モバイルプラットフォーム向け Cisco AnyConnect リリース 4.8 管理者ガイド

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/

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. 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. (1721R)

© 2019–2020 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 **モバイル デバイスの AnyConnect 1**

モバイル デバイスでの AnyConnect の動作およびオプション 1

AnyConnect Mobile VPN 接続について 1

モバイル デバイスでの AnyConnect VPN 接続エントリ 2

トンネリング モード 2

モバイル デバイスでのセキュア ゲートウェイ認証 3

モバイル デバイスでのクライアント認証 5

モバイル デバイスでのローカリゼーション 6

適応型セキュリティ アプライアンスへの変換テーブルのインポート 8

モバイル デバイスでの FIPS および Suite B 暗号化 8

Android デバイスの AnyConnect 9

Android での AnyConnect の注意事項と制約事項 9

Android 固有の考慮事項 10

Android モバイル ポスチャ デバイスの ID 生成 10

Android デバイスのアクセス許可 11

ASA セキュア ゲートウェイでのモバイル デバイスの VPN 接続の設定 12

アプリケーション単位 VPN の設定 14

Cisco AnyConnect 企業アプリケーション セレクタ ツールのインストール 15

Android デバイスのアプリケーション単位 VPN ポリシーの定義 15

アプリケーション単位カスタム属性の作成 17

ASA のポリシーへのカスタム属性の割り当て 18

AnyConnect VPN プロファイルでのモバイル デバイス接続の設定 18

URI ハンドラを使用した AnyConnect アクションの自動化 20

VPN 接続エントリの生成 21

VPN 接続の確立 25
VPN からの接続解除 28
証明書のインポート 28
VPN クライアント プロファイルのインポート 28
AnyConnect UI とメッセージのローカライズ 29
モバイル デバイスでの AnyConnect のトラブルシューティング 29

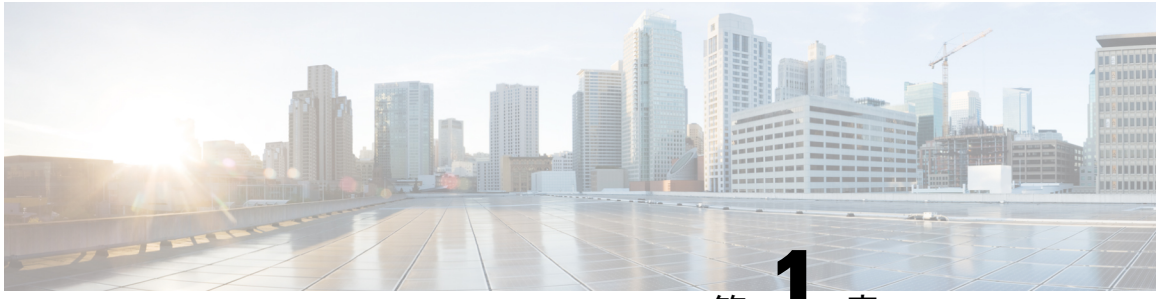
第 2 章
AnyConnect プロファイル エディタ 31
プロファイル エディタについて 31
ASDM からの新しいプロファイルの追加 31
AnyConnect VPN プロファイル 32
AnyConnect プロファイル エディタ、プリファレンス（Part 1） 33
AnyConnect プロファイル エディタ、プリファレンス（Part 2） 38
AnyConnect プロファイル エディタのバックアップ サーバ 44
AnyConnect プロファイル エディタの証明書照合 45
AnyConnect プロファイル エディタの証明書の登録 48
AnyConnect プロファイル エディタの証明書ピン 50
証明書ピン留めウィザード 50
AnyConnect プロファイル エディタのモバイル ポリシー 51
AnyConnect プロファイル エディタのサーバ リスト 51
AnyConnect プロファイル エディタのサーバ リストの追加/編集 52
AnyConnect プロファイル エディタのモバイル設定 54
NVM プロファイル エディタ 57
AnyConnect ローカル ポリシー 62
ローカル ポリシー パラメータと値 62
ローカル ポリシー パラメータの手動変更 66
MST ファイルでのローカル ポリシー パラメータの有効化 67
Enable FIPS ツールによるローカル ポリシー パラメータの有効化 67

第 3 章
VPN アクセスの設定 69
VPN への接続と接続解除 69

AnyConnect VPN 接続オプション 69
VPN 接続サーバの設定 71
ログイン前の Windows VPN 接続の自動開始 73
Start Before Logon について 73
Start Before Logon の制限 74
Start Before Logon の設定 74
Start Before Logon のトラブルシューティング 76
AnyConnect 起動時の VPN 接続の自動開始 76
Windows システムにおける Start Before Logon（PLAP）の設定 77
PLAP のインストール 77
PLAP を使用した Windows PC へのログオン 78
PLAP を使用した AnyConnect からの接続解除 78
VPN 接続の自動リスタート 79
Trusted Network Detection を使用した接続または接続解除 79
Trusted Network Detection について 79
Trusted Network Detection のガイドライン 80
Trusted Network Detection の設定 81
Always-Onを使用した VPN 接続の必要性 83
Always-On VPN について 83
Always-On VPN の制限事項 84
Always-On VPN のガイドライン 84
Always-On VPN の設定 85
キャプティブ ポータル ホットスポットの検出と修復の使用 89
キャプティブ ポータルについて 89
キャプティブ ポータル修復の設定 90
キャプティブ ポータルの修復の強化（Windows のみ） 91
キャプティブ ポータルの修復の設定ブラウザのフェールオーバー 91
キャプティブ ポータルの検出と修復のトラブルシューティング 92
AnyConnect over L2TP または PPTP の設定 93
ユーザに対する PPP 除外上書きの指示 94
管理 VPN トンネルの使用 95

管理 VPN トンネルについて 95
管理 VPN トンネルの設定 97
管理 VPN トンネル接続問題のトラブルシューティング 101
AnyConnect プロキシ接続の設定 102
AnyConnect プロキシ接続について 102
AnyConnect プロキシ接続の要件 104
プロキシ接続の制限 104
ローカル プロキシ接続の許可 104
パブリック プロキシ 104
プライベート プロキシ接続の設定 106
プロキシ設定の確認 107
VPN トラフィックの選択および除外 107
VPN をバイパスするための IPv4 または IPv6 トラフィックの設定 107
ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定 109
スプリット トンネリングの設定 109
ダイナミック スプリット トンネリングについて 109
スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性 110
スプリット トンネリング設定をともなう重複シナリオの結果 111
ダイナミック スプリット トンネリングの使用状況の通知 112
スプリット DNS 112
スプリット DNS の要件 112
スプリット DNS の設定 113
AnyConnect ログを使用したスプリット DNS の確認 114
スプリット DNS を使用しているドメインの確認 114
VPN 認証の管理 114
重要なセキュリティ上の考慮事項 114
サーバ証明書処理の設定 115
サーバ証明書の確認 115
無効なサーバ証明書の処理 116

Certificate-Only 認証の設定 118
証明書登録の設定 119
SCEP プロキシの登録と動作 119
認証局の要件 120
証明書登録のガイドライン 120
SCEP プロキシ証明書登録の設定 121
SCEP 用の Windows 2008 Server の認証局の設定 122
証明書失効通知の設定 124
証明書選択の設定 125
使用する証明書ストアの設定 125
Windows ユーザに認証証明書の選択を求めるプロンプトの表示 128
macOS および Linux での PEM 証明書ストアの作成 129
証明書照合の設定 130
SAML を使用した VPN 認証 133
SDI トークン（SoftID）統合を使用した VPN 認証 134
SDI 認証交換のカテゴリ 136
ネイティブ SDI と RADIUS SDI の比較 138
RADIUS/SDI メッセージをサポートするための ASA の設定 139
証明書のピン留めについて 141
グローバル ピンとホストごとのピン 142



第 1 章

モバイル デバイスの AnyConnect

モバイル デバイスの AnyConnect は、Windows、Mac、および Linux プラットフォームの AnyConnect に似ています。この章では、モバイルデバイスでの AnyConnect に固有のデバイス情報、設定情報、サポート情報、およびその他の管理タスクについて説明します。

- モバイル デバイスでの AnyConnect の動作およびオプション （1 ページ）
- Android デバイスの AnyConnect （9 ページ）
- ASA セキュア ゲートウェイでのモバイル デバイスの VPN 接続の設定 （12 ページ）
- アプリケーション単位 VPN の設定 （14 ページ）
- AnyConnect VPN プロファイルでのモバイル デバイス接続の設定 （18 ページ）
- URI ハンドラを使用した AnyConnect アクションの自動化 （20 ページ）
- モバイル デバイスでの AnyConnect のトラブルシューティング （29 ページ）

モバイルデバイスでのAnyConnectの動作およびオプション

AnyConnect Mobile VPN 接続について

このリリースの AnyConnect Secure Mobility Client は、次のモバイル プラットフォームに対応しています。

- Android

Cisco AnyConnect は、サポートされている各プラットフォームのアプリストアに用意されています。www.cisco.com では入手できません。また、セキュリティで保護されたゲートウェイから配布されていません。

AnyConnect モバイルアプリには、コア VPN クライアントのみが含まれています。ネットワーク アクセス マネージャ、ポスチャ、Web セキュリティなどの他の AnyConnect モジュールは含まれていません。VPN が接続中の場合は、モバイル ポスチャと呼ばれるポスチャ情報が、AnyConnect Identify Extensions（ACIDex）を使用してヘッドエンドに提供されます。

AnyConnect VPN 接続は、次のいずれかの方法で確立できます。

- ユーザが手動で確立する。
- ユーザが管理者により提供された自動接続アクションをクリックする際に手動で確立する（Android および Apple iOS のみ）。
- 自動：Connect on-Demand 機能により確立される（Apple iOS のみ）。

モバイル デバイスでの AnyConnect VPN 接続エントリ

接続エントリは、セキュア ゲートウェイのアドレスを完全修飾ドメイン名または IP アドレス（必要に応じてトンネル グループ URL を含む）で識別します。また、他の接続属性を含めることもできます。

AnyConnect では、1 台のモバイル デバイス上の複数の接続エントリをサポートすることで、異なるセキュア ゲートウェイや VPN トンネル グループに対応します。複数の接続エントリが設定されている場合は、VPN 接続を開始するためにユーザがどれを使用するかを理解することが重要です。接続エントリは次の方法のいずれかで設定されます。

- ユーザが手動で設定します。モバイル デバイスの接続エントリを設定する手順については、該当するプラットフォームのユーザ ガイドを参照してください。
- ユーザが管理者により提供されたリンクをクリックした後で追加し、接続エントリを設定します。

  ユーザにこの種の接続エントリ設定を提供するには、「VPN 接続エントリの生成 （21 ページ）」を参照してください。
- Anyconnect VPN クライアント プロファイルで定義されます。

  AnyConnect VPN クライアント プロファイルでは、クライアント動作を指定し、VPN 接続エントリを定義します。詳細については、「AnyConnect VPN プロファイルでのモバイル デバイス接続の設定 （18 ページ）」を参照してください。

トンネリング モード

AnyConnect は、マネージド BYOD またはアンマネージド BYOD 環境で動作可能です。これらの環境での VPN トンネリングは、次のいずれかのモードでのみ動作します。

