CHAPTER 10

VPN 認証の管理

この章では、Cisco AnyConnect Secure Mobility Client を使用してユーザの VPN 認証を管理する方法について説明します。またこの章では、次のテーマおよびタスクについても説明します。

サーバ証明書の確認（Server Certificate Verification）

次の検証は、受信したサーバ証明書に適用されます。

- FQDN を使用して初期検証に失敗すると、セキュア ゲートウェイの FQDN を使用して実行された AnyConnect クライアントからセキュア ゲートウェイへの SSL および IPSec 接続は、名前検証のために FQDN の解決された IP アドレスでセカンダリ サーバ証明書の確認を行いません。
- AnyConnect クライアントからセキュア ゲートウェイへの SSL および IPSec 接続は、サーバ証明書がデジタル署名とキー暗号化の Key Usage 属性を含める必要があります。
- AnyConnect クライアントからセキュア ゲートウェイへの SSL 接続により、サーバ証明書はサーバ認証の Enhanced Key Usage 属性を含める必要があります。
- AnyConnect クライアントからセキュア ゲートウェイへの IPsec 接続により、サーバ証明書はサーバ認証または IKE 中間の Enhanced Key Usage 属性を含める必要があります。

（注） Key Usage を含まないサーバ証明書は、すべての Key Usage に対して無効と見なされ、同様に、Enhanced Key Usage を含まないサーバ証明書は、すべての Enhanced Key Usage に対して無効と見なされることに注意してください。

- AnyConnect のこのリリースでは、AnyConnect クライアントからセキュア ゲートウェイへの IPsec 接続がサーバ証明書の名前検証を実行します。次の規則は、IPSec および SSL の両方の名前検証を目的として適用されます。

- Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name に対してのみ実行されます。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
- Subject Alternative Name 拡張子がない場合、または、あるけれども関連する属性を含んでいない場合、名前検証は、証明書の Subject で見つかった Common Name 属性に対して実行されます。
- 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。この規則に準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

証明書のみの認証の設定

ユーザ名とパスワードを使用して AAA でユーザを認証するか、デジタル証明書で認証するか（または、その両方を使用するか）を指定する必要があります。証明書のみの認証を設定すると、ユーザはデジタル証明書で接続でき、ユーザ ID とパスワードを入力する必要がなくなります。

証明書のみの認証は、接続プロファイルの中で設定できます。この設定をイネーブルにするには、次の手順に従います。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。接続プロファイルを選択し、[編集（Edit）] をクリックします。[AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウが開きます。

ステップ 2　選択されていない場合は、ウィンドウの左ペインにあるナビゲーション ツリーの [基本（Basic）] ノードをクリックします。ウィンドウの右ペインにある [認証（Authentication）] エリアで、[証明書（Certificate）] 方式をイネーブルにします。

ステップ 3　[OK] をクリックします。

ステップ 4　（省略可能）各インターフェイスで SSL 認証に使用する証明書があれば、その証明書を指定できます。特定のインターフェイスに対して証明書を指定しない場合、フォールバック証明書が使用されます。

これを実行するには、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。右ペインの [アクセス インターフェイス（Access Interfaces）] エリアで、証明書を指定する対象のインターフェイスを選択して、[デバイス証明書（Device Certificate）] をクリックします。

ステップ 5　[デバイス証明書の指定（Specify Device Certificate）] ダイアログで、[デバイス証明書（Device Certificate）] フィールドをクリックして、選択したインターフェイスへの認証接続に使用する証明書を選択するか、[管理（Manage）] をクリックして、その証明書を追加します。

ステップ 6　[OK] をクリックし、変更を適用します。

（注）

- AnyConnect クライアントが認証証明書を検索する証明書ストアを設定するには、「証明書ストアの設定」（P.3-45）を参照してください。Linux および Mac OS X オペレーティング システムに対する証明書制限の設定についても参照できます。

