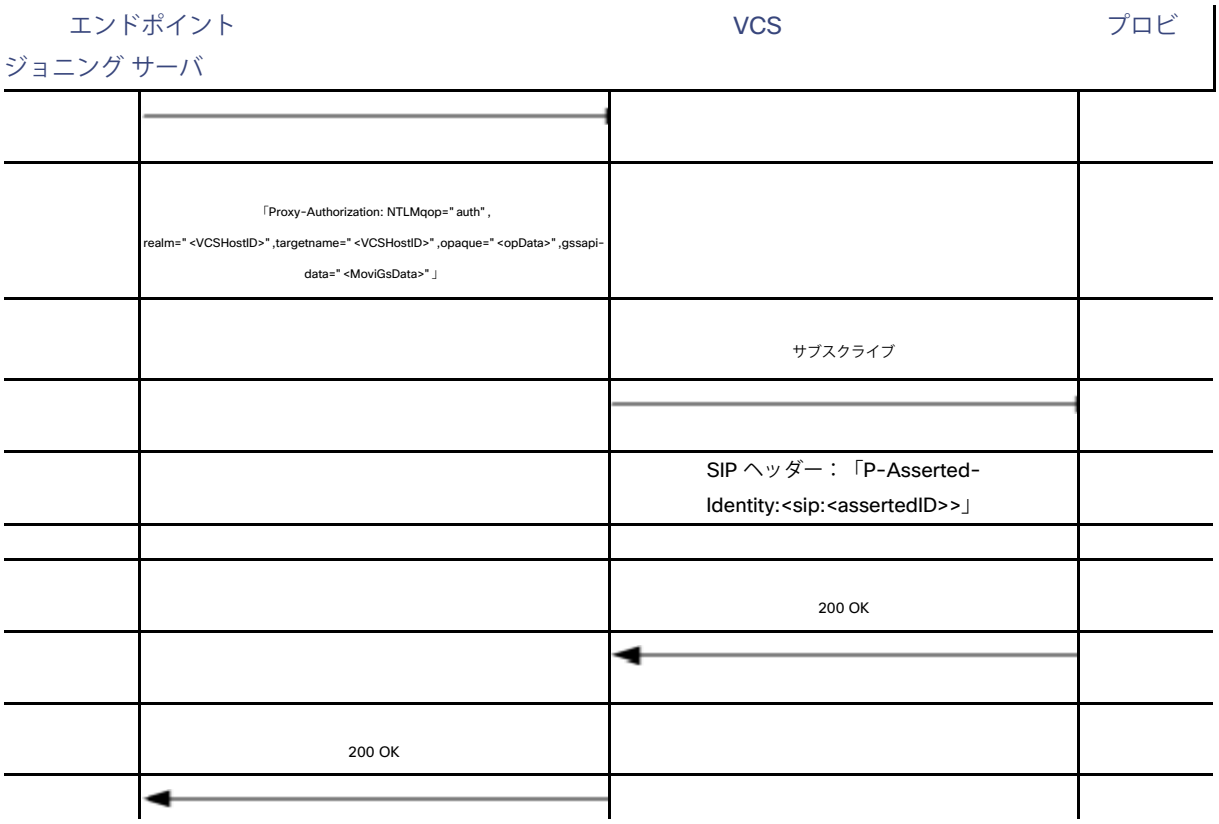
付録 3：Active Directory（直接）

プロビジョニング サブスクリプション用の SIP メッセージ

次のラダー図に、NTLM（Active Directory 直接）を使用して認証がチャレンジされる場合の SIP メッセージングのコール フローを示します。

プロビジョニング サーバは、メッセージングを認証する VCS 上に常駐することもできます。その場合、シグナリングの宛先は、127.0.0.1 になります。あるいは、プロビジョニング サーバが常駐しているのとは別の VCS にメッセージを送信することもできます（たとえば、VCS Expressway から VCS Control）。





AD 用の DNS SRV の設定例

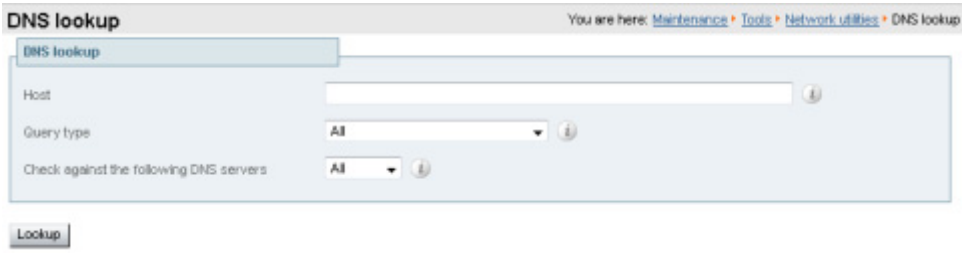
想定される DNS SRV の値

VCS では、以下の DNS SRV レコードが検出されると想定されています。AD サーバが DNS サーバにアクセス可能な場合、DNS SRV レコードは AD サーバによって自動的にセットアップされます。

SRV 検索	コメント
_ldap._tcp.dc._msdcs.<Domain>	ドメインのドメイン コントローラのアドレスを提供します。
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.<Domain>	最初のサイト名を提供します。
_kerberos._udp.<Domain>	UDP 経由でアクセスするための KDC サーバ アドレスを指定します。 このエントリには、各 KDC のポート 88 を含める必要があります。
_kerberos._tcp.<Domain>	TCP 経由でアクセスするための KDC サーバ アドレスを指定します。 このエントリには、各 KDC のポート 88 を含める必要があります。
_ldap._tcp.<Domain>	ドメイン コントローラ上の LDAP サービスを指定します。 このレコードには、DC のポート 389 を含める必要があります。

DNS SRV の設定の確認

1. [メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [DNS ルックアップ（DNS lookup）] に移動します。
2. [ホスト（Host）] フィールドに SRV のパスを入力します。
3. [ルックアップ（Lookup）] をクリックします。



DNS SRV の設定の確認（Dig コマンド）

次のコマンドを実行して、正しい DNS エントリが存在することを確認できます。

```
root#  dig <DNS server> -t any <full dnssrv record, e.g. _ldap._tcp.dc._msdcs.<DOMAIN>>
```