- システム トンネリング モード：VPN 接続が、すべてのデータをトンネリングするために（完全トンネリング）、または特定のドメインまたはアドレスとの間で送受信されるデータのみをトンネリングするために（スプリット トンネリング）使用されます。このモードは、すべてのモバイル プラットフォームで使用できます。
- アプリケーション単位 VPN モード：VPN 接続はモバイル デバイス上の特定のアプリケーション セットで使用されます（Android および Apple iOS のみ）。

  AnyConnect では、管理者によってヘッドエンドで定義されているアプリケーションのセットを使用できます。このリストを定義するには、ASA のカスタム属性のメカニズムを使用します。このリストは AnyConnect クライアントに送信され、デバイスで適用されます。

他のすべてのアプリケーションに対しては、データはトンネルを介さずに、または暗号化されずに送信されます。

Apple iOS でこのモードで実行するには、マネージド環境が必要です。Android では、マネージドとアンマネージドの両方の環境がサポートされます。いずれのプラットフォームでも、マネージド環境では、AnyConnect でトンネリングするように設定されている一連のアプリケーションと同じアプリケーションをトンネリングするように Mobile Device Manager でデバイスを設定する必要があります。

AnyConnect は、ASA ヘッドエンドから受信した設定情報で決定したモードで動作します。具体的には、接続に関連付けられたグループ ポリシーまたはダイナミック アクセス ポリシー（DAP）内に、アプリケーション単位VPNのリストがあるかどうかに基づきます。アプリケーション単位 VPN のリストが存在する場合、AnyConnect はアプリケーション単位 VPN モードで動作し、存在しない場合は AnyConnect はシステム トンネリング モードで動作します。

モバイル デバイスでのセキュア ゲートウェイ認証

信頼されていないサーバのブロック

VPN 接続を確立するときに、AnyConnect はセキュア ゲートウェイから受信したデジタル証明書を使用してサーバの身元を確認します。サーバ証明書が無効な場合（期限切れか無効な日付、キーの誤用、名前の不一致により証明書エラーがある）、または信頼できない場合（認証局が確認できない）場合、接続はブロックされます。ブロッキング メッセージが表示されるため、ユーザは処理を選択する必要があります。

[信頼されていないサーバをブロック（Block Untrusted Servers）] アプリケーション設定は、セキュア ゲートウェイを識別できない場合、AnyConnectがどのように反応するかを決定します。この保護はデフォルトではオンです。ユーザはオフにできますが、これは推奨されません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオンの場合、信頼できない VPN サーバをブロックするという通知によって、ユーザにセキュリティ上の脅威が警告されます。ユーザは以下を選択できます。

- [安全を確保（Keep Me Safe）] を選択して、この接続を終わらせ、安全にしておきます。
- [設定の変更（Change Settings）] を選択して、[信頼されていないサーバをブロック（Block Untrusted Servers）] アプリケーション プリファレンスをオフにします。ただし、これは推奨されません。ユーザがこのセキュリティ保護を無効にすると、VPN 接続を再起動しなくてはなりません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオフの場合、信頼できない VPN サーバをブロックしないという通知によって、ユーザにセキュリティ上の脅威が警告されます。ユーザは以下を選択できます。

- [キャンセル（Cancel）] を選択して、接続をキャンセルし、安全にしておきます。
- [続行（Continue）] を選択して、接続を続行します。ただし、これは推奨されません。

- [詳細の表示（View Details）] を選択して、証明書の詳細を表示して受け入れるかどうかを判断します。

  ユーザが確認している証明書が有効であるが信頼できない場合、ユーザは次のことを実行できます。

  - 再使用できるようにサーバ証明書を AnyConnect 証明書ストアにインポートし、[インポートおよび継続（Import and Continue）] を選択して接続を継続します。

    AnyConnect ストアにこの証明書がインポートされると、このデジタル証明書を使用しているそのサーバに対する後続の接続は自動的に受け入れられます。

  - 前の画面に戻り、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

  証明書が無効な場合、または何らかの理由で、ユーザが前の画面にだけ戻ることができる場合、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

VPN 接続の最も安全な設定では、[信頼されていないサーバをブロック（Block Untrusted Servers）] の設定をオン（デフォルト設定）のままにし、自身のセキュア ゲートウェイで設定された（有効で信頼できる）サーバ証明書を所有し、モバイル ユーザには常に [安全を確保（Keep Me Safe）] を選択させる必要があります。

（注） [厳格な証明書トラスト（Strict Certificate Trust）] はこの設定を上書きします（以下の説明を参照）。

OCSP 失効

AnyConnect クライアントは OCSP（Online Certificate Status Protocol）をサポートします。これにより、OCSP レスポンダに要求を行い OCSP 応答を解析して証明書のステータスを取得することで、クライアントはリアルタイムで個々の証明書のステータスを照会できます。OCSP は、証明書チェーン全体を確認するために使用されます。OCSP レスポンダにアクセスする際、証明書ごとに 5 秒のタイムアウト間隔があります。

ユーザは Anyconnect 設定アクティビティで OCSP 検証を有効または無効にすることができます。詳細については、『Cisco AnyConnect Secure Mobility Client の Android 向けユーザガイド リリース 4.6』を参照してください。MDM 管理者がリモートでこの機能を制御するために使用できる新しい API がフレームワークに追加されました。現在、Samsung と Google MDM がサポートされています。

厳格な証明書トラスト

ユーザーによって有効にされた場合、リモートセキュリティゲートウェイの認証時に AnyConnect は確認できない証明書を許可しません。これらの証明書を受け入れるようユーザにプロンプトを表示するのではなく、クライアントはセキュリティ ゲートウェイへの接続に失敗します。

（注） この設定は、[信頼されていないサーバをブロック（Block Untrusted Servers）] よりも優先されます。

オフにすると、クライアントはユーザに証明書を受け入れるように求めます。これはデフォルトの動作です。

以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

- 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザが接続している場合に「中間者」攻撃を防ぐために役立ちます。
- 完全に検証可能で信頼できる証明書を使用する場合でも、AnyConnect クライアントは、デフォルトでは、未検証の証明書の受け入れをエンド ユーザに許可します。エンド ユーザが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエンドユーザに求めます。エンドユーザによるこの判断を回避するには、厳格な証明書トラストを有効にします。

モバイル デバイスでのクライアント認証

VPN 接続を完了するには、ユーザはユーザ名とパスワード、もしくはデジタル証明書、またはその両方の形式でクレデンシャルを提供して認証する必要があります。管理者は、トンネル グループの認証方式を定義します。モバイル デバイスでの最適なユーザ エクスペリエンスを達成するために、認証設定に応じて複数の AnyConnect 接続プロファイルを使用することをお勧めします。ユーザエクスペリエンスとセキュリティのバランスを最適に保つ方法を決める必要があります。推奨事項は次のとおりです。

- モバイル デバイスの AAA 対応認証トンネル グループについては、クライアントを再接続状態にし、ユーザが再認証しなくても済むよう、グループ ポリシーは 24 時間など非常に長時間のアイドル タイムアウトが必要になります。
- 最もトランスペアレントなユーザエクスペリエンスを達成するには、証明書のみの認証を使用します。デジタル証明書を使用すると、VPN 接続は、ユーザとの対話なしで確立されます。

証明書を使用してセキュア ゲートウェイにモバイル デバイスを認証するため、エンド ユーザは、デバイスに証明書をインポートする必要があります。インポートすると、この証明書が自動証明書選択の対象として有効になり、特定の接続エントリに手動で関連付けることもできるようになります。証明書は、次の方法を使用してインポートされます。

- ユーザが手動でインポートします。モバイルデバイスに証明書をインポートする手順については、適切なユーザ ガイドを参照してください。
- SCEP を使用します。詳細については、「証明書登録の設定 （119 ページ）」を参照してください。

- 証明書をインポートするために管理者により提供されたリンクをユーザがクリックした後に追加されます。

  ユーザにこの種の証明書展開を提供するための詳細については、「証明書のインポート（28 ページ）」を参照してください。

モバイル デバイスでのローカリゼーション

Android および Apple iOS 用 AnyConnect Secure Mobility Client は、ローカリゼーションをサポートし、AnyConnect ユーザ インターフェイスやメッセージをユーザのロケールに適用しています。

パッケージ済みのローカリゼーション

AnyConnect Android および Apple iOS アプリには、次の言語訳が含まれます。

- カナダ フランス語（fr-ca）
- 中国語（台湾）（zh-tw）
- チェコ語（cs-cz）
- オランダ語（nl-nl）
- フランス語（fr-fr）
- ドイツ語（de-de）
- ハンガリー語（hu-hu）
- イタリア語（it-it）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- 中南米スペイン語（es-co）
- ポーランド語（pl-pl）
- ポルトガル語（ブラジル）（pt-br）
- ロシア語（ru-ru）
- 簡体字中国語（zh-cn）
- スペイン語（es-es）

AnyConnect のインストール時には、これらの言語のローカリゼーション データがモバイル デバイスにインストールされます。モバイルデバイスで指定されている地域に従って、表示される言語が決定します。AnyConnect は最適なものを判断するため、言語仕様を使用してから、リージョン仕様を使用します。たとえば、インストール後にロケール設定をスイス フランス語

（fr-ch）にすると、カナダ フランス語（fr-ca）表示になります。AnyConnect の UI とメッセージは、AnyConnect の起動時に変換されます。

ダウンロードされたローカリゼーション

AnyConnect パッケージにはない言語に関して、管理者は、AnyConnect VPN 接続のデバイスにダウンロードされるローカライズ データを ASA に追加します。

シスコでは、ローカライズ可能な AnyConnect 文字列をすべて含む anyconnect.po ファイルを Cisco.com の製品ダウンロードセンターで提供しています。AnyConnect 管理者は、anyconnect.po ファイルをダウンロードし、使用可能な文字列を翻訳してから、ASA にファイルをアップロードします。anyconnect.po ファイルを ASA にすでにインストールしている AnyConnect 管理者は、この更新バージョンをダウンロードしてください。

初期状態では、AnyConnect ユーザ インターフェイスおよびメッセージがインストールした言語でユーザに表示されます。デバイスユーザが ASA への初めての接続を確立すると、AnyConnect では、デバイスの優先言語と ASA 上で使用可能なローカリゼーション言語が比較されます。一致するローカリゼーションファイルが検索されると、ローカライズされたファイルがダウンロードされます。ダウンロードが完了すると、AnyConnect は anyconnect.po ファイルに追加された変換文字列を使用してユーザ インターフェイスおよびユーザ メッセージを表示します。文字列が翻訳されていない場合、AnyConnect ではデフォルトの英語文字列が表示されます。

ASA でのローカリゼーションの設定手順については、「適応型セキュリティ アプライアンスへの変換テーブルのインポート （8 ページ）」を参照してください。ASA にデバイスのロケールのローカリゼーション データが含まれていない場合、AnyConnect アプリケーション パッケージにプリインストールされたローカリゼーション データを引き続き使用します。

モバイル デバイスにローカリゼーションを提供するその他の方法

ユーザに URI リンクを提供することにより、AnyConnect UI とメッセージのローカライズ （29 ページ）を実行します。

モバイル デバイスのユーザに、所有するデバイスでのローカリゼーション データの管理を依頼します。次のローカリゼーションアクティビティを実行する手順については、該当するユーザ ガイドを参照してください。