- セキュア ゲートウェイに対してクライアントを認証するために使用される証明書は有効であり、（CA によって署名された）信頼できるものである必要があります。自己署名されたクライアント証明書は受け入れられません。

AnyConnect のスマート カード サポート

AnyConnect は、次の環境でスマート カードをサポートします。

- Windows XP、7、および Vista 上の Microsoft CAPI 1.0 および CAPI 2.0
- Mac OS X（10.4 以降）でトークンされたキーチェーン

（注） AnyConnect は、Linux または PKCS #11 デバイスではスマート カードをサポートしていません。

SHA 2 証明書検証エラーの回避

AnyConnect クライアントは、IPsec/IKEv2 VPN 接続の IKEv2 認証フェーズ中に必要とされるデータのハッシングおよび署名を Windows Cryptographic Service Provider（CSP）に依存しています。CSP が SHA 2 アルゴリズムをサポートしていておらず、ASA が疑似乱数関数（PRF）SHA256、SHA384、SHA512 用に設定されていて、接続プロファイル（tunnel-group）が証明書用、または証明書と AAA 認証用に設定されている場合、証明書認証は失敗します。ユーザは「*Certificate Validation Failure*」というメッセージを受け取ります。

このエラーは、SHA 2 タイプのアルゴリズムをサポートしていない CSP に属する証明書を、Windows で使用した場合のみ発生します。その他のサポート対象 OS では、この問題は発生しません。

この問題を回避するには、ASA の IKEv2 ポリシーで、PRF を **md5** または **sha**（SHA 1）に設定します。

または、次の機能がわかっているネイティブ CSP の証明書 CSP 値を変更します。

- Windows XP の場合：Microsoft Enhanced RSA および AES Cryptographic Provider（Prototype）
- Windows 7 および Vista の場合：Microsoft Enhanced RSA および AES Cryptographic Provider

注意 SmartCards 証明書には、この回避策を使用しないでください。CSP 名は絶対に変更してはいけません。代わりに、SmartCard のプロバイダーに問い合わせて、SHA 2 アルゴリズムをサポートする、更新された CSP を入手してください。

注意 次の回避策は、手順を誤って実行した場合、ユーザ証明書を破損するおそれがあります。証明書で変更を指定するときは、十分に注意してください。

Microsoft Certutil.exe ユーティリティを使用して、証明書 CSP 値を変更できます。Certutil は、Windows CA を管理するためのコマンドライン ユーティリティで、Microsoft Windows Server 2003 Administration Tools Pack に同梱されています。Tools Pack は、次の URL からダウンロードできます。

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Certutil.exe を実行して証明書 CSP 値を変更するには、次の作業を実行します。

ステップ 1　エンドポイント コンピュータでコマンド ウィンドウを開きます。

ステップ 2　次のコマンドを使用して、ユーザ ストアに格納されている証明書と、その証明書の現在の CSP 値を表示します。

```
certutil -store -user My
```

次に、このコマンドで表示される証明書の内容の例を示します。

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

ステップ 3　この証明書の <CN> 属性を特定します。この例では、CN は *Carol Smith* です。この情報は次のステップに必要です。

ステップ 4　次のコマンドを使用して、証明書 CSP を変更します。次に、サブジェクト <CN> 値を使用して、変更する証明書を選択する例を示します。その他の属性も使用できます。

Windows Vista および Windows 7 の場合は、次のコマンドを使用します。

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore
-user My <CN> carol smith
```

Windows XP の場合は、次のコマンドを使用します。

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" -f
-repairstore -user My <CN> carol smith
```

ステップ 5　ステップ 2 を繰り返して、表示される証明書の新しい CSP 値を確認します。

SDI トークン（SoftID）の統合

AnyConnect は、Windows 7 x86（32 ビット版）と x64（64 ビット版）、Vista x86 と x64、および XP x86 で動作する RSA SecurID クライアント ソフトウェア バージョン 1.1 以降のサポートを統合します。