応答の例：

```
 ; <<>> DiG 9.4.1 <<>> <DNS server> -t any <full dnssrv record> ;; global options:  printcmd ;; Got
answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44952 ;; flags: qr aa rd ra; QUERY: 1, ANSWER:
2, AUTHORITY: 0, ADDITIONAL: 2  ;; QUESTION SECTION: ; <full dnssrv record>.       IN      ANY  ;; ANSWER
SECTION: <full dnssrv record>. 600     IN      SRV     0 100 389 <A record 1>.
 <full dnssrv record>.600     IN      SRV     1 100 389 <A record 2>.

 ;; ADDITIONAL SECTION: <A record 1>.        3600     IN      A       <IP address 1> <A record
1>.        1200     IN      A       <IP address 2>  ;; Query time: 0 msec ;; SERVER: <DNS
server>#53(10.1.1.16) ;; WHEN: Mon Jul 26 11:09:59 2010 ;; MSG SIZE  rcvd: 171 ~ #
```

Jabber Video PC および AD サーバの互換性の設定

Jabber Video および AD サーバの LmCompatibilityLevel

LmCompatibilityLevel は、クライアント（Jabber Video PC など）と、Active Directory サーバをホストしているドメイン コントローラの両方で設定されます。Jabber Video PC で選択される値は、AD データベース ドメイン コントローラに設定されている値と適合している必要があります。

LmCompatibilityLevel の値の意味については、http://technet.microsoft.com/en-us/library/cc960646.aspx [英語] に説明されています。ここでは要約を示します。

Jabber Video クライアント PC

水準器	クライアントから送信： LM	NTLM	NTLM 2	NTLM2 セキュリティ（ネゴシエートされる場合）
[0]	✓	✓	-	-
1	✓	✓	-	✓
2	-	✓	-	✓
3	-	-	✓	✓
4	-	-	✓	✓
5	-	-	✓	✓

AD ドメイン コントローラ

水準器	DC で受け入れ： LM	NTLM	NTLM 2
[0]	✓	✓	✓
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	-	✓	✓
5	-	-	✓

適合性

AD ドメイン コントローラのレベル	Jabber Video クライアント PC
0、1、2、3、4	0、1、2、3、4、5
5	3、4、5

「LmCompatibilityLevel」と呼ばれる設定は、Windows レジストリ内にあります。

regedit を使用して、My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa を参照します

このキーが LmCompatibilityLevel（REG_DWORD）と呼ばれています

NtlmMinClientSec とセッション セキュリティ レベル

Microsoft は、NTLM v2 でさまざまなバージョンのセッション セキュリティをサポートしています。

拡張されたセッション セキュリティは、X7.1 よりも前の VCS ではサポートされていません。そのため、X7.1 よりも前の VCS バージョンを使用しているときにクライアントで選択されると、認証が失敗します。

セッション セキュリティ レベルは、次のレジストリ キーで制御されます。

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA\MSV1_0\NtlmMinClientSec
```

X7.1 よりも前の VCS では、NtlmMinClientSec が命令「NTLM 2 session security」に設定されると、Jabber Video の認証が失敗します。

VCS ソフトウェア X7.1 以降での使用が推奨されるクライアント設定：

```
LmCompatibilitylevel set to 3, 4 or 5 NtlmMinClientSec set to 0x20080000
```

前述の設定では、Jabber Video クライアントが、128 ビットで暗号化された NTLM 2 セッション セキュリティによる NTLMv2 を使用します。

Microsoft からの情報：

```
   Value: NtlmMinClientSec    Value Type: REG_DWORD - Number    Valid Range: the logical 'or' of any of the
following values:       0x00000010       0x00000020       0x00080000       0x20000000    Default:
0     Value: NtlmMinServerSec    Value Type: REG_DWORD - Number    Valid Range: same as
NtlmMinClientSec    Default: 0    Description: This parameter specifies the minimum security to be used.
       0x00000010  Message integrity       0x00000020  Message confidentiality       0x00080000  NTLMv2
session security       0x20000000  128 bit encryption
```

ドメイン情報および VCS のステータスの確認

この付録では、AD ドメインへの VCS の接続のステータスを確認するために使用できるコマンドについて説明します。クラスタ化された VCS システムでは、各ピアを別々に確認する必要があります。

domain_management

1. SSH またはシリアル インターフェイス経由で root としてログインします。
2. 次のコマンドを入力します。

   ```
   domain_management
   ```

   次のオプションが表示されます。

   ```
   ----------------------------------1) Join Domain2) Leave Domain3) VCS Status4) Domain Information5)
   Exit----------------------------------
   ```

3. `4) Domain Information` オプションを選択します。

   VCS から次の情報が報告されます。

   ```
   LDAP server: <IP of AD server>LDAP server name: <AD server name>Realm: <AD DOMAIN (FQDN)>Bind Path:
   dc= .. dc= … (representing <DOMAIN>)LDAP port: <port, e.g. 389>Server time: <Time>KDC server: <IP of
   KDC server>Server time offset: <offset between AD server and VCS>Domain information request succeeded
   ```

4. `3) VCS Status` オプションを選択します。
5. 要求に応じて、ドメイン管理者のユーザ名を入力します。
6. 要求に応じて、ドメイン管理者のパスワードを入力します（大文字と小文字が区別されます）。

   VCS から次の情報が報告されます。

   ```
   … <lots of details> …Domain status request succeeded
   ```

ドメイン管理者のユーザ名とパスワードは VCS に保存されないことに注意してください。それらは、AD ドメインへの参加操作、AD ドメインからの離脱操作、および VCS ステータス操作でのみ使用されます。

Net Ads Info

1. SSH またはシリアル インターフェイス経由で root としてログインします。
2. 次のコマンドを入力します。

   ```
   net ads info
   ```

   VCS から次の情報が報告されます。

   ```
   LDAP server: <IP of AD server>
   LDAP server name: <AD server name>
   Realm: <AD DOMAIN (FQDN)>
   Bind Path: dc= .. dc= … (representing <DOMAIN>)
   LDAP port: <port, e.g. 389>
   Server time: <Time>
   KDC server: <IP of KDC server>
   Server time offset: <offset between AD server and VCS>