- 指定したサーバからのローカリゼーションデータのインポート。ユーザは、ローカリゼーション データのインポートを選択し、セキュア ゲートウェイのアドレスとロケールを指定します。ロケールは ISO 639-1 で指定されており、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。このローカリゼーション データは、インストールされたローカリゼーション データの代わりに使用されます。
- デフォルトのローカリゼーションデータのリストア。AnyConnect パッケージから事前ロードされたローカリゼーションデータの使用を復元し、インポートされたローカリゼーション データをすべて削除します。

適応型セキュリティ アプライアンスへの変換テーブルのインポート

手順

ステップ 1 www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2 ASDM で、**[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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 3 [インポート（Import）] をクリックします。[言語ローカリゼーション エントリのインポート（Import Language Localization Entry）] ウィンドウが表示されます。

ステップ 4 ドロップダウン リストから適切な言語を選択します。

ステップ 5 変換テーブルのインポート元を指定します。

ステップ 6 [今すぐインポート（Import Now）] をクリックします。この変換テーブルが、この優先言語で AnyConnect クライアントに展開されます。ローカリゼーションは、AnyConnect がリスタートし、再接続した後に適用されます。

（注） 非モバイルデバイスで実行される AnyConnect の場合、Cisco Secure Desktop が使用されていない場合でも、ホストスキャンメッセージがローカライズされるためには、適応型セキュリティ アプライアンスに Cisco Secure Desktop 変換テーブルもインポートする必要があります。

モバイル デバイスでの FIPS および Suite B 暗号化

モバイル デバイス向け AnyConnect には、Cisco Common Cryptographic Module（C3M）が組み込まれています。これは、新世代の暗号化（NGE）アルゴリズムの一部として FIPS 140-2 に準拠した暗号化モジュールや NSA Suite B 暗号化が含まれる Cisco SSL の実装です。Suite-B 暗号化は、IPSec VPN でのみ使用可能です。FIPS 準拠の暗号化は、IPSec VPN および SSL VPN の両方で使用可能です。

暗号化アルゴリズムを使用すると、接続の間、ヘッドエンドルータとネゴシエートされます。ネゴシエーションは、VPN 接続の両端の機能によって異なります。したがって、セキュア ゲートウェイは、FIPS に準拠する暗号化および Suite B の暗号化をサポートする必要があります。

ユーザは、AnyConnect アプリケーション設定の **FIPS モード**を有効にすることで、ネゴシエーションにおいて NGE アルゴリズムだけを受け入れるように AnyConnect を設定します。FIPS モードが無効の場合、AnyConnect は VPN 接続の非 FIPS 暗号アルゴリズムも受け入れます。

モバイルのその他のガイドラインと制限事項

- Apple iOS 5.0 以降が Suite B の暗号化に必要です。これは Suite B で使用される ECDSA の証明書をサポートする Apple iOS の最も低いバージョンです。

- Android 4.0（Ice Cream Sandwich）以降が Suite B の暗号化に必要です。これは、SuiteB で使用される ECDSA の証明書をサポートする Android の最も低いバージョンです。
- FIPS モードで動作しているデバイスには、プロキシ方式または従来の方法でデジタル証明書をモバイルユーザに提供するための SCEP の使用との互換性がありません。状況に応じた展開計画を立ててください。

Android デバイスの AnyConnect

このリリースでサポートされている機能およびデバイスについては、『Cisco AnyConnect Secure Mobility Client リリースノート アンドロイド用リリース 4.6.x』を参照してください。

AnyConnect アプリケーションをインストール、アップグレード、使用する方法の詳細については、『 Cisco AnyConnect Secure Mobility Client の Android 向けユーザガイド リリース 4.6』を参照してください。

Android での AnyConnect の注意事項と制約事項

- ASA は、AnyConnect for Android のディストリビューションと更新プログラムを提供しません。Google Play からのみ入手できます。
- AnyConnect for Android はネットワーク可視性モジュールのみサポートし、他の AnyConnect モジュールはサポートしていません。
- Android デバイスでは 1 つの AnyConnect プロファイル（ヘッドエンドから受信した最後のプロファイル）だけがサポートされます。ただし、プロファイルは複数の接続エントリで構成できます。
- ユーザが、サポートされていないデバイスに AnyConnect をインストールしようとすると、「インストールエラー: 原因不明 -8（Installation Error: Unknown reason -8）」というポップアップ メッセージが表示されます。これは Android OS により生成されるメッセージです。
- ユーザがホーム スクリーンに AnyConnect ウィジェットを表示している場合、[始動時に開始（Launch at startup）] 設定に関わらず AnyConnect サービスが自動的に開始されます（ただし接続は確立されません）。
- AnyConnect for Android では、クライアント証明書からの事前入力を使用する場合に、拡張 ASCII 文字のために UTF-8 文字エンコードが必要です。事前入力機能を使用する場合は、クライアント証明書が UTF-8 でなければなりません（KB-890772 および KB-888180 の説明を参照）。
- AnyConnect は、EDGE の固有の性質およびその他の早期無線テクノロジーによって EDGE 接続上の VPN トラフィックを送受信する場合、ボイスコールをブロックします。
- いくつかのよく知られているファイル圧縮ユーティリティでは、[AnyConnect ログ送信（AnyConnect Send Log）] ボタンを使用してパッケージされたログ バンドルを圧縮解除で

きません。回避策として、AnyConnect ログ ファイルの圧縮解除には Windows および Mac OS X のネイティブ ユーティリティを使用してください。

- **DHE の非互換性**

  AnyConnect リリース 4.6 で導入された DHE 暗号サポートにより、ASA 9.2 より前の ASA バージョンで非互換性の問題が発生します。9.2 より前の ASA リリースで DHE 暗号を使用している場合、これらの ASA バージョンで DHE 暗号を無効にする必要があります。

Android 固有の考慮事項

Android モバイル ポスチャ デバイスの ID 生成

新規インストール時、またはユーザがアプリケーション データを消去した後、AnyConnect は Android ID に基づいて 256 バイトの一意のデバイス ID を生成します。この ID は、以前のリリースで生成された IMEI と MAC アドレスに基づく 40 バイトのレガシー デバイス ID を置き換えます。

AnyConnect の以前のバージョンがインストールされている場合、レガシー ID はすでに生成されています。AnyConnect のこのバージョンにアップグレードすると、ユーザがアプリケーション データを消去するか AnyConnect をアンインストールするまで、このレガシー ID は引き続きデバイスの固有 ID として報告されます。

生成されたデバイス ID は、AnyConnect アプリケーションの初回起動時に、AnyConnect の **[診断（Diagnostics）] > [ログインとシステム情報（Logging and System Information）] > [システム（System）] > [デバイス識別子（Device Identifiers）]** 画面、`device_identifiers.txt` ファイルの AnyConnect ログ、または [情報（About）] 画面から参照できます。

（注） セキュア ゲートウェイ上の DAP ポリシーは、新しいデバイス ID を使用するように更新する必要があります。

`Device-ID` は、次のように決定されます。

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

ここで、`Android ID` と `bytesToHexString` は次のように定義されます。

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

Android デバイスのアクセス許可

次のアクセス許可が AnyConnect の動作用に Android マニフェスト ファイルで宣言されます。

マニフェストのアクセス許可	説明
uses-permission: android.permission.ACCESS_NETWORK_STATE	アプリケーションがネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.ACCESS_WIFI_STATE	アプリケーションが Wi-Fi ネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.BROADCAST_STICKY	アプリケーションがスティッキ インテントをブロードキャストすることを許可します。これは、クライアントが次のブロードキャストを待たなくてもデータをすぐに取得できるよう、完了後もデータがシステムによって保持されるブロードキャストです。
uses-permission: android.permission.INTERNET	アプリケーションがネットワーク ソケットを開くことを許可します。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	アプリケーションが外部ストレージから読み取ることを許可します。
uses-permission: android.permission.READ_LOGS	アプリケーションが低レベルのシステム ログ ファイルを読み取ることを許可します。
uses-permission: android.permission.READ_PHONE_STATE	デバイスの電話番号、現在の携帯電話ネットワーク情報、通話中のコールのステータス、デバイスに登録されているすべての PhoneAccounts のリストなどの電話状態への読み取り専用アクセスを許可します。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	システムの起動完了後にアプリケーションがブロードキャストを受信することを許可します。

ASA セキュア ゲートウェイでのモバイル デバイスの VPN 接続の設定

手順

ステップ 1 デスクトップ/モバイル エンドポイントに共通の設定手順については、該当するリリースの『Cisco ASA 5500-X Series Next-Generation Firewall 構成ガイド』を参照してください。モバイル デバイスの場合は以下を考慮してください。

属性	ASDM ロケーション	例外
ホーム ページ URL	**[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）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタマイズ（Customization）]**	AnyConnect Mobile は、ホームページの URL 設定を無視します。認証の成功後に、モバイル クライアントをリダイレクトすることはできません。
AnyConnect 接続プロファイル名およびエイリアス	**[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）] > [追加/編集（Add / Edit）]**	AnyConnect モバイル クライアント接続に使用するトンネル グループ（接続プロファイル）の [名前（Name）] または [エイリアス（Aliases）] フィールドに特殊文字を使用しないでください。特殊文字を使用すると、[ゲートウェイからの応答を処理できません（Unable to process response from Gateway）] とログに記録された後、[接続に失敗しました（Connect attempt has failed）] というエラー メッセージが AnyConnect クライアントに表示される場合があります。

属性	ASDM ロケーション	例外
デッド ピア検出	**[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）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]**	サーバ側のデッド ピア検出機能はデバイスがスリープ状態になることを防ぐため、オフに切り替えます。ただし、ネットワークの接続性が失われたことによってトンネルが終了したとき、そのことをクライアントが判断できるように、クライアント側のデッド ピア検出はオンにしておく必要があります。
SSL キープアライブ メッセージ	**[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）] > [グループ ポリシー（Group Policies）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]**	クライアント側のデッド ピア検出がすでに有効になっている場合、モバイルデバイスのバッテリ寿命を延ばすため、これらのキープアライブ メッセージを無効にすることを推奨します。
IPsec over NAT-T キープアライブ メッセージ	**[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）] > [詳細設定（Advanced）] > [IPsec] > [IKEポリシー（IKE Policies）]**	AnyConnect IPsec が機能するようにするには、[IPsec over NAT-Tの有効化（Enable IPsec over NAT-T）] を選択する必要があります。有効にすると、デフォルトでは NAT キープアライブ メッセージが 20 秒ごとに送信されるため、モバイル デバイスのバッテリーが過剰に消費されます。 これらのメッセージを無効にすることはできないため、モバイル デバイスのバッテリ消費への影響を最小限に抑えるには、NAT-T キープアライブを最大値（3600）に設定することを推奨します。 ASA CLI でこれを指定するには、`crypto isakmp nat-traversal 3600` コマンドを使用します。

ステップ 2 必要に応じてモバイルの接続を受け入れるか、拒否するか、または制限するようにモバイル ポスチャ（AnyConnect Identity Extensions（ACIDex）とも呼ばれる）を設定します。

適切なリリースの『Cisco ASA 5500-X Series Next-Generation Firewall 構成ガイド』で「Configuring Endpoint Attributes Used in DAPs」の手順を参照してください。