RSA SecurID ソフトウェア オーセンティケータは、企業の資産へのセキュアなアクセスのために必要となる管理項目数を減らします。リモート デバイスに常駐する RSA SecurID Software Token は、1 回限定で使用可能なパスコードを 60 秒ごとにランダムに生成します。SDI は Security Dynamics 社製テクノロジーの略称で、ハードウェアとソフトウェアの両方のトークンを使用する、この 1 回限定利用のパスワード生成テクノロジーを意味します。

RSASecureIDIntegration プロファイル設定は、次の 3 つの値のいずれかになります。

- [自動（Automatic）] : クライアントはまずメソッドを 1 つ試行し、それが失敗したら別のメソッドを試行します。デフォルトでは、ユーザ入力がトークン パスコード（HardwareToken）として処理され、これが失敗したら、ユーザ入力がソフトウェア トークン PIN（SoftwareToken）として処理されます。認証が成功すると、成功したメソッドが新しい SDI トークン タイプとして設定され、ユーザ プリファレンス ファイルにキャッシュされます。SDI トークン タイプは、次回の認証試行でいずれのメソッドが最初に試行されるかを定義します。通常、現行の認証試行には、最後に成功した認証試行で使用されたトークンと同じものが使用されます。ただし、ユーザ名またはグループの選択を変更した場合は、入力フィールド ラベルに示されている、デフォルトのメソッドが最初に試行される状態に戻ります。

（注）　SDI トークン タイプは、設定が自動の場合のみ、意味を持ちます。認証モードが自動以外の場合は、SKI トークン タイプのログを無視できます。HardwareToken がデフォルトの場合、次のトークン モードはトリガーされません。

- SoftwareToken : クライアントは、ユーザ入力を常にソフトウェア トークン PIN として解釈し、入力フィールド ラベルは [PIN :（PIN:）] になります。
- HardwareToken : クライアントは、ユーザ入力を常にトークン パスコードとして解釈し、入力フィールド ラベルは [パスコード :（Passcode:）] になります。

（注）　AnyConnect では、RSA Software Token クライアント ソフトウェアにインポートした複数のトークンからの、トークンの選択はサポートされていません。その代わりに、クライアントは RSA SecurID Software Token GUI を介してデフォルト選択のトークンを使用します。

ネイティブ SDI と RADIUS SDI の比較

ネットワーク管理者は、SDI 認証を可能にするセキュア ゲートウェイを次のいずれかのモードで設定することができます。

- *ネイティブ SDI* : SDI サーバと直接通信して SDI 認証を処理できるセキュア ゲートウェイのネイティブ機能です。
- *RADIUS SDI* : RADIUS SDI プロキシを使用して SDI サーバと通信することで SDI 認証を行うセキュア ゲートウェイのプロセスです。

リリース 2.1 以降では、後述の場合を除いて、リモート ユーザからネイティブ SDI と RADIUS SDI を区別できません。SDI メッセージは SDI サーバ上で設定が可能なため、これには、ASA 上のメッセージ テキスト（(P.10-13) を参照）は、SDI サーバ上のメッセージ テキストに一致する必要があります。一致しないと、リモート クライアント ユーザに表示されるプロンプトが、認証中に必要なアクションとして適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS SDI チャレンジは、少数の例外はありますが、基本的にはミラー ネイティブの SDI 交換です。両者とも最終的には SDI サーバと通信するため、クライアントから必要な情報と要求される情報の順序は同じです。明記した場合を除き、ここでは今後、ネイティブ SDI について説明します。

RADIUS SDI 認証を行うリモート ユーザが AnyConnect で ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信し、次にこのサーバは認証について SDI サーバと通信します。