   Domain information request succeeded
   ```

   これは、domain_management のオプション 4) と同じ情報です。

Net Ads Testjoin

1. SSH またはシリアル インターフェイス経由で root としてログインします。
2. 次のコマンドを入力します。

   net ads testjoin

   VCS から次の情報が報告されます。

   [<Date, Time>] <success or failure logs>Join to domain <success or failure>

   失敗した場合、次の理由が表示されることがあります。

   Preauthentication failed

   これを解決するには、Web インターフェイス上でユーザ名とパスワードを再入力して、[保存（Save）] をクリックします。
   ユーザ名とパスワードを設定可能にするために、Web ページ上の他のフィールドを編集する必要がある場合があります。その場合は、編集したフィールドを必要な値に戻してから、[保存（Save）] をクリックします）。

ドメインからの離脱

注：クラスタの場合、ドメインからの離脱は、ピアごとに実行する必要があります。

VCS を AD ドメインから離脱させるには、以下の手順を実行します。

1. SSH またはシリアル インターフェイス経由で root としてログインします。
2. 次のコマンドを入力します。

   domain_management

   次のオプションが表示されます。

   ```
   ------------------------------------
   1) Join Domain
   2) Leave Domain
   3) VCS Status
   4) Domain Information
   5) Exit
   ------------------------------------
   ```

3. **2 Leave Domain** オプションを選択します。
4. 要求に応じて、ドメイン管理者のユーザ名を入力します。
5. 要求に応じて、ドメイン管理者のパスワードを入力します（大文字と小文字が区別されます）。

   離脱に成功すると、次のメッセージが表示されます。

   Deleted account for '<DNS Local hostname>' in realm '<AD DOMAIN (FQDN)>'…Domain leave succeeded

ドメイン管理者のユーザ名とパスワードは VCS に保存されないことに注意してください。それらは、AD ドメインへの参加操作、AD ドメインからの離脱操作、および VCS ステータス操作でのみ使用されます。

Jabber Video ユーザを AD 直接認証に移行するプロセスの例

Jabber Video ユーザを AD 直接認証に移行するには、以下の手順を実行します。

1. VCS がバージョン X6.1 以降のコードで実行されていることを確認します。