例：

接続の確立時に Apple iOS で AnyConnect によりヘッドエンドに送信される属性を次に示します。

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

ステップ 3 （任意） アプリケーション単位 VPN トンネリング モードを設定します。

「アプリケーション単位 VPN の設定 （14 ページ）」を参照してください。

アプリケーション単位 VPN トンネリングモードが設定されていない場合、AnyConnect アプリケーションはシステム トンネリング モードで動作します。

アプリケーション単位 VPN の設定

始める前に

AnyConnect アプリケーション単位 VPN トンネリングには、次のものが必要です。

- ASA 9.3.1 以降（アプリケーション単位 VPN トンネリングを設定する場合）。
- AnyConnect v4.0 Plus または Apex ライセンス。

AnyConnect アプリケーション単位 VPN では、次のモバイル プラットフォームがサポートされています。

- Android 5.0（Lollipop）以降を実行している Android デバイス。
- モバイルデバイス管理（MDM）ソリューションでアプリケーション単位 VPN を使用するように設定されている、Apple iOS 8.3 以降を実行している Apple iOS デバイス。

手順

ステップ 1 Cisco AnyConnect 企業アプリケーション セレクタ ツールのインストール （15 ページ）。

ステップ 2 アプリケーション セレクタ ツールを使用して、プラットフォームに対する AnyConnect のアプリケーション単位 VPN ポリシーを指定します。

- Android デバイスのアプリケーション単位 VPN ポリシーの定義 （15 ページ）

ステップ 3 ASA でのアプリケーション単位カスタム属性の作成 （17 ページ）。

ステップ 4 ASA のポリシーへのカスタム属性の割り当て （18 ページ）。

Cisco AnyConnect 企業アプリケーション セレクタ ツールのインストール

アプリケーション セレクタ ツールは、Android デバイスと Apple iOS デバイスの両方のポリシー生成をサポートするスタンドアロン アプリケーションです。

始める前に

Cisco AnyConnect 企業アプリケーション セレクタには Java 7 以降が必要です。

手順

ステップ 1 Cisco.com AnyConnect セキュア モビリティ クライアント v4.x ソフトウェアセンター から Cisco AnyConnect 企業アプリケーション セレクタ ツールをダウンロードします。

ステップ 2 ポリシーで Android アプリケーションを使用している場合は、Android SDK および Android SDK Build-tools をシステムにインストールしておく必要があります。そうしない場合は、次のようにインストールします。

a) アプリケーション セレクタ ツールを実行するプラットフォーム用の Android SDK Tools の最新バージョンをインストールします。

デフォルトのパスと設定（[全ユーザ用のインストール（Install for All Users）] が含まれるため、パッケージエンティティへのアクセスは前述のとおりになる）を使用して、プラットフォーム用の推奨された **SDK Tools Only** パッケージをインストールします。

b) Android SDK Manager を使用して、**Android SDK Build-tools** の最新バージョンをインストールします。

次のタスク

（注） アプリケーション セレクタ ツールで要求されたら、インストール場所（`Android SDK` のインストール ディレクトリ\`build-tools`*`build-tools`* バージョン番号\）を指定して、Android Asset Packaging Tool（**aapt**）へのアクセスを設定します。

Android デバイスのアプリケーション単位 VPN ポリシーの定義

アプリケーション単位 VPN ポリシーは一連のルールで構成され、各ルールではデータがトンネルを経由するアプリケーションが識別されます。モバイルデバイス環境内で許容されるアプ

リケーションとその使用方法をより厳密に特定するには、ルールオプションを指定します。アプリケーション セレクタ ツールは、アプリケーション パッケージ ファイル `*.apk` からの情報を使用して、ルールオプションを設定します。Android パッケージマニフェスト情報については、http://developer.android.com/guide/topics/manifest/manifest-element.html を参照してください。

始める前に

Cisco AnyConnect 企業アプリケーション セレクタには Java 7 以降が必要です。

手順

ステップ 1 アプリケーション セレクタを起動し、[Android] モバイル デバイス プラットフォームを選択します。

ステップ 2 必須の [アプリケーションID（App ID）] フィールドに値を設定します。

- ローカル システムに保存されているアプリケーションからアプリケーション固有のパッケージ情報をインポートするため、[ディスクからインポート（Import from Disk）] を選択します。

  [アプリケーションID（APP ID）] フィールド（逆 DNS 形式の文字列）には値が自動的に取り込まれます。例えば Apple iOS ポリシーに Chrome アプリケーションを選択した場合、[アプリケーションID（APP ID）] フィールドは **`com.google.chrome.ios`** に設定されます。Android の Chrome の場合、これは **`com.android.chrome`** に設定されます。

- あるいは、アプリケーション固有の情報を直接入力することもできます。

- ワイルドカードを使用した逆 DNS 形式を指定します。たとえば、ルールでアプリケーションを 1 つずつリストする代わりに、すべての Cisco アプリケーションをトンネリングするには com.cisco.* と指定します。ワイルドカードは、[アプリケーションID（APP ID）] のエントリの最後の文字である必要があります。

  管理対象環境でアプリケーション単位 VPN を設定している場合は、ASA ポリシーで同じアプリケーションを MDM ポリシーとしてトンネリングすることが許可されていることを確認します。アプリケーション ID として *.* を指定すると、すべてのアプリケーションをトンネリングでき、MDM ポリシーが、トンネリングされたアプリケーションの唯一のアービターとなります。

ステップ 3 （任意）リストされたアプリケーションを選択し、必要に応じてその他のパラメータを設定します。

- [最小バージョン（Minimum Version）]：パッケージのマニフェスト属性 *android:versionCode* で指定された、選択したアプリケーションの最小バージョン。

- [一致証明書 ID（Match Certificate ID）]：アプリケーション署名証明書のダイジェスト。

- [共有 UID を許可（Allow Shared UID）]：デフォルト値は true です。false に設定した場合、パッケージ マニフェストで *android: sharedUserId* 属性が指定されたアプリケーションはこのルールに一致せず、トンネルにアクセスできません。

ステップ 4 [ファイル（File）] > [保存（Save）] をクリックして、アプリケーション単位 VPN ポリシーを保存します。

ステップ 5 [ポリシー（Policy）] > [ポリシーの表示（View Policy）] を選択し、定義したポリシーの表示を確認します。

この文字列をコピーします。これは、ASA の *perapp* カスタム属性の値になる文字列です。

アプリケーション単位カスタム属性の作成

手順

ステップ 1 ASDM で、[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）] > [詳細（Advanced）] > [AnyConnect カスタム属性（AnyConnect Custom Attributes）] に移動してカスタム属性タイプを設定します。

ステップ 2 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性タイプの作成/編集（Create / Edit Custom Attribute Type）] ペインで次の設定を行います。

a) タイプとして *perapp* を入力します。

タイプは *perapp* にする必要があります。これは、アプリケーション単位 VPN に関して AnyConnect クライアントが認識する唯一の属性タイプであるためです。

b) 任意の説明を入力します。

ステップ 3 [OK] をクリックして、このペインを閉じます。

ステップ 4 [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）] > [詳細（Advanced）] > [AnyConnect カスタム属性名（AnyConnect Custom Attribute Names）] に移動してカスタム属性を設定します。

ステップ 5 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性名の作成/編集（Create / Edit Custom Attribute Name）] ペインで次の設定を行います。

a) *perapp* 属性タイプを選択します。

b) 名前を入力します。 この名前は、ポリシーにこの属性を割り当てるために使用されます。

c) ポリシー ツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

各値は 420 文字を超えることはできません。値がこの長さを超える場合は、追加の値コンテンツ用の複数の値を追加します。設定値は AnyConnect クライアントに送信される前に連結されます。

ASA のポリシーへのカスタム属性の割り当て

perapp カスタム属性は、グループ ポリシーまたはダイナミック アクセス ポリシーに割り当てることができます。

手順

ステップ 1 次のように ASA でポリシーを開きます。

- グループポリシーの場合、[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）]>[グループポリシー（Group Policies）]>[追加/編集（Add / Edit）]>[詳細（Advanced）]>[AnyConnect クライアント（AnyConnect Client）]>[カスタム属性（Custom Attributes）] に移動します。
- ダイナミック アクセス ポリシーの場合、[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）]>[ダイナミックアクセスポリシー（Dynamic Access Policies）]>[追加/編集（Add / Edit）] に移動します。[アクセス/認証ポリシーの属性（Access/Authorization Policy Attributes）] セクションで、[AnyConnect カスタム属性（AnyConnect Custom Attributes）] タブを選択します。

ステップ 2 既存の属性の [追加（Add）] または [編集（Edit）] をクリックして、[カスタム属性の作成/編集（Create / Edit Custom Attribute）] ペインを開きます。

ステップ 3 ドロップダウン リストから定義済みの *perapp* 属性タイプを選択します。

ステップ 4 [値の選択（Select Value）] を選択し、ドロップダウン リストから定義済みの値を選択します。

ステップ 5 [OK] をクリックして、開いた設定ペインを閉じます。

AnyConnect VPN プロファイルでのモバイル デバイス接続の設定

AnyConnect VPN クライアント プロファイルは XML ファイルであり、クライアントの動作を指定し、VPN 接続エントリを識別します。各接続エントリは、このエンドポイント デバイスにアクセス可能なセキュア ゲートウェイとその他の接続属性、ポリシー、および制約を指定します。モバイル デバイスのホスト接続エントリを含む VPN クライアント プロファイルを作成するには、AnyConnect プロファイル エディタを使用します。

ASA からモバイル デバイスに配信される VPN プロファイルで定義された接続エントリを、ユーザが変更したり削除したりすることはできません。ユーザは、手動で作成する接続エントリだけを変更および削除できます。

AnyConnect は、モバイル デバイス上で一度に 1 つの現在の VPN クライアント プロファイルのみ維持します。自動または手動の VPN 接続を開始すると、現在のプロファイルが新しい VPN プロファイルによって完全に置き換えられます。ユーザが手動で現在のプロファイルを削除した場合、そのプロファイルは削除され、そのプロファイルに定義されているすべての接続エントリが削除されます。

手順

ステップ 1 基本的な VPN アクセスを設定します。

次の例外を考慮した、デスクトップ/モバイルエンドポイントに共通の手順については、「VPN アクセスの設定 （69 ページ）」を参照してください。

プロファイル属性	Exception
自動再接続	Apple iOS 以外のすべてのプラットフォームでは、自動再接続の指定に関係なく、AnyConnect Mobile は常に ReconnectAfterResume を試行します。 Apple iOS の場合のみ、[中断時に接続解除（Disconnect On Suspend）] がサポートされています。[中断時に接続解除（Disconnect On Suspend）] を選択すると、AnyConnect は切断してから、VPN セッションに割り当てられたリソースを解放します。ユーザの手動接続またはオンデマンド接続（設定されている場合）に応答する形でのみ再接続されます。
ローカル LAN へのアクセス	AnyConnect Mobile はローカル LAN アクセス設定を無視し、クライアント プロファイルの設定に関係なく常にローカル LAN アクセスを許可します。