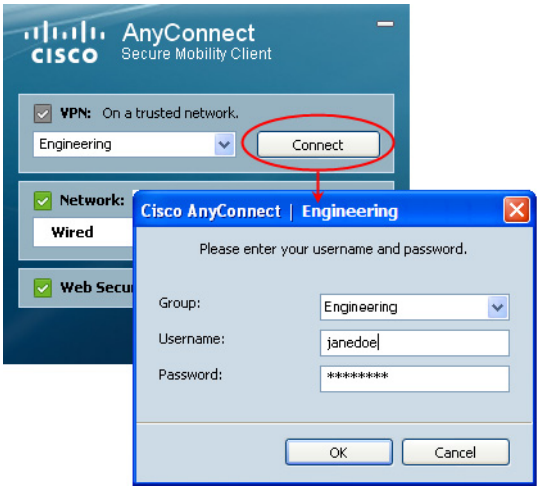
AnyConnect との互換性が保持される ASA 設定の詳細については、「RADIUS/SDI プロキシと AnyConnect との互換性の保持」（P.10-10）を参照してください。

SDI 認証の使用

ログイン（チャレンジ）ダイアログボックスは、ユーザが属するトンネル グループに設定されている認証タイプと一致しています。ログイン ダイアログボックスの入力フィールドには、どのような種類の入力が認証に必要か明確に示されます。

通常、ユーザはツール トレイの [AnyConnect] アイコンをクリックし、接続する接続プロファイルを選択してから、認証ダイアログボックスに適切なクレデンシャルを入力することで AnyConnect に接続します。ユーザ名 / パスワードによる認証を行うユーザには、図 10-1 のようなダイアログボックスが表示されます。

図 10-1　ユーザ名 / パスワードを入力する認証用ログイン ダイアログボックス



SDI 認証では、リモート ユーザは AnyConnect ソフトウェア インターフェイスに個人識別番号（PIN）を入力して RSA SecurID パスコードを受け取ります。セキュアなアプリケーションにパスコードを入力すると、RSA Authentication Manager がこのパスコードを確認してユーザにアクセスを許可します。

RSA SecurID ハードウェアまたはソフトウェアのトークンを使用するユーザには、パスコードまたは PIN、PIN、パスコードのいずれかを入力する入力フィールドが表示されます。ダイアログボックス下部のステータス行には、さらにこの点に関連する情報が表示されます。ユーザは、ソフトウェア トークンの PIN またはパスコードを AnyConnect ユーザ インターフェイスに直接入力します。図 10-2、図 10-3、および図 10-4 を参照してください。

図 10-2　パスコードまたは PIN ダイアログボックス

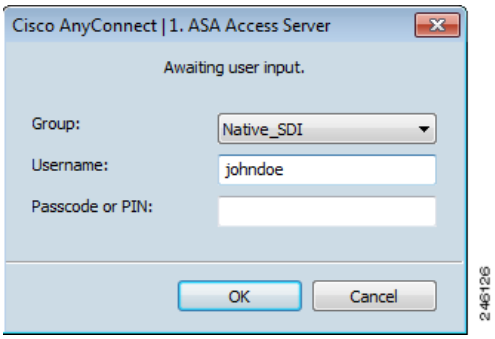


図 10-3　PIN ダイアログボックス

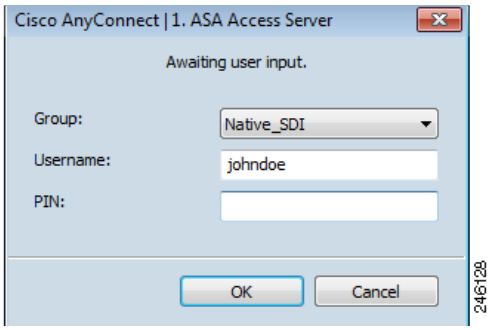
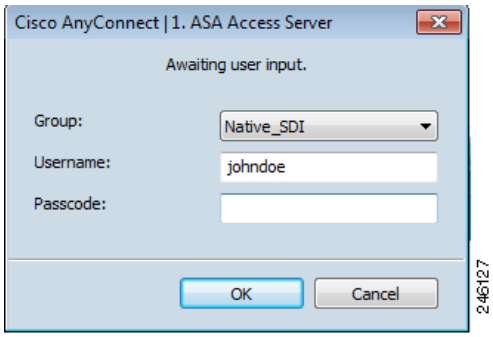