2. すべての Jabber Video クライアントをバージョン 4.2 以降にアップグレードします。

   このアップグレードはプロビジョニングを利用して実行でき、コードの新しいバージョがダウンロード可能になったことがユーザに通知されます。詳細については、『*Cisco Jabber Video for Telepresence 管理者ガイド（Cisco Jabber Video for Telepresence Administrator Guide）*』を参照してください。
3. すべてのユーザに Jabber Video のアップグレードを求める電子メールを送信します。

   ログイン パスワードがユーザの AD パスワードに間もなく変更されること、および Jabber Video の [ユーザ名（Username）] を「<AD Short Domain Name>\username」の形式に更新する必要があることを説明します。

   - 既存のユーザ名は、AD ユーザ名と同じでなければなりません。そうでない場合、認証された名前はプロビジョニング データ ユーザ名と一致しません。
   - ユーザ名は 20 文字以下でなければなりません（Active Directory の制限）。

   定められた期日以降は、アップグレードしないと Jabber Video にサインインできなくなることを説明します。

   Jabber Video for Mac ユーザ向けのメッセージを追加します。「Mac ユーザにはアップグレード プロンプトは表示されません。Mac ユーザは、手動で新しい Jabber Video コードをダウンロードし、アップグレードする必要があります。」
4. AD 直接認証用の VCS を設定します。ただし、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] は [オフ（Off）] に設定します。
5. 切り替えの準備が整ったら、VCS 上で次の作業を実行します。

   1.VCS のデフォルト ゾーン、およびデフォルト サブゾーン（または関連するサブゾーン）上で、[クレデンシャルを確認する（Check Credentials）] を設定します。

   2.[NTLM プロトコル チャレンジ（NTLM protocol challenges）] を [自動（Auto）] に設定します。
6. 古い Jabber Video と古いパスワードが機能しなくなること、Jabber Video 4.2 以降と AD パスワードを使用する必要があること、および Jabber Video の [ユーザ名（Username）] を「<AD Short Domain Name>\username」の形式で設定する必要があることを伝えるリマインダ メールをユーザに送信します。

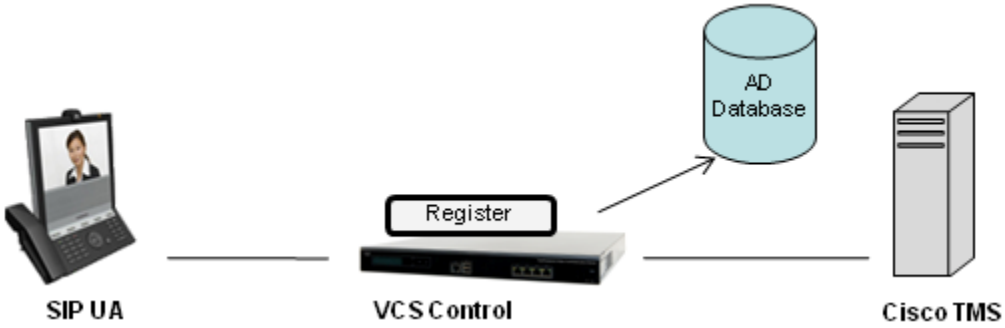
AD 直接認証の導入例

認証を有効にする場合、複数の設定アーキテクチャを検討することができます。