ステップ 2 モバイル固有の属性を設定します。

a) VPN クライアント プロファイルで、ナビゲーション ペインの [サーバ リスト（Server List）] を選択します。

b) リストに新しいサーバ エントリを追加するには、[追加（Add）] を選択するか、リストからサーバ エントリを選択し、サーバ リストの [エントリ（Entry）] ダイアログボックスを開くには、[編集（Edit）] をクリックします。

c) 「AnyConnect プロファイル エディタのモバイル設定 （54 ページ）」の説明に従ってモバイル固有のパラメータを設定します。

d) [OK] をクリックします。

ステップ 3 次のいずれかの方法で VPN クライアント プロファイルを配布します。

- VPN 接続のモバイル デバイス設定にクライアント プロファイルをアップロードするように ASA を設定します。

  VPN クライアント プロファイルを ASA にインポートして、グループ ポリシーに関連付ける方法については、「AnyConnect プロファイル エディタ （31 ページ）」の章を参照してください。

- クライアント プロファイルをインポートするために、ユーザに AnyConnect URI リンクを提供します。（Android および Apple iOS のみ）

  ユーザにこのタイプの展開手順を提供するには、「VPN クライアント プロファイルのインポート （28 ページ）」を参照してください。

- モバイル デバイスで [プロファイル管理（Profile Management）] を使用して、AnyConnect プロファイルをユーザがインポートするようにします。（Android および Apple iOS のみ）

  デバイス固有の手順については、該当するモバイル デバイスのユーザ ガイドを参照してください。

URI ハンドラを使用した AnyConnect アクションの自動化

AnyConnect の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で AnyConnect にアクション要求を渡すようにします。AnyConnect ユーザ設定プロセスを簡素化するため、URI を Web ページまたは電子メール メッセージにリンクとして埋め込み、これらにアクセスする方法をユーザに提供します。

始める前に

- AnyConnect の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で AnyConnect にアクション要求を渡すようにします。

  管理された環境の場合：

  外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。これらを使用する場合、URI の処理に関連付けられたプロンプトに応答する方法をユーザに知らせる必要があります。MDM で設定値を構成するキーと値は次のとおりです。

  キー - *UriExternalControl*

  値 - [有効（Enabled）]、[プロンプト（Prompt）]、または [無効（Disabled）]

  （注） 構成設定を MDM で実行してユーザ デバイスにプッシュすると、ユーザによるこの設定の変更は許可されなくなります。

管理されていない環境の場合：

AnyConnect アプリケーションで処理する URI はデフォルトで無効です。モバイル デバイスのユーザは、[外部制御（External Control）] アプリケーション設定を [有効（Enable）] または[プロンプト（Prompt）] に設定することで、この機能を許可します。外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。

- URI ハンドラ パラメータ値を入力する場合、URL エンコーディングを使用する必要があります。このリンクで示すようなツールを使用して、アクション要求を符号化します。次の例も参照してください。
- URI では `%20` はスペース、`%3A` はコロン（:）、`%2F` はスラッシュ（/）、`%40` はアンパサンド（@）を表します。
- URI のスラッシュは任意です。

次のいずれかのアクションをユーザに指定します。

VPN 接続エントリの生成

この AnyConnect URI ハンドラを使用して、ユーザの AnyConnect 接続エントリの生成を簡略化します。

anyconnect:[//]**create**[/]**?name**=説明**&host**=サーバ アドレス[**&Parameter1**=値**&Parameter2**=値 ...]

ガイドライン

- *host* パラメータは必須です。その他すべてのパラメータはオプションです。アクションがデバイスで実行されると、AnyConnect は、その *name* と *host* に関連付けられた接続エントリに入力するすべてのパラメータ値を保存します。
- デバイスに追加する各接続エントリの個別のリンクを使用します。単一のリンクで複数の作成接続エントリ アクションを指定することはサポートされていません。

パラメータ

- **name**：AnyConnect のホーム画面の接続リストおよび AnyConnect 接続エントリの [説明（Description）] フィールドに表示される接続エントリの一意の名前。AnyConnect は名前が一意の場合のみ応答します。接続リストに収まるように、半角 24 文字以内にすることを推奨します。テキストをフィールドに入力する場合、デバイスに表示されたキーボード上の任意の文字、数字、または記号を使用します。文字の大文字と小文字が区別されます。
- **host**：接続に使用する ASA のドメイン名、IP アドレス、またはグループ URL を入力します。AnyConnect はこのパラメータの値を AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドに挿入します。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol** （任意、指定されていない場合は、デフォルトの SSL になる）：この接続に使用される VPN プロトコル。有効な値は次のとおりです。
  - SSL
  - IPsec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication** （任意、プロトコルが IPsec のみを指定している場合に適用、デフォルトは EAP-AnyConnect）：IPsec VPN 接続で使用される認証方式。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA

- **ike-identity** （authentication が EAP-GTC、EAP-MD5、EAP-MSCAPv2 に設定されている場合に必要）：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 に設定されているときの IKE ID。このパラメータは、他の認証設定に使用されたときに無効になります。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam** （任意、Apple iOS にのみ適用）：デバイスの起動後または接続タイプ（EDGE、3G、Wi-Fi など）の変更後、再接続にかかる時間を制限するかどうかを決定します。このパラメータは、データ ローミングまたは複数のモバイル サービス プロバイダーの使用には影響しません。有効な値は次のとおりです。
  - true：（デフォルト）このオプションでは、VPN アクセスが最適化されます。AnyConnect は値 ON を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドに挿入します。AnyConnect が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定では、アプリケーションは VPN への持続的な接続に依存します。AnyConnect は、再接続にかかる時間を制限しません。
  - false：このオプションでは、バッテリ寿命が最適化されます。AnyConnect はこの値を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドの OFF 値と関連付けます。AnyConnect が接続を失った場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias** （任意）：システムの証明書ストアから AnyConnect の証明書ストアに証明書をインポートします。このオプションは、Android のモバイル プラットフォーム専用です。

名前の付いた証明書がまだシステムストアに存在しない場合、ユーザは証明書を選択してインストールするように求められ、その後、AnyConnect ストアへのコピーを許可または拒否するかを求めるプロンプトが表示されます。モバイルデバイスで外部制御を有効にする必要があります。

次の例では、IP アドレスが *vpn.example.com* に設定され、認証用に *client* という名前の証明書が割り当てられている *SimpleExample* という名前の新しい接続エントリを作成します。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
```

- **usecert** （任意）：ホストへの VPN 接続を確立するときに、デバイスにインストールされているデジタル証明書を使用するかどうかを決定します。有効な値は次のとおりです。
  - true（デフォルト設定）：ホストとの VPN 接続を確立するときに自動証明書選択を無効化します。[証明書（Certificate）] フィールドを自動にする certcommonname 値を指定することなしに usecert を true に返し、接続時に AnyConnect 証明書ストアから証明書を選択します。
  - false：自動証明書の選択を無効化します。

```
anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
```

- **certcommonname** （任意、ただし usecert パラメータは必要）：デバイスにあらかじめインストールされた有効な証明書の共通名を照合します。AnyConnect はその値を AnyConnect 接続エントリの [証明書（Certificate）] フィールドに挿入します。

  デバイスにインストールされているこの証明書を表示するには、**[診断（Diagnostics）] > [証明書（Certificates）]** をタップします。host によって要求された証明書を表示するには、スクロールが必要な場合があります。証明書から読み取った共通名パラメータ、およびその他の値を表示するには、詳細表示ボタンをタップします。

- **useondemand** （任意、Apple iOS だけに適用、usecert、certcommonname パラメータ、および下記のドメイン指定が必要）：Safari などのアプリケーションが、VPN 接続を開始できるかどうか決定します。有効な値は次のとおりです。
  - false（デフォルト）：アプリケーションは VPN 接続を開始できません。このオプションは、DNS 要求を行うアプリケーションが VPN 接続をトリガーしないようにする唯一の手段です。AnyConnect は、AnyConnect 接続エントリの Connect on Demand フィールドに OFF 値でこのオプションを関連付けます。
  - true：アプリケーションは Apple iOS を使用して VPN 接続を開始できます。useondemand パラメータを true に設定すると、AnyConnect は値 ON を AnyConnect 接続エントリの [オンデマンド接続（Connect on Demand）] フィールドに挿入します。
    （useondemand=true の場合、domainlistalways パラメータまたは domainlistifneeded パラメータは必須）

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever** （オプション、useondemand=true が必要）：Connect on Demand 機能の使用を不適格とするために、一致を評価するドメインをリストにまとめます。このリスト

は、ドメイン要求の一致を評価する場合に AnyConnect が最初に使用するリストです。ドメイン要求が一致すると、ドメイン要求は無視されます。AnyConnect はこのリストを AnyConnect 接続エントリの [接続しない（Never Connect）] フィールドに挿入します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動VPN接続を許可しない場合などが考えられます。値は `www.example.com` などのように指定します。

- **domainlistalways**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：Connect on Demand 機能について一致を評価するドメインをリストします。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が 2 番目に使用するリストです。アプリケーションがこのパラメータで指定されたいずれかのドメインへのアクセスを要求し、VPN 接続がまだ行われていない場合、Apple iOS は VPN 接続を確立しようとします。AnyConnect はこのリストを AnyConnect 接続エントリの [常に接続（Always Connect）] フィールドに挿入します。値リストの例は `email.example.com,pay.examplecloud.com` です。
- **domainlistifneeded** （useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：DNS エラーが発生した場合、AnyConnect はこのリストに対してドメイン要求が一致しているかどうか評価します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。AnyConnect はこのリストを AnyConnect 接続エントリの [必要に応じて接続（Connect if Needed）] フィールドに挿入します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

カンマで区切ったリストを使用して、複数のドメインを指定します。Connect-on-Demand の規則は IP アドレスではなく、ドメイン名のみサポートしています。ただし AnyConnect は、各リスト エントリのドメイン名形式について次のような柔軟性があります。

一致（Match）	指示	エントリの例	一致する例	一致しない例
プレフィックスおよびドメイン名が正確に一致。	プレフィックス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org

一致（Match）	指示	エントリの例	一致する例	一致しない例
ドメイン名は正確に一致し、プレフィックスは任意。先頭にドットを付けると、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net anytext.	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

VPN 接続の確立

VPN に接続してユーザが容易に VPN 接続を確立できるようにするには、この AnyConnect URI ハンドラを使用します。また、URI に次のタスクを実行するための追加情報を埋め込むことができます。

- ユーザ名とパスワードの事前入力
- 二重認証用のユーザ名とパスワードの事前入力
- ユーザ名とパスワードの事前入力および接続プロファイル エイリアスの指定

このアクションには name または host のいずれかのパラメータが必要ですが、次の構文のいずれかを使用して両方を指定することもできます。

anyconnect:[//]**connect**[/]**?**[**name=**説明|**host=**サーバ アドレス] [**&Parameter1**=値**&Parameter2**=値..]

または

anyconnect:[//]**connect**[/]**?name=**説明**&host=**サーバ アドレス [**&Parameter1**=値**&Parameter2**=値..]

ガイドライン

- ステートメントのすべてのパラメータ値がデバイスの AnyConnect 接続エントリに一致する場合、AnyConnect は接続を確立するために残りのパラメータを使用します。

- ステートメントのすべてのパラメータが接続エントリのパラメータと一致せず、name パラメータが一意の場合、新しい接続エントリが生成され、VPN 接続が試行されます。
- URI を使用して、VPN 接続を確立するためにワンタイム パスワード（OTP）インフラストラクチャとの組み合わせのみ使用する必要がある場合、パスワードを指定します。

パラメータ

- **name**：AnyConnect ホーム ウィンドウの接続リストに表示される、接続エントリの名前。AnyConnect はこの値を AnyConnect 接続エントリの [説明（Description）] フィールドに対して評価し、前回の手順を使用してデバイスに接続エントリを作成した場合、name とも呼ばれます。この値は大文字と小文字が区別されます。
- **host**：AnyConnect 接続エントリの [サーバアドレス（Server Address）] フィールドと一致させるには、ASA のドメイン名、IP アドレス、またはグループ URL を入力します。前回の手順を使用してデバイスに接続エントリを生成した場合、host とも呼ばれます。

  グループ URL は、[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）] > [詳細（Advanced）] > [グループ エイリアス/グループ URL（Group Alias/Group URL）] > [グループ URL（Group-URL）] を選択して、ASDM に設定されます。
- **onsuccess**：接続が正常である場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が接続状態に遷移するとき、または anyconnect:close コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が遷移するとき、またはすでに接続状態であるときに表示される URL を指定します。複数の onsuccess アクションを指定できます。AnyConnect は、Android デバイスでの接続が成功した後で常に GUI を閉じます。
- **onerror**：接続に失敗した場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が失敗したとき、または anyconnect:close コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が失敗したときに表示される URL を指定します。複数の onerror アクションを指定できます。AnyConnect は、Android デバイスでの接続が失敗した後で常に GUI を閉じます。
- **prefill_username**：connect URI にユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_password**：connect URI にパスワードを指定し、接続プロンプトに自動入力します。このフィールドは、ワンタイム パスワード用に設定した接続プロファイルでの使用のみとしてください。

- **prefill_secondary_username**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_secondary_password**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名のパスワードを指定し、接続プロンプトに自動入力します。
- **prefill_group_list**：これは、[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）] > [詳細（Advanced）] > [グループエイリアス/グループURL（Group Alias/Group URL）] > [接続エイリアス（Connection Aliases）] を選択して、ASDM で定義されている接続エイリアスです。

例

- URI に接続名およびホスト名またはグループ URL を入力します。