図 10-4　パスコード ダイアログボックス



最初に表示されるログイン ダイアログボックスの外観は、セキュア ゲートウェイの設定によって異なります。セキュア ゲートウェイには、メインのログイン ページ、メインのインデックス URL、トンネル グループのログイン ページ、またはトンネル グループの URL（URL/ トンネル グループ）からアクセスできます。メインのログイン ページからセキュア ゲートウェイにアクセスするには、[ネットワーク（クライアント）アクセス（Network (Client) Access）] の [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] ページで [ユーザに接続の選択を許可する（Allow user to select connection）] チェックボックスをオンにする必要があります。いずれの方法でも、ゲートウェイはクライアントにログイン ページを送信します。メインのログイン ページにはドロップダウン リストがあり、ここからトンネル グループを選択します。トンネルグループ ログイン ページにはこの表示はありません。トンネルグループは URL で指定されるためです。

（接続プロファイルまたはトンネル グループのドロップダウン リストが表示される）メインのログイン ページの場合、デフォルト トンネル グループの認証タイプによって、パスワードの入力フィールド ラベルの初期設定が決まります。たとえば、デフォルト トンネル グループが SDI 認証を使用する場合、フィールド ラベルは [パスコード（Passcode）] になりますが、デフォルト トンネル グループが NTLM 認証を使用する場合は、フィールド ラベルは [パスワード（Password）] になります。リリース 2.1 以降では、異なるトンネル グループをユーザが選択しても、フィールド ラベルが動的に更新されることはありません。トンネルグループのログイン ページでは、フィールド ラベルはトンネルグループの要件に一致します。

クライアントは、パスワード入力フィールドへの RSA SecurID Software Token の PIN の入力をサポートします。RSA SecurID Software Token ソフトウェアがインストールされており、トンネルグループ認証タイプが SDI の場合、フィールド ラベルは [パスコード（Passcode）] となり、ステータス バーに

は、「Enter a username and passcode or software token PIN」と表示されます。PIN を使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [PIN] のフィールドが表示されます。クライアントは、入力された PIN を使用して RSA SecurID Software Token DLL からパスコードを取得します。認証が成功するたびにクライアントはトンネル グループ、ユーザ名、認証タイプを保存し、保存されたトンネル グループが新たにデフォルトのトンネル グループとなります。

AnyConnect では、すべての SDI 認証でパスコードを使用できます。パスワード入力ラベルが [PIN] の場合でも、ユーザはステータス バーの指示どおりにパスコードを入力することができます。クライアントは、セキュア ゲートウェイにパスコードをそのまま送信します。パスコードを使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [パスコード（Passcode）] のフィールドが表示されます。

SDI 認証交換のカテゴリ

すべての SDI 認証交換は次のいずれかのカテゴリに分類されます。

- 通常の SDI 認証ログイン
- 通常ログイン チャレンジ
- 新規ユーザ モード
- 新規 PIN モード
- PIN クリア モード
- 次のトークン コード モード

通常の SDI 認証ログイン

通常ログイン チャレンジは、常に最初のチャレンジです。SDI 認証ユーザは、ユーザ名およびトークン パスコード（ソフトウェア トークンの場合は PIN）を、ユーザ名とパスコードまたは PIN フィールドにそれぞれ指定する必要があります。クライアントはユーザの入力に応じてセキュア ゲートウェイ（中央サイトのデバイス）に情報を返し、セキュア ゲートウェイはこの認証を認証サーバ（SDI または RADIUS プロキシ経由の SDI）で確認します。