- VCS Control、Active Directory（直接）認証を使用
- VCS Control と VCS Expressway、それぞれで Active Directory（直接）認証を使用
- VCS Control と VCS Expressway、VCS Control に委任された Active Directory（直接）認証を使用

VCS Control、Active Directory（直接）認証を使用

SIP UA が VCS Control に要求を送信し、VCS Control が認証をチャレンジし、認証の詳細を検証用に AD サーバへ送信します。

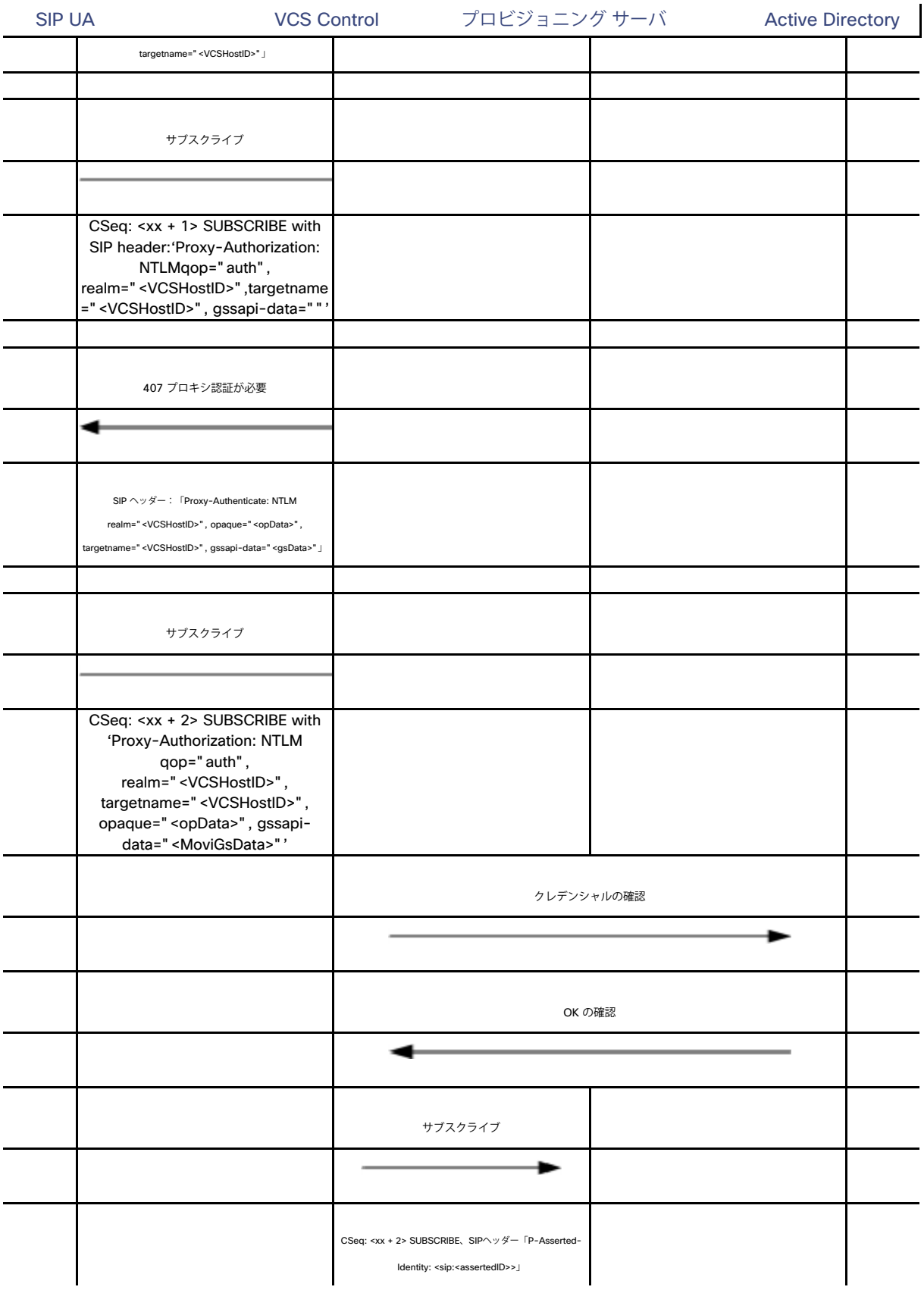


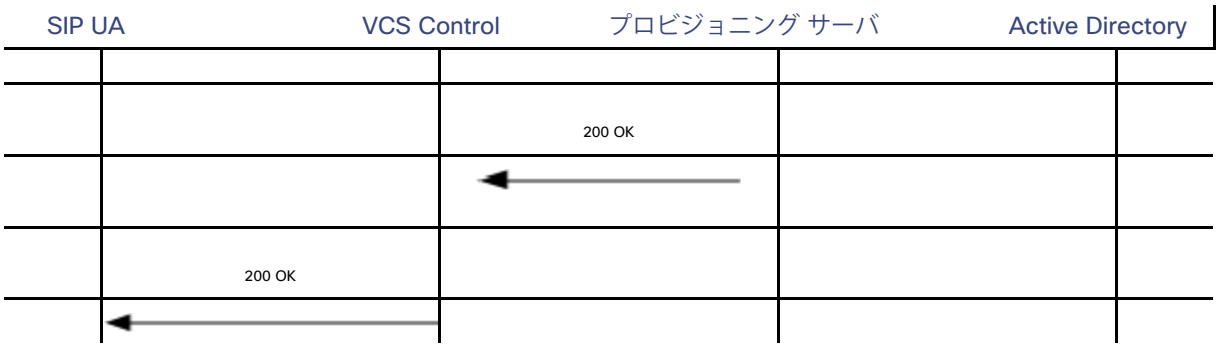
設定	VCS Control
プロビジョニング	✓
AD の設定	✓
デフォルト ゾーン	クレデンシャルを確認する
デフォルト サブゾーン	クレデンシャルを確認する
SIP ドメイン	SIP アカウントのドメイン

設定	Cisco TMS
SIP サーバ	VCS Control の IP アドレスまたは FQDN

次のコール フロー図の例は、AD（直接）認証を使用してチャレンジされるプロビジョニング用のサブスクライブを示しています。

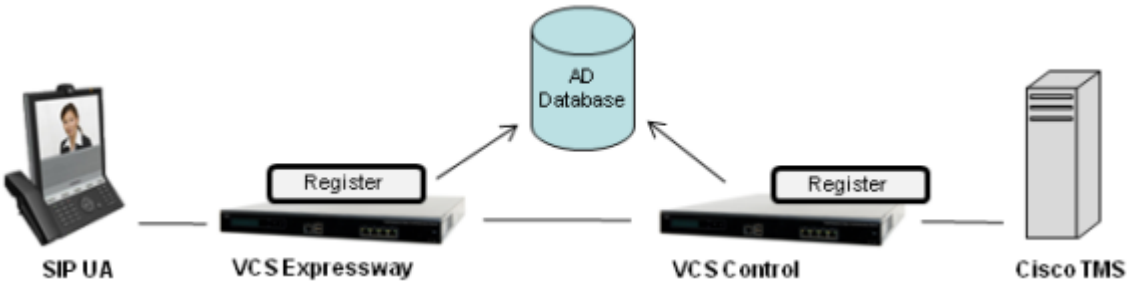
SIP UA	VCS Control	プロビジョニング サーバ	Active Directory
	サブスクライブ		
	CSeq: <xx> SUBSCRIBE		
	407 プロキシ認証が必要		
	SIP ヘッダー：「Proxy-Authenticate: NTLM realm="<VCSHostID>", qop="auth",		


SIP UA
VCS Control
プロビジョニング サーバ
Active Directory
targetname=" <VCSHostID>" 」
サブスクライブ
CSeq: <xx + 1> SUBSCRIBE with SIP header:‘Proxy-Authorization: NTLMqop=" auth" , realm=" <VCSHostID>" ,targetname =" <VCSHostID>" , gssapi-data=" " ’
407 プロキシ認証が必要
SIP ヘッダー：「Proxy-Authenticate: NTLM realm=" <VCSHostID>" , opaque=" <opData>" , targetname=" <VCSHostID>" , gssapi-data=" <gsData>" 」
サブスクライブ
CSeq: <xx + 2> SUBSCRIBE with ‘Proxy-Authorization: NTLM qop=" auth" , realm=" <VCSHostID>" , targetname=" <VCSHostID>" , opaque=" <opData>" , gssapi-data=" <MoviGsData>" ’
クレデンシャルの確認