```
anyconnect://connect/?name=Example
```

```
anyconnect:connect?host=hr.example.com
```

```
anyconnect:connect?name=Example&host=hr.example.com
```

```
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 成功または失敗に対するアクションの指定

  connect アクションの結果に基づいて特定の URL ベースを開始するために、onsuccess または onerror パラメータを使用します。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  Android では複数の onsuccess アクションを指定できます。

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  Apple iOS デバイスでは、onsuccess パラメータまたは onerror パラメータで anyconnect://close コマンドを使用して、AnyConnect GUI を閉じることができます。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- URI での接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 接続情報の指定、ユーザ名とパスワードの自動入力、および接続プロファイルエイリアスの指定：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

VPN からの接続解除

VPN からユーザの接続を解除するには、この AnyConnect URI ハンドラを使用します。

anyconnect:[//]**disconnect**[/]**&onsuccess=**URL

パラメータ

onsuccess パラメータは、Android デバイスだけに適用されます。この接続が解除されるとき、またはすでに接続解除状態であるときに表示される URL を指定します。

例

```
anyconnect:disconnect
```

証明書のインポート

このURIハンドラ コマンドを使用して、PKCS12符号化証明書バンドルをエンドポイントにインポートします。AnyConnectクライアントは、エンドポイントにインストールされたPKCS12符号化証明書を使用して自らASAに認証を行います。PKCS12証明書タイプのみをサポートします。

anyconnect:[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

パラメータ

- **type**：PKCS12 証明書タイプのみをサポートします。
- **uri**：証明書がある場所の URL エンコード ID。

例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

VPN クライアント プロファイルのインポート

AnyConnect クライアントにクライアント プロファイルを配布するため、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=profile&uri=***filename.xml*

例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

AnyConnect UI とメッセージのローカライズ

AnyConnect クライアントをローカライズするには、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=***ServerAddress*

パラメータ

インポート アクションには、すべてのパラメータが必要です。

- **type**：インポートのタイプ（この場合はローカリゼーション）。
- **lang**：anyconnect.po ファイルで指定されて言語を表す 2 文字または 4 文字の言語タグ。たとえば、言語タグは単純に「French」なら fr、「Canadian French」なら fr-ca となります。
- **host**：AnyConnect 接続エントリの [サーバアドレス（Server Address）] フィールドと一致させるには、ASA のドメイン名または IP アドレスを入力します。

例

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

モバイルデバイスでのAnyConnectのトラブルシューティング

始める前に

モバイル デバイスでロギングを有効にし、適切なユーザ ガイドのトラブルシューティングの指示に従ってください。

- Cisco AnyConnect Secure Mobility Client の Android 向けユーザガイド リリース 4.6

これらの指示に従っても問題が解決しない場合は、次のことを試してください。

手順

ステップ 1 同じ問題がデスクトップ クライアントまたは別のモバイル OS で発生するかどうかを確認します。

ステップ 2 適切なライセンスが ASA にインストールされていることを確認します。

ステップ 3 証明書認証が失敗する場合は、次のことを確認してください。

a) 適切な証明書が選択されていることを確認します。

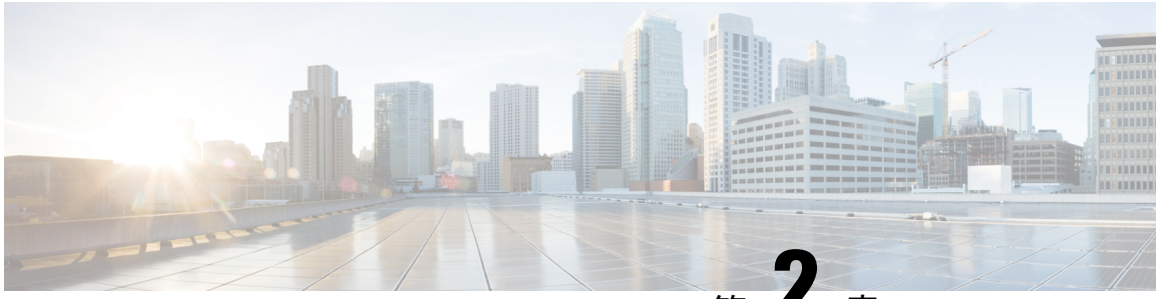
b) デバイスのクライアント証明書に Extended Key Usage として Client Authentication があることを確認します。
c) AnyConnect プロファイルの証明書一致規則によってユーザの選択した証明書を除外されていないことを確認します。

   ユーザが証明書を選択しても、プロファイルのフィルタリングルールに一致しなければ認証には使用されません。

d) 認証メカニズムで ASA に関連するアカウンティングポリシーが使用されている場合、ユーザが正常に認証できることを確認します。
e) 証明書のみの認証を使用しようとしている場合に認証画面が表示されたら、グループ URL を使用するよう接続を設定し、トンネルグループのセカンダリ認証が設定されていないことを確認します。

次のタスク

それでも問題が解決されない場合は、クライアントのロギングを有効にし、ASA のデバッグロギングを有効にします。詳細については、適切なリリースの Cisco ASA 5500-X Series Next-Generation Firewall 構成ガイド を参照してください。



第 2 章

AnyConnect プロファイル エディタ

- プロファイル エディタについて （31 ページ）
- AnyConnect VPN プロファイル （32 ページ）
- AnyConnect ローカル ポリシー （62 ページ）

プロファイル エディタについて

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージには、すべてのオペレーティング システム用のプロファイル エディタが含まれています。AnyConnect クライアント イメージを ASA にロードすると、ASDM はプロファイル エディタをアクティブ化します。ローカルまたはフラッシュからクライアント プロファイルをアップロードできます。

複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージのクライアント プロファイル エディタがアクティブ化されます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

Windows で動作するスタンドアロン プロファイル エディタもあります。

ASDM からの新しいプロファイルの追加

（注） クライアント プロファイルを作成する前に、まずクライアント イメージをアップロードする必要があります。

プロファイルが AnyConnect の一部としてエンドポイント上の管理者定義のエンド ユーザ要件および認証ポリシーに展開され、これにより、エンド ユーザが設定済みのネットワーク プロファイルを使用できるようになります。1 つ以上のプロファイルを作成および設定するには、プロファイル エディタを使用します。AnyConnect には ASDM の一部であるプロファイル エディタが、スタンドアロン Windows プログラムとして組み込まれています。

新しいクライアント プロファイルを ASDM から ASA に追加するには、次の手順を実行します。

手順

ステップ 1 ASDM で、**[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 クライアント プロファイル（AnyConnect Client Profile）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 [プロファイルの使用（Profile Usage）] ドロップダウン リストから、プロファイルを作成するモジュールを選択します。

ステップ 5 （任意）[プロファイルの場所（Profile Location）] フィールドで [フラッシュの参照（Browse Flash）] をクリックし、ASA の XML ファイルのデバイス ファイル パスを選択します。

ステップ 6 （任意）スタンドアロン エディタを使用してプロファイルを作成した場合、[アップロード（Upload）] をクリックして、そのプロファイル定義を使用します。

ステップ 7 （任意）ドロップダウン リストから AnyConnect グループ ポリシーを選択します。

ステップ 8 [OK] をクリックします。

AnyConnect VPN プロファイル

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect プロファイルで有効になります。これらのプロファイルには、コア クライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、ISE ポスチャ、カスタマー エクスペリエンス フィードバック、Web セキュリティの構成設定が含まれています。ASA は、AnyConnect のインストールと更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

ASA または ISE は、すべての AnyConnect ユーザにグローバルにプロファイルを展開するか、ユーザのグループ ポリシーに基づいて展開するように設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのプロファイル ファイルを持ちます。場合により、1 人のユーザに複数の VPN プロファイルを割り当てることがあります。複数の場所で作業するユーザには、複数の VPN プロファイルが必要になります。

一部のプロファイル設定は、ユーザのコンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、AnyConnect クライアントが、クライアント GUI の [プリファレンス（Preferences）] タブにユーザ制御可能設定を表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

AnyConnect プロファイル エディタ、プリファレンス（Part 1）

- [Start Before Logon の使用（Use Start Before Logon）]（Windows のみ）：Windows のログイン ダイアログボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。認証後、ログイン ダイアログボックスが表示され、ユーザは通常どおりログインします。

- [事前接続メッセージの表示（Show Pre-connect Message）]：管理者は、ユーザが初めて接続を試行する前にワンタイム メッセージを表示させることができます。たとえば、メッセージを表示して、ユーザにスマート カードをリーダに挿入するよう促すことができます。このメッセージは、AnyConnect メッセージ カタログに表示され、ローカライズされています。

- [証明書ストア（Certificate Store）]：AnyConnect がどの証明書ストアで証明書を保存し、読み取るかを制御します。セキュア ゲートウェイは、適切に設定し、複数の証明書認証の組み合わせのうちどれが特定の VPN 接続で許容されるかをクライアントに指定する必要があります。