認証サーバが認証要求を受け入れた場合、セキュア ゲートウェイは認証が成功したページをクライアントに送信します。これで認証交換が完了します。

パスコードが拒否された場合は認証は失敗し、セキュア ゲートウェイは、エラー メッセージとともに新しいログイン チャレンジ ページを送信します。SDI サーバでパスコード失敗しきい値に達した場合、SDI サーバはトークンを次のトークン コード モードに配置します。「「Next Passcode」および「Next Token Code」チャレンジ」（P.10-10）を参照してください。

新規ユーザ モード、PIN クリア モード、および新規 PIN モード

PIN のクリアは、ネットワーク管理者だけの権限で、SDI サーバでのみ実行できます。

新規ユーザ モード、PIN クリア モード、新規 PIN モードでは、AnyConnect は、後の「next passcode」ログイン チャレンジで使用するために、ユーザ作成 PIN またはシステムが割り当てた PIN をキャッシュに入れます。

PIN クリア モードと新規ユーザ モードは、リモート ユーザから見ると違いがなく、また、セキュア ゲートウェイでの処理も同じです。いずれの場合も、リモート ユーザは新しい PIN を入力するか、SDI サーバから割り当てられる新しい PIN を受け入れる必要があります。唯一の相違点は、最初のチャレンジでのユーザの応答です。

新規 PIN モードでは、通常のチャレンジと同様に、既存の PIN を使用してパスコードが生成されます。PIN クリア モードでは、ユーザがトークン コードだけを入力するハードウェア トークンとして PIN が使用されることはありません。RSA ソフトウェア トークンのパスコードを生成するためにゼロが 8 つ並ぶ PIN（00000000）が使用されます。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新規ユーザを SDI サーバに追加すると、既存ユーザの PIN をクリアする場合と同じ結果になります。いずれの場合も、ユーザは新しい PIN を指定するか、SDI サーバから割り当てられる新しい PIN を受け入れる必要があります。これらのモードでは、ユーザはハードウェア トークンとして、RSA デバイスのトークン コードのみ入力します。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新しい PIN の入手

現行の PIN がない場合、システム設定に応じて、SDI サーバは次の条件のいずれかを満たす必要があります。

- ユーザは、PIN を作成するか、システムの割り当てを受け入れるかを選択できる。
- ユーザは新規 PIN を作成する必要がある。
- システムがユーザに新規 PIN を割り当てる必要がある。

デフォルトでは、PIN はシステムによって割り当てられます。

PIN をリモート ユーザ自身で作成する方法とシステムで割り当てる方法を選択できるように SDI サーバを設定している場合、ログイン画面にはオプションを示すドロップダウン リストが表示されます。ステータス行にプロンプト メッセージが表示されます。いずれの場合も、ユーザは今後のログイン認証のためにこの新規 PIN を忘れないようにする必要があります。

新規 PIN の作成

ユーザが新しく PIN を作成するように選択して [続行（Continue）]（図 10-5）をクリックすると、AnyConnect にこの PIN を入力するためのダイアログボックス（図 10-6）が表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。