OK の確認
サブスクライブ
CSeq: <xx + 2> SUBSCRIBE、SIPヘッダー「P-Asserted-Identity: <sip:<assertedID>>」



VCS Control と VCS Expressway、それぞれで Active Directory（直接）認証を使用

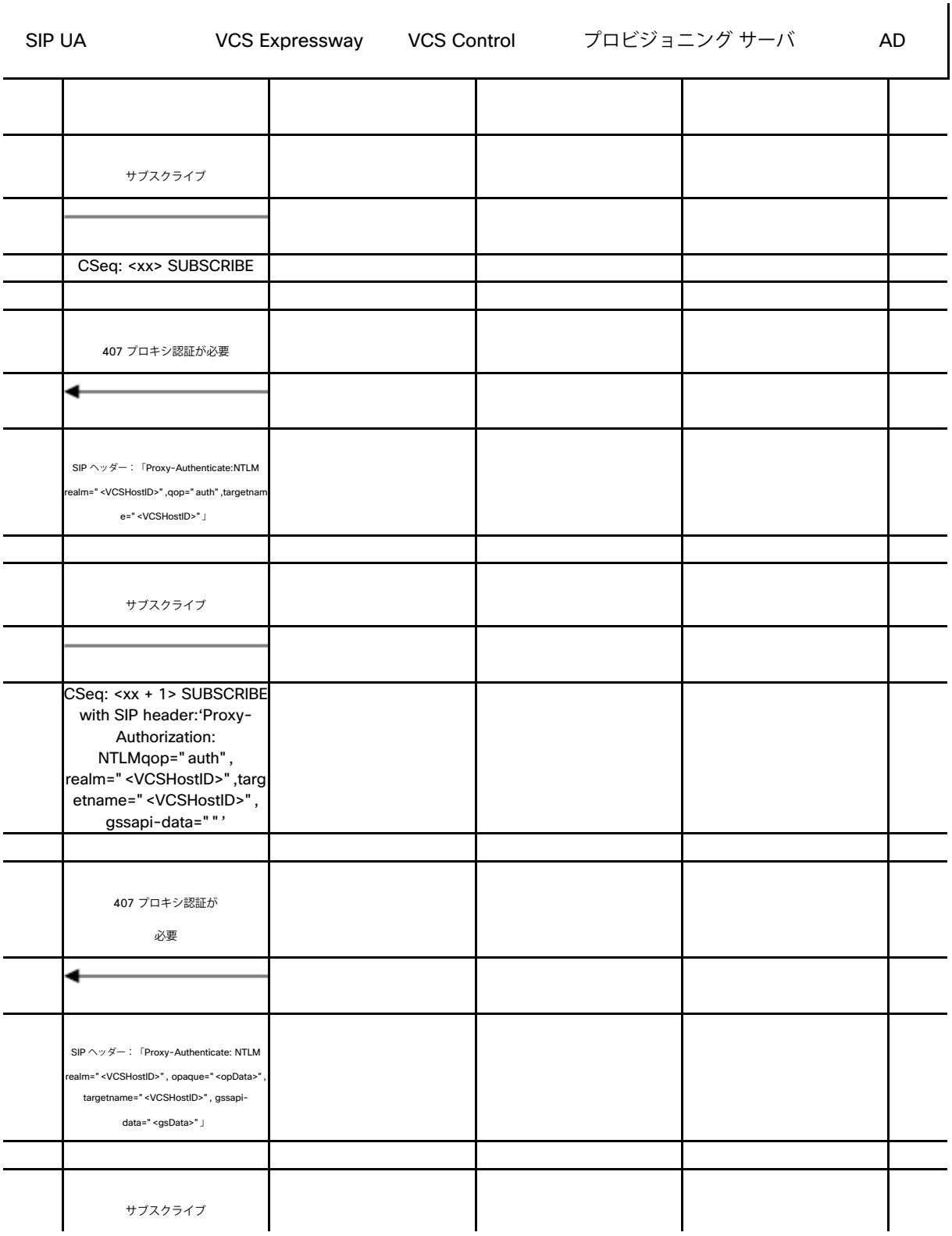
VCS Expressway と VCS Control の両方を、AD サーバに対して直接認証を実行するように設定できます。

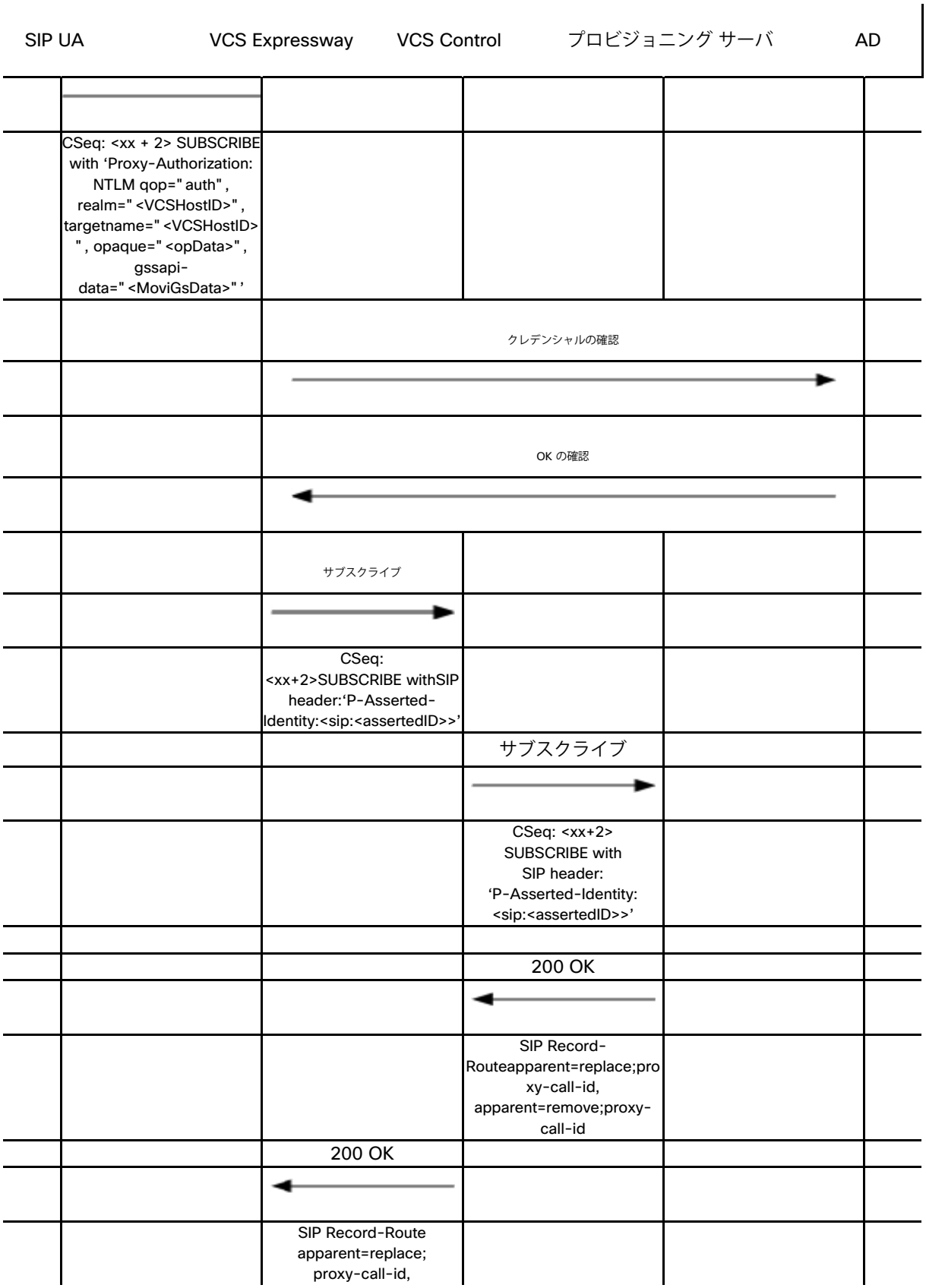


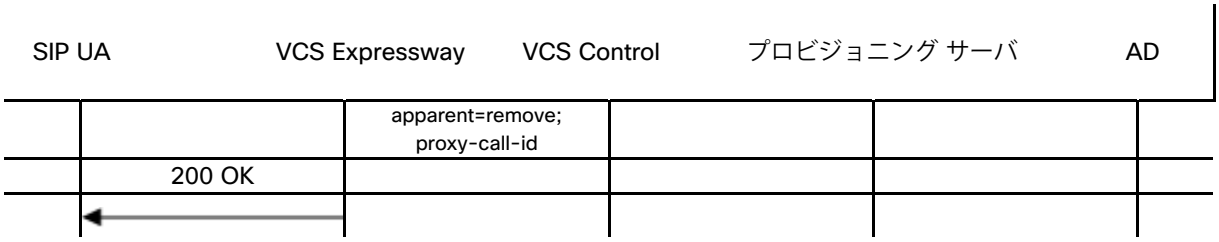
設定	VCS Expressway	VCS Control
プロビジョニング	X	✓
AD の設定	✓	✓
デフォルト ゾーン	クレデンシャルを確認する	クレデンシャルを確認する
デフォルト サブゾーン	クレデンシャルを確認する	クレデンシャルを確認する
トラバーサル ゾーン	クレデンシャルを確認する	クレデンシャルを確認する
SIP ドメイン	SIP アカウントのドメイン	SIP アカウントのドメイン
SIP 登録プロキシ モード	オフ	オフ

設定	Cisco TMS
SIP サーバ	VCS Control の IP アドレスまたは FQDN
パブリック SIP サーバ	VCS Expressway の IP アドレスまたは FQDN

次に、VCS Expressway によって AD（直接）認証チャレンジを使用してチャレンジされるプロビジョニング用サブスクライブの例を示します。認証後は VCS Control 経由でプロビジョニング サーバへ渡されます。




SIP UA
VCS Expressway
VCS Control
プロビジョニング サーバ
AD
CSeq: <xx + 2> SUBSCRIBE with 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", opaque="<opData>", gssapi-data="<MoviGsData>"'
クレデンシャルの確認
OK の確認
サブスクライブ
CSeq: <xx+2>SUBSCRIBE withSIP header:'P-Asserted-Identity:<sip:<assertedID>>'
サブスクライブ
CSeq: <xx+2> SUBSCRIBE with SIP header: 'P-Asserted-Identity: <sip:<assertedID>>'
200 OK
SIP Record-Routeapparent=replace;proxy-call-id, apparent=remove;proxy-call-id
200 OK
SIP Record-Route apparent=replace; proxy-call-id,



VCS Expressway、VCS Control に委任された Active Directory（直接）認証を使用