  VPN プロファイルの CertificateStore 設定の値は、セキュア ゲートウェイに許容される証明書のタイプによって異なります。証明書のタイプは、2 ユーザ証明書か、1 マシンおよび 1 ユーザ証明書のどちらかです。

  macOS 上で AnyConnect がアクセスできる証明書ストアをさらに絞りこめるようにするには、Windows 用または macOS 用のドロップダウンから証明書ストアを設定できます。macOS のための新しいプロファイル プリファレンスは CertificateStoreMac といい、次の追加された値をサポートします。

  - [すべて（All）]（Windows 用）：1 マシンおよび 1 ユーザ証明書が ASA 設定によって許容されます。
  - [ユーザ（User）]（Windows 用）：2 ユーザ証明書が ASA 設定によって許容されます。
  - [すべて（All）]（macOS 用）：利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。
  - [システム（System）]（macOS 用）：macOS システム キーチェーンおよびシステム ファイル/PEM ストアからの証明書のみを使用します。
  - [ログイン（Log in）]（macOS 用）：ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

- [証明書ストアの上書き（Certificate Store Override）]：ユーザに自分のデバイスに対する管理者権限がない場合、管理者は Windows マシン証明書ストアで証明書を検索するように AnyConnect に指示できます。証明書ストアの上書きは、デフォルトでは UI プロセスによって接続が開始される SSL にのみ適用されます。IPSec/IKEv2 を使用している場合、AnyConnect プロファイルのこの機能は適用されません。

（注） マシン証明書を使用して Windows に接続するには、このオプションが有効にされている事前展開されたプロファイルが必要です。接続する前に Windows デバイスにこのプロファイルが存在しない場合、証明書はマシン ストアにアクセスできず、接続は失敗します。

- True：AnyConnect は、Windows マシン証明書ストア内の証明書を検索します。CertificateStore を [すべて（all）] に設定する場合、CertificateStoreOverride は true に設定する必要があります。
- False：AnyConnect は、Windows マシン証明書ストア内の証明書を検索しません。

- AutomaticCertSelection：セキュア ゲートウェイで複数証明書の認証を設定するときは、この値を true に設定する必要があります。
- [起動時に自動接続（Auto Connect on Start）]：AnyConnect の起動時に、プロファイルで指定されたセキュア ゲートウェイまたはクライアントが最後に接続していたゲートウェイとの VPN 接続が自動的に確立されます。
- [接続時に最小化（Minimize On Connect）]：VPN 接続の確立後、AnyConnect GUI が最小化されます。
- [ローカル LAN アドレス（Local LAN Access）]：ASA への VPN セッション中にリモート コンピュータへ接続したローカル LAN に対してユーザが無制限にアクセスできるようになります。

（注） ローカル LAN アクセスを有効にすると、パブリック ネットワークからユーザ コンピュータを経由して、社内ネットワークにセキュリティの脆弱性が生じる可能性があります。代替手段として、セキュリティ アプライアンス（バージョン 8.4(1) 以降）で、デフォルト グループ ポリシーに含まれている AnyConnect クライアント ローカル印刷ファイアウォール ルールを使用した SSL クライアント ファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [プリファレンス（Part 2）（Preferences (Part 2)）] で、[自動 VPN ポリシー（Automatic VPN Policy）]、[常にオン（Always on）]、および [VPN の接続解除を許可（Allow VPN Disconnect）] も有効にする必要があります。

- [キャプティブポータル検出を無効にする（Disable Captive Portal Detection）]：AnyConnect クライアントが受信する証明書の共通名が、ASA 名と一致しない場合、キャプティブ ポータルが検出されます。この動作により、ユーザによる認証が促されます。自己署名証明書を使用する一部のユーザは、HTTP キャプティブ ポータルで保護されている企業リソース

への接続を有効にすることを望むことがあるため、[キャプティブポータル検出を無効にする（Disable Captive Portal Detection）] チェックボックスをオンにする必要があります。管理者は、このオプションをユーザが設定できるようにするかどうかを判断し、判断に基づいてチェックボックスをオンにすることもできます。ユーザが設定できるようにした場合は、AnyConnect Secure Mobility Client UI の [プリファレンス（Preferences）] タブにチェックボックスが表示されます。

- [自動再接続（Auto Reconnect）]：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。[自動再接続（Auto Reconnect）] を無効にすると、接続解除の原因にかかわらず、再接続は試行されません。

（注） 自動再接続は、ユーザがクライアントの動作を制御するシナリオで使用します。この機能は、AlwaysOn ではサポートされません。

  - **自動再接続の動作**
    - DisconnectOnSuspend：AnyConnect では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムの再開後も再接続は試行されません。
    - ReconnectAfterResume（デフォルト）：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。

- [自動更新（Auto Update）]：オンにすると、クライアントの自動アップデートが有効になります。[ユーザ制御可（User Controllable）] チェックボックスをオンにすると、クライアントのこの設定を無効にできます。
- [RSA セキュア ID 連携（RSA Secure ID Integration）]（Windows のみ）：ユーザが RSA とどのように対話するかを制御します。デフォルトでは、AnyConnect が RSA の適切な対話方法を決定します（自動設定：ソフトウェア トークンとハードウェア トークンの両方を受け入れます）。
- [Windows ログインの強制（Windows Logon Enforcement）]：Remote Desktop Protocol（RDP）セッションから VPN セッションを確立することを許可します。スプリット トンネリングはグループ ポリシーで設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は AnyConnect により解除されます。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。
  - [シングル ローカル ログイン（Single Local Logon）]（デフォルト）：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザがログインしている場合でも、ローカル ユーザが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

- [シングル ログイン（Single Logon）]：VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

（注） 複数同時ログオンはサポートされません。

- [Windows VPN 確立（Windows VPN Establishment）]：クライアント PC にリモート ログインしたユーザが VPN 接続を確立した場合の AnyConnect の動作を決定します。設定可能な値は次のとおりです。
  - [ローカルユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect と同じ機能です。
  - [リモートユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。リモートユーザが VPN 接続を終了せずにリモート ログイン セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。
- [Linux ログインの適用（Linux Logon Enforcement）]：SSH セッションから VPN セッションを確立できます。グループ ポリシーにスプリット トンネリングを設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は AnyConnect により解除されます。接続がリモートユーザによって確立されていた場合、そのリモートユーザがログオフすると、VPN 接続は終了します。
  - [シングル ローカル ログイン（Single Local Logon）]（デフォルト）：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザがログインしている場合でも、ローカル ユーザが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

- [シングル ログイン（Single Logon）]：VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

（注） 複数の同時ログインは、単一のログインセッションとして処理されます。ユーザにローカルとリモートの両方のログインセッションがある場合、ユーザはローカル ユーザとして扱われます。

- [Linux VPN 確立（Linux VPN Establishment）]：SSH を使用してクライアント PC にログインしたユーザが VPN 接続を確立した場合の AnyConnect の動作を決定します。設定可能な値は次のとおりです。
  - [ローカル ユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは VPN 接続を確立できません。
  - [リモート ユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。
- **[スマートカードのピンのクリア（Clear SmartCard PIN）]**
- [サポートされている IP プロトコル（IP Protocol Supported）]：IPv4 アドレスおよび IPv6 アドレスの両方で AnyConnect を使用して ASA に接続しようとしているクライアントの場合、AnyConnect は接続の開始に際してどの IP プロトコルを使用するか決定する必要があります。デフォルトで、AnyConnect は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、IPv6 を使用して接続を開始しようとします。

  このフィールドでは、最初の IP プロトコルとフォールバックの順序を設定します。
  - [IPv4]：ASA に対して IPv4 接続のみ可能です。
  - [IPv6]：ASA に対して IPv6 接続のみ可能です。
  - [IPv4, IPv6]：最初に ASA に IPv4 接続しようとします。クライアントが IPv4 を使用して接続できない場合、IPv6 接続をしようとします。

- [IPv6, IPv4]：最初に ASA に IPv6 接続しようとします。クライアントが IPv6 を使用して接続できない場合、IPv4 接続をしようとします。

（注） IPv4 から IPv6、IPv6 から IPv4 プロトコルへのフェールオーバーも VPN セッション中に行うことができます。プライマリ IP プロトコルが失われると、可能な場合に、セカンダリ IP プロトコルを介して VPN セッションが再確立されます。

AnyConnect プロファイル エディタ、プリファレンス（Part 2）

- [自動証明書選択の無効化（Disable Automatic Certificate Selection）]（Windows のみ）：クライアントによる自動証明書選択を無効にし、ユーザに対して認証証明書を選択するためのプロンプトを表示します。

  関連項目：証明書選択の設定

- [プロキシ設定（Proxy Settings）]：プロキシ サーバへのクライアント アクセスを制御するために AnyConnect プロファイルにポリシーを指定します。これは、プロキシ設定によってユーザが社内ネットワークの外からトンネルを確立できない場合に使用します。
  - [ネイティブ（Native）]：クライアントは、AnyConnect によって以前に設定されたプロキシ設定とブラウザに設定されたプロキシ設定の両方を使用します。グローバル ユーザ プリファレンスに設定されたプロキシ設定は、ブラウザのプロキシ設定に追加されます。
  - [プロキシを無視（IgnoreProxy）]：ユーザのコンピュータのブラウザのプロキシ設定を無視します。
  - [上書き（Override）]：パブリック プロキシ サーバのアドレスを手動で設定します。パブリック プロキシは、Linux でサポートされている唯一のプロキシです。Windows も、パブリック プロキシをサポートしています。[ユーザ制御可（User Controllable）] になるようにパブリック プロキシ アドレスを設定できます。

- [ローカルプロキシ接続を許可（Allow Local Proxy Connections）]：デフォルトでは、Windows ユーザは AnyConnect でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシ サービスを介して VPN セッションを確立するようになっています。ローカル プロキシ接続のサポートを無効にする場合は、このパラメータをオフにします。トランスペアレント プロキシ サービスを提供する要素の例として、一部のワイヤレス データ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェアに備えられたネットワーク コンポーネントなどがあります。

- [最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）]（OGS）、（IPv4 クライアントのみ）：AnyConnect では、ラウンド トリップ時間（RTT）に基づいて接続または再接続に最適なセキュア ゲートウェイが特定され、それが選択されます。これによ

り、ユーザが介入することなくインターネット トラフィックの遅延を最小限に抑えることができます。OGS はセキュリティ機能ではなく、セキュア ゲートウェイ クラスタ間またはクラスタ内部でのロード バランシングは実行されません。OGS のアクティブ化/非アクティブ化を制御し、エンドユーザがこの機能そのものを制御できるようにするかどうかを指定します。クライアント GUI の [接続（Connection）] タブにある [接続先（Connect To）] ドロップダウン リストには [自動選択（Automatic Selection）] が表示されます。

- [一時停止時間しきい値（時間）（Suspension Time Threshold (hours)）]：新しいゲートウェイ選択の計算を呼び出す前に VPN を一時停止しておく必要がある最小時間を（時間単位で）入力します。次の設定可能パラメータ（パフォーマンス向上しきい値（Performance Improvement Threshold））と組み合わせてこの値を最適化することで、最適なゲートウェイの選択と、クレデンシャルの再入力を強制する回数の削減の間の適切なバランスを見つけることができます。
- [パフォーマンス向上しきい値（%）（Performance Improvement Threshold (%)）]：システムの再開後にクライアントが別のセキュア ゲートウェイに再接続する際の基準となるパフォーマンス向上率。特定のネットワークに対してこれらの値を調整すれば、最適なゲートウェイを選択することと、クレデンシャルを強制的に入力させる回数を減らすこととの間で適切なバランスを取ることができます。デフォルトは 20% です。