図 10-5　ユーザが PIN の作成を選択

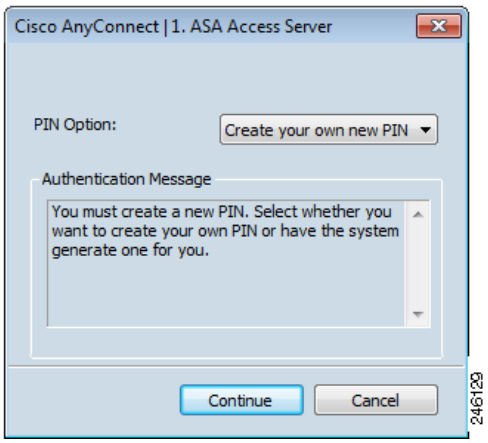
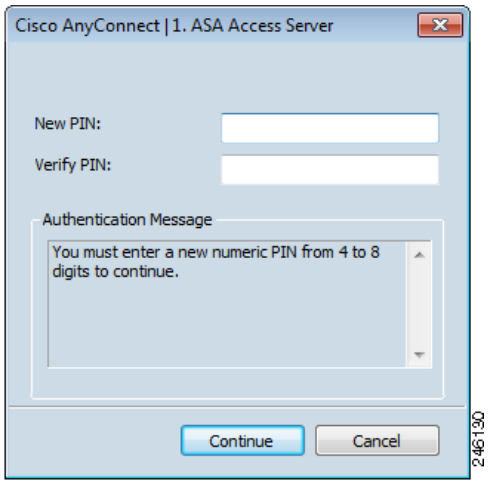


図 10-6　新規 PIN の作成



ユーザが PIN を作成する場合、新規 PIN を入力および確認したら、[続行（Continue）] をクリックします。PIN は一種のパスワードであるため、ユーザがこの入力フィールドに入力する内容はアスタリスクで表示されます。RADIUS プロキシを使用する場合、PIN の確認は、最初のダイアログボックスの次に表示される、別のチャレンジで行われます。クライアントは新しい PIN をセキュア ゲートウェイに送信し、セキュア ゲートウェイは「next passcode」チャレンジに進みます。

システムが割り当てる PIN の場合、ユーザがログイン ページで入力したパスコードを SDI サーバが受け入れると、セキュア ゲートウェイはシステムが割り当てた PIN をクライアントに送信します。ユーザは [続行（Continue）] をクリックする必要があります。クライアントは、ユーザが新規 PIN を確認したことを示す応答をセキュア ゲートウェイに返し、システムは「next passcode」チャレンジに進みます。

いずれの場合も、ユーザは次回のログイン認証のために PIN を忘れないようにする必要があります。

「Next Passcode」および「Next Token Code」チャレンジ

「next passcode」チャレンジでは、クライアントが新規 PIN の作成または割り当て時にキャッシュに入れられた PIN 値を使用して RSA SecurID Software Token DLL から次のパスコードを取得し、ユーザにプロンプト表示せずにこれをセキュア ゲートウェイに返します。同様に、ソフトウェア トークン用の「next Token Code」チャレンジでは、クライアントは RSA SecurID Software Token DLL から次のトークン コードを取得します。

RADIUS/SDI プロキシと AnyConnect との互換性の保持

ここでは、AnyConnect が、RSA SecureID ソフトウェア トークンを使用して、1 台以上の SDI サーバのプロキシ サーバである RADIUS サーバ経由でクライアントに配布されたユーザ プロンプトに適切に応答する手順について説明します。ここでは、次の項目について説明します。

- AnyConnect と RADIUS/SDI サーバのインタラクション
- RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

AnyConnect と RADIUS/SDI サーバのインタラクション

リモート ユーザが AnyConnect で ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信を行い、次に、このサーバが認証について SDI サーバと通信を行います。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージ テキストは、ASA が SDI サーバと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、AnyConnect にネイティブ SDI サーバとして認識させるために、ASA は RADIUS サーバからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージ テキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトは、認証中に必要とされるアクションに対して適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

次の項では、SDI 固有の RADIUS 応答メッセージを解釈し、AnyConnect ユーザに適切なアクションを求めるプロンプトを表示するように ASA を設定する手順について説明します。

RADIUS 応答メッセージを転送するための接続プロファイル（トンネル グループ）を、SDI サーバとの直接通信をシミュレートする方法で設定します。SDI サーバに認証されるユーザは、この接続プロファイルを介して接続する必要があります。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。