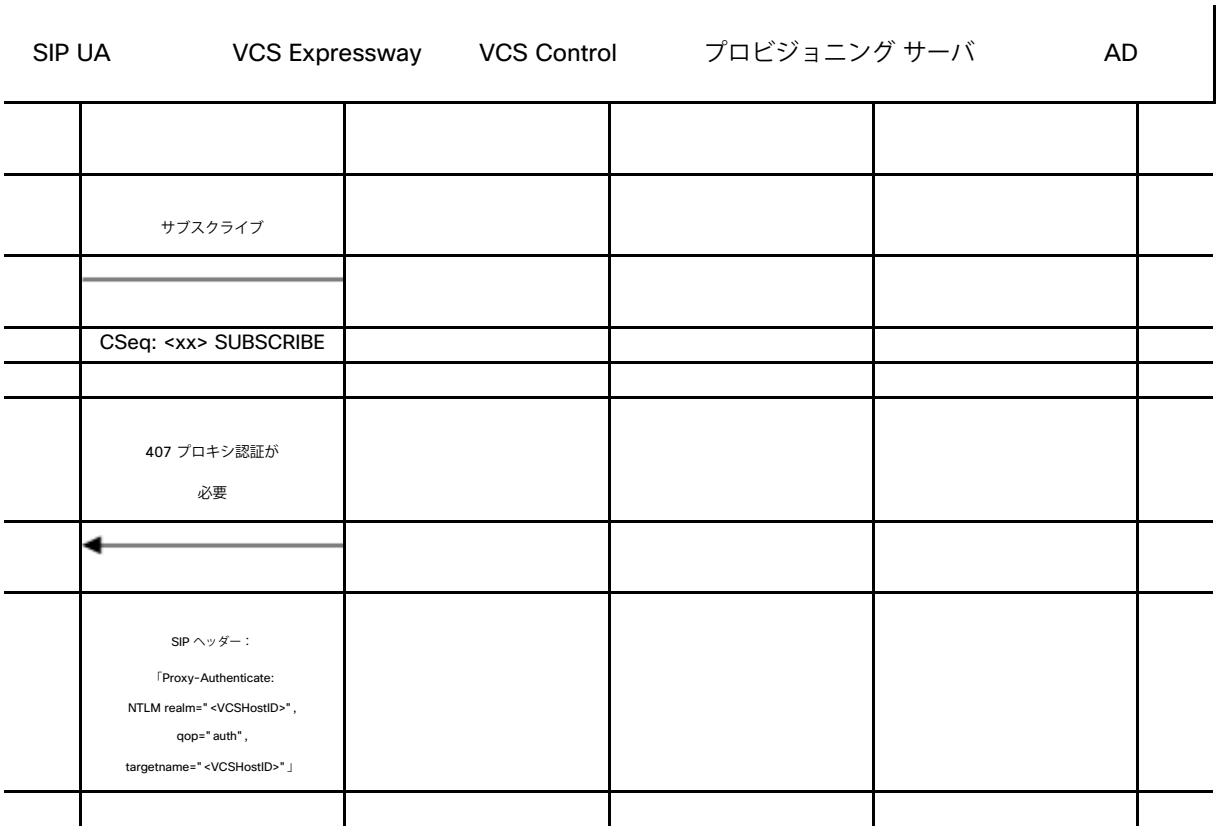
VCS Expressway を AD サーバに直接接続できない場合は、VCS Control に認証を委任できます。

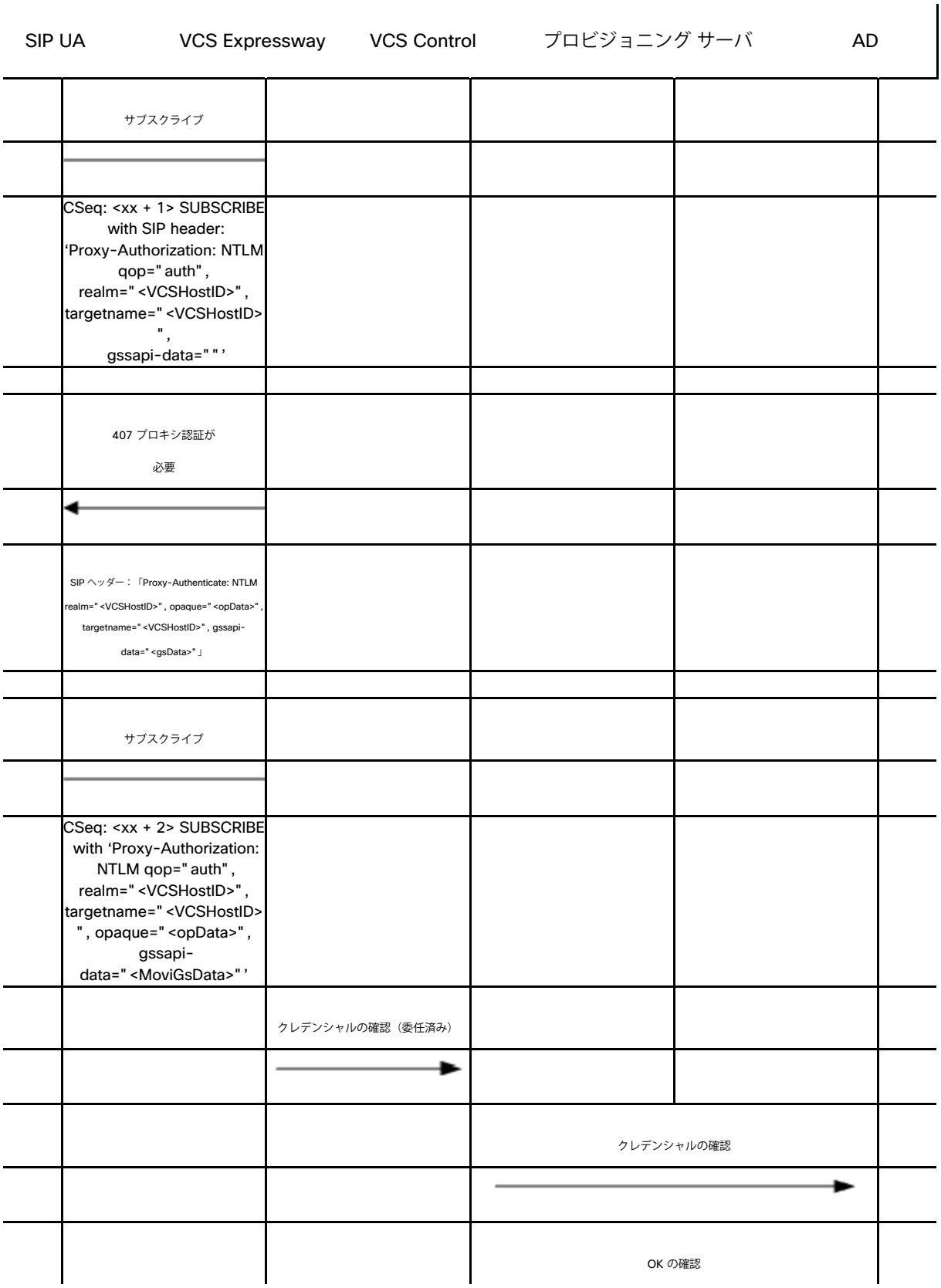
- SIP UA が VCS Expressway に要求を送信し、VCS Expressway が認証をチャレンジします。
- VCS Expressway が SIP UA のクレデンシャルのチェックを VCS Control に委任し、トラバーサル ゾーン経由で認証の詳細を VCS Control に渡します。
- VCS Control が認証の詳細を検証のために AD サーバに送信し、結果を VCS Expressway に戻します。
- 認証された登録は VCS Expressway で行われ、VCS Control にプロキシする必要はありません。このため、どちらも VCS Expressway に登録されている SIP UA 間でのコール時にメディアがファイアウォールを通過する必要がなくなります。

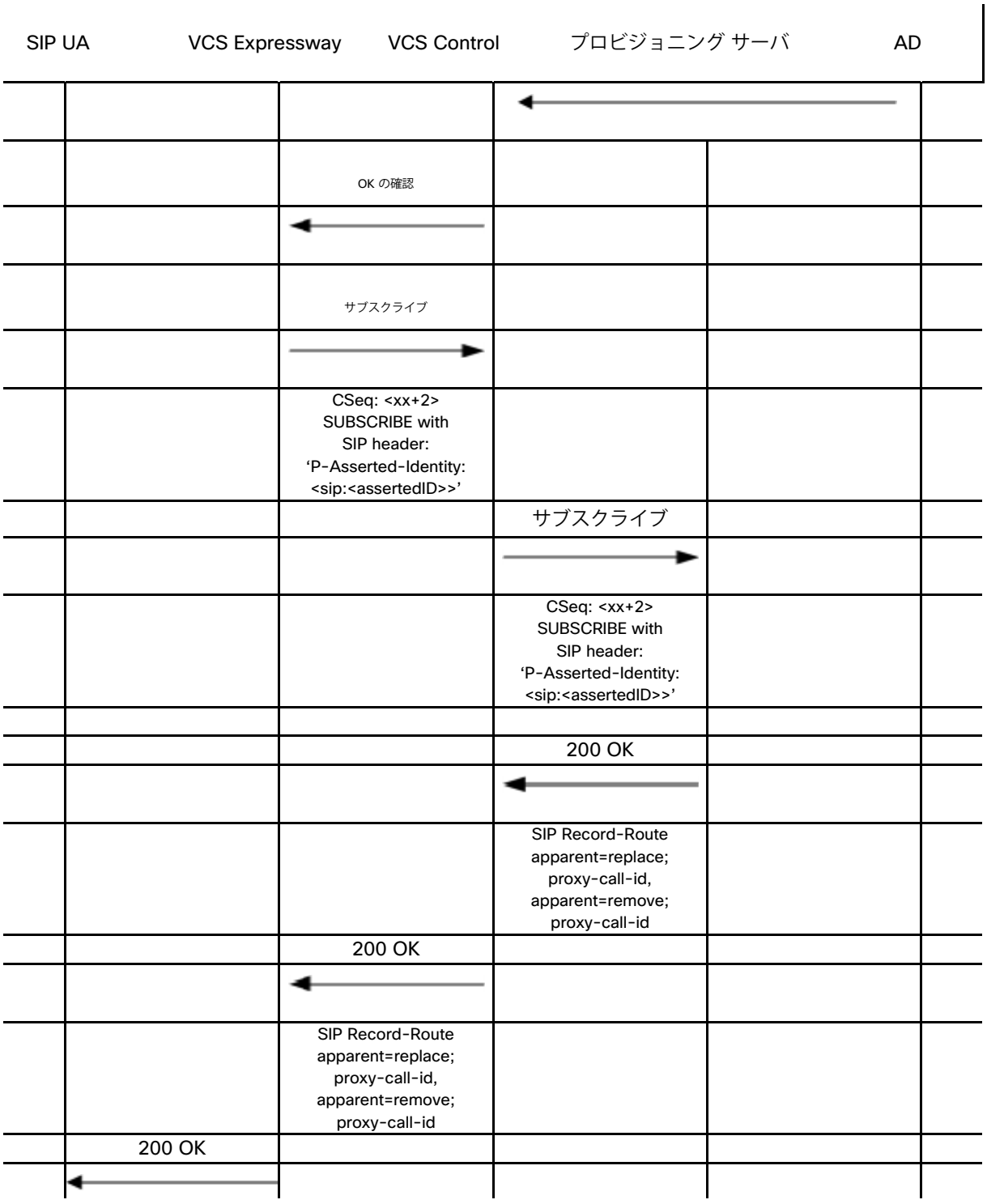
設定	VCS Expressway	VCS Control
プロビジョニング	X	✓
AD の設定	X	✓
デフォルト ゾーン	クレデンシャルを確認する	クレデンシャルを確認する
デフォルト サブゾーン	クレデンシャルを確認する	クレデンシャルを確認する
トラバーサル ゾーン	クレデンシャルを確認する	クレデンシャルを確認する
SIP ドメイン	SIP アカウントのドメイン	SIP アカウントのドメイン
SIP 登録プロキシ モード	オフ	オフ
SIP の委任クレデンシャル チェック	オン	オン

設定	Cisco TMS
SIP サーバ	VCS Control の IP アドレスまたは FQDN
パブリック SIP サーバ	VCS Expressway の IP アドレスまたは FQDN

次に、VCS Expressway によって AD（直接）認証チャレンジを使用してチャレンジされるプロビジョニング用サブスクライブの例を示します。クレデンシャル チェックは VCS Control に委任されます。その後、認証された要求が VCS Control に転送されてからプロビジョニング サーバに渡されます。




SIP UA
VCS Expressway
VCS Control
プロビジョニング サーバ
AD
サブスクライブ
CSeq: <xx + 1> SUBSCRIBE with SIP header: 'Proxy-Authorization: NTLM qop=" auth" , realm=" <VCSHostID>" , targetname=" <VCSHostID> " , gssapi-data=" "'
407 プロキシ認証が必要
SIP ヘッダー:「Proxy-Authenticate: NTLM realm=" <VCSHostID>" , opaque=" <opData>" , targetname=" <VCSHostID>" , gssapi-data=" <gsData>" 」