ステップ 2　SDI 固有の RADIUS 応答メッセージを解釈するために設定する接続プロファイルを選択して、[編集（Edit）] をクリックします。

ステップ 3　[EAnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウで、左側のナビゲーション ペインにある [詳細（Advanced）] ノードを展開して、[グループ エイリアス / グループ URL（Group Alias/Group URL）] を選択します。

ステップ 4　[ログイン画面への SecurID メッセージの表示を有効にする（Enable the display of SecurID messages on the login screen）] にチェックマークを付けます。

ステップ 5　[OK] をクリックします。

ステップ 6　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [AAA/ ローカル ユーザ（AAA/Local Users）] > [AAA サーバ グループ（AAA Server Groups）] を選択します。

ステップ 7　[追加（Add）] をクリックして、AAA サーバ グループを追加します。

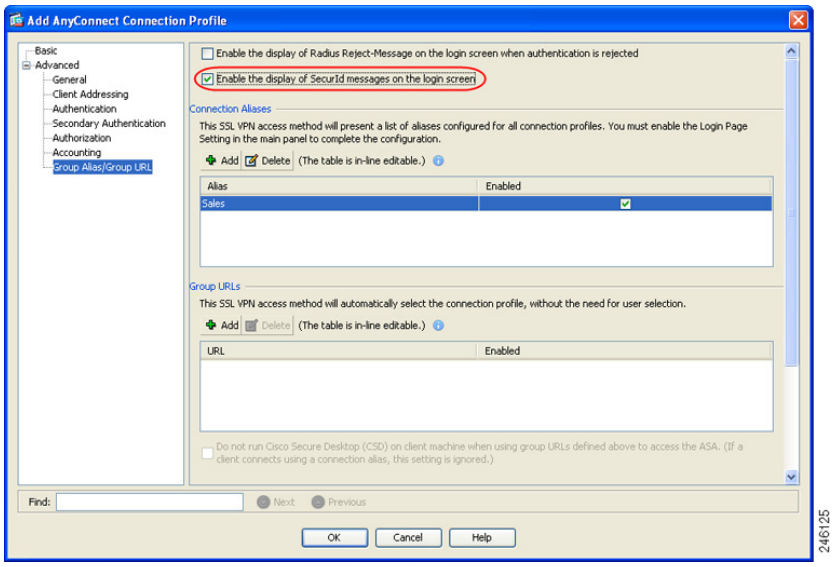
ステップ 8　[AAA サーバ グループの編集（Edit AAA Server Group）] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9　[AAA サーバ グループ（AAA Server Groups）] 領域で作成した AAA サーバ グループを選択し、[選択したグループ内のサーバ（Servers in the Selected Group）] 領域で [追加（Add）] をクリックします。

ステップ 10　[SDI メッセージ（SDI Messages）] 領域で [メッセージ テーブル（Message Table）] 領域を展開します。メッセージ テキスト フィールドをダブルクリックするとメッセージを編集できます。RADIUS サーバから送信されたメッセージとテキストの一部または全体が一致するように、RADIUS 応答メッセージ テキストを ASA で設定します。

ステップ 11　[OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

図 10-7　[AnyConnect 接続プロファイルの追加 / 編集（Add/Edit AnyConnect Connection Profile）] 画面



が使用するデフォルトのメッセージ テキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージ テキストです。ASACisco Secure ACS を使用していて、デフォルトのメッセージ テキストを使用している場合、ASA でメッセージ テキストを設定する必要はありません。これ以外の場合は、メッセージ テキストが一致するようにメッセージを設定します。

表 10-1 は、メッセージ コード、デフォルトの RADIUS 応答メッセージ テキスト、および各メッセージの機能を示しています。セキュリティ アプライアンスは、表での出現順に文字列を検索するため、メッセージ テキスト用に使用する文字列が別の文字列のサブセットでないことを確認する必要があります。

たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージ テキストのサブセットだとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを一致させます。

表 10-1　SDI 操作コード、デフォルト メッセージ テキスト、およびメッセージ機能

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。