サブスクライブ
CSeq: <xx + 2> SUBSCRIBE with 'Proxy-Authorization: NTLM qop=" auth" , realm=" <VCSHostID>" , targetname=" <VCSHostID> " , opaque=" <opData>" , gssapi-data=" <MoviGsData>" '
クレデンシャルの確認（委任済み）
クレデンシャルの確認
OK の確認


SIP UA
VCS Expressway
VCS Control
プロビジョニング サーバ
AD
OK の確認
サブスクライブ
CSeq: <xx+2>
SUBSCRIBE with
SIP header:
‘P-Asserted-Identity:
<sip:<assertedID>>’
サブスクライブ
CSeq: <xx+2>
SUBSCRIBE with
SIP header:
‘P-Asserted-Identity:
<sip:<assertedID>>’
200 OK
SIP Record-Route
apparent=replace;
proxy-call-id,
apparent=remove;
proxy-call-id
200 OK
SIP Record-Route
apparent=replace;
proxy-call-id,
apparent=remove;
proxy-call-id
200 OK

マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

日付	説明
2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。
2014 年 12 月	X8.5 用に再発行。
2014 年 6 月	X8.2 用に再発行。
2013 年 12 月	VCS X8.1 に関する内容を更新。委任クレデンシャル チェックを含む。
2012 年 8 月	VCS X7.2 に関する内容を更新。
2012 年 3 月	VCS X7.1 に関する内容を更新。Cisco TMS Provisioning Extension モードの使用を含む。
2012 年 2 月	認証ポリシーの設定に関する概要情報を追加。
2011 年 11 月	Movi PC 上の NTLM バージョンの確認および設定に関する情報を追加。
2011 年 8 月	VCS X7.0 に関する内容を更新。
2011 年 5 月	初版。

シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices [英語]）をご覧ください。

シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は www.cisco.com/web/JP/trademark_statement.html に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)