OGS が有効な場合は、この機能の設定をユーザが行えるようにすることも推奨します。

OGS には次の制約事項があります。

- Always-On を設定した状態では動作できません
- 自動プロキシ検出を設定した状態では動作できません。
- プロキシ自動設定（PAC）ファイルを設定した状態では動作できません。
- AAA が使用されている場合は、別のセキュア ゲートウェイへの遷移時にユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。この問題は、証明書を使用すると解消されます。

- [自動 VPN ポリシー（Automatic VPN Policy）]（Windows および macOS のみ）：Trusted Network Detection を有効にして、AnyConnect が信頼ネットワーク ポリシーと非信頼ネットワーク ポリシーに従って VPN 接続をいつ開始または停止するかを自動的に管理できるようにします。無効の場合、VPN 接続の開始および停止は手動でのみ行うことができます。[自動 VPN ポリシー（Automatic VPN Policy）] を設定しても、ユーザは VPN 接続を手動で制御できます。
  - [信頼されたネットワーク ポリシー（Trusted Network Policy）]：ユーザが社内ネットワーク（信頼ネットワーク）に存在する場合に AnyConnect が VPN 接続で自動的に実行するアクション。
    - [接続解除（Disconnect）]（デフォルト）：信頼ネットワークが検出されると VPN 接続が解除されます。
    - [接続（Connect）]：信頼ネットワークが検出されると VPN 接続が開始されます。

- [何もしない（Do Nothing）]：非信頼ネットワークでは動作はありません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。
- [一時停止（Pause）]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は VPN セッションを接続解除するのではなく、一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

- [信頼されていないネットワークポリシー（Untrusted Network Policy）]：ユーザが社内ネットワークの外（非信頼ネットワーク）に存在する場合、AnyConnect により VPN 接続が自動的に開始されます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。
  - [接続（Connect）]（デフォルト）：非信頼ネットワークが検出されると、VPN 接続が開始されます。
  - [何もしない（Do Nothing）]：信頼ネットワークでは動作はありません。このオプションを指定すると、 Always-OnVPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

- [信頼された DNS ドメイン（Trusted DNS Domains）]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。
- [信頼された DNS サーバ（Trusted DNS Servers）]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サーバ アドレス（カンマ区切りの IP アドレス）。たとえば、192.168.1.2, 2001:DB8::1 です。IPv4 または IPv6 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされています。
- **Trusted Servers @ https://<server>[:<port>]**：信頼できる URL として追加するホスト URL。信頼できる証明書を使用してアクセス可能なセキュア Web サーバが、信頼できるサーバとして見なされる必要があります。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼されたDNSサーバを1つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバが定義されていない場合、このフィールドは無効になります。

- [常時接続（Always On）]：対応している Windows または macOS オペレーティング システムのいずれかを実行しているコンピュータにユーザがログインした場合、AnyConnect が VPN へ自動的に接続するかどうかを判断します。コンピュータが信頼ネットワーク内に存在しない場合にはインターネット リソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーを適用できます。グループ ポリシーおよびダイナミック アクセス ポリシーに Always-On VPN パラメータを設定し、ポリシーの割り当てに使用される一致基準に基づいて例外を指定することにより、この設定を上書きすることもできます。AnyConnect ポリシーではAlways-On VPN が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。有効にした後に、追加のパラメータを設定できます。

（注） AlwaysOn は、ユーザによる設定なしで接続が確立し冗長性が動作するシナリオで使用します。そのため、この機能を使用しているときは、[プリファレンス,パート 1（Preferences, part 1）] で自動再接続を有効に設定する必要はありません。

関連項目：Always-Onを使用した VPN 接続の必要性

- [VPN の接続解除を許可（Allow VPN Disconnect）]：AnyConnect でAlways-On VPN セッション用の [接続解除（Disconnect）] ボタンが表示されるようにするかどうかを指定します。VPN セッションの中断後に現在の VPN セッションまたは再接続で問題が発生し、パフォーマンスが低下したなどの理由により、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

  [接続解除（Disconnect）]ボタンを使用すると、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。上述した理由により、[接続解除（Disconnect）] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

- [接続エラー ポリシー（Connect Failure Policy）]：AnyConnect が VPN セッションを確立できない場合（ASA が到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、[Always-On] および [VPN の接続解除を許可（Allow VPN Disconnect）] が有効の

場合にだけ適用されます。[Always-On] を選択した場合、フェールオープン ポリシーはネットワーク接続を許可し、フェールクローズポリシーはネットワーク接続を無効にします。

- [クローズド（Closed）]：VPN が到達不能の場合にネットワーク アクセスを制限します。この設定の目的は、エンドポイントを保護するプライベートネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。
- [オープン（Open）]：VPN が到達不能の場合でもネットワーク アクセスを許可します。

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。このポリシーは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する非常にセキュリティの高い組織向きです。このポリシーでは、スプリットトンネリングによって許可され、ACL によって制限されたすべてのプリンタやテザード デバイスなどのローカル リソース以外のネットワーク アクセスを防止します。ユーザが VPN を越えてインターネットにアクセスする必要がある場合に、セキュア ゲートウェイを利用できないときには、このポリシーを適用すると生産性が低下する可能性があります。AnyConnectは、ほとんどのキャプティブ ポータルを検出します。キャプティブ ポータルを検出できない場合、接続障害クローズドポリシーによりすべてのネットワーク接続が制限されます。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープン ポリシーを使用して Always-On VPN を展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPNユーザに対して接続障害クローズドポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

関連項目：キャプティブ ポータルについて

[接続エラー ポリシー（Connect Failure Policy）] が [クローズド（Closed）] である場合、次の設定を行うことができます。

- [キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]：クライアントによりキャプティブ ポータル（ホットスポット）が検出された

場合、クローズ接続障害ポリシーにより適用されるネットワークアクセスの制限が AnyConnect により解除されます。ホテルや空港では、ユーザがブラウザを開いてインターネットアクセスの許可に必要な条件を満たすことができるようにするため、キャプティブポータルを使用するのが一般的です。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブ ポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。

- [修復タイムアウト（Remediation Timeout）]：AnyConnect によりネットワークアクセスの制限が解除されるまでの時間（分）。このパラメータは、[キャプティブポータルの修復を許可（Allow Captive Portal Remediation）] パラメータがオンになっており、かつクライアントによりキャプティブポータルが検出された場合に適用されます。キャプティブ ポータルの通常の要求を満たすことができるだけの十分な時間を指定します（5 分など）。
- [最新の VPN ローカル リソース ルールを適用（Apply Last VPN Local Resource Rules）]：VPN が到達不能の場合、クライアントでは ASA から受信した最後のクライアントファイアウォールが適用されます。この中には、ローカル LAN 上のリソースへのアクセスを許可する ACL が含まれている場合もあります。

関連項目：接続障害ポリシーの設定

- [手動でのホスト入力を許可する（Allow Manual Host Input）]：ユーザが、AnyConnect UI のドロップダウン ボックスにリストされていない VPN アドレスを入力できるようにします。このチェックボックスをオフにすると、VPN 接続の選択項目は、ドロップダウンボックスに表示されているものに限定され、ユーザによる新しい VPN アドレスの入力が制限されます。
- [PPP 除外（PPP Exclusion）]：PPP 接続上の VPN トンネルの場合、除外ルートを決定するかどうかとその方法を指定します。クライアントでは、セキュア ゲートウェイより先を宛先としてトンネリングされたトラフィックから、このセキュア ゲートウェイを宛先とするトラフィックを除外できます。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。この機能をユーザ設定可能にした場合、ユーザは PPP 除外設定の読み取りや変更を行うことができます。
  - [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
  - [無効（Disabled）]：PPP 除外は適用されません。
  - [上書き（Override）]：同様に PPP 除外を有効にします。自動検出による PPP サーバの IP アドレスの取得に失敗し、PPP 除外をユーザ制御可能として設定した場合に選択します。

[PPP 除外（PPP Exclusion）] を有効にした場合は、次も設定します。

- [PPP 除外サーバ IP（PPP Exclusion Server IP）]：PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレス。

- [スクリプトの有効化（Enable Scripting）]：OnConnect スクリプトおよび OnDisconnect スクリプトがセキュリティ アプライアンスのフラッシュ メモリに存在する場合はそれらを起動します。
  - [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）]：スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプトプロセスを終了します。たとえば、VPN セッションが終了すると、AnyConnect では実行中の OnConnect スクリプトが終了し、クライアントで新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。
  - [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）]：SBL で VPN セッションが確立された場合に OnConnect スクリプトが（存在すれば）起動されるようにします（VPN エンドポイントで Microsoft Windows を実行している場合にのみサポート）。

- [ログオフ時に VPN を保持（Retain VPN On Logoff）]：ユーザが Windows または Mac OS からログオフした場合に、VPN セッションを維持するかどうかを指定します。
  - [ユーザの強制設定（User Enforcement）]：別のユーザがログインした場合に VPN セッションを終了するかどうかを指定します。このパラメータが適用されるのは、[ログオフ時に VPN を保持（Retain VPN On Logoff）] がオンになっており、かつ VPN セッションが確立されている間に元のユーザが Windows または Mac OS X からログオフした場合のみです。

- [認証タイムアウト値（Authentication Timeout Values）]：デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。10 ～ 120 の範囲で秒数を入力します。

AnyConnect プロファイル エディタのバックアップ サーバ

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定できます。ユーザが選択したサーバで障害が発生した場合、クライアントはリストの先頭にある最適なサーバのバックアップに接続しようとします。それが失敗した場合、クライアントは選択結果の順序に従って [最適なゲートウェイの選択（Optimal Gateway Selection）] リストの残りの各サーバを試します。

（注） ここで設定するバックアップ サーバは、「AnyConnect プロファイル エディタのサーバ リストの追加/編集 （52 ページ）」でバックアップ サーバが定義されていないときに**のみ**、試行されます。サーバのリストで設定されるサーバが優先され、ここにリストされているバックアップ サーバは上書きされます。

[ホスト アドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

AnyConnect プロファイル エディタの証明書照合

このペインでは、クライアント証明書の自動選択の詳細設定に使用できるさまざまな属性の定義を有効にします。

証明書一致基準を指定しない場合、AnyConnect は、次の証明書照合ルールを適用します。

- キーの使用状況：Digital_Signature
- 拡張キーの使用状況：Client Auth

仕様に一致する任意の条件がプロファイルで作成される場合、プロファイルに明記されない限り、上記一致ルールのいずれも適用されません。

- [キーの使用状況（Key Usage）]：受け入れ可能なクライアント証明書を選択する場合は、次のような証明書キー属性を使用できます。
  - Decipher_Only：データを復号化します。他のビットは設定されません（Key_Agreement は除く）。
  - Encipher_Only：データを暗号化します。他のビットは設定されません（Key_Agreement は除く）。
  - CRL_Sign：CRL の CA 署名を確認します。
  - Key_Cert_Sign：証明書の CA 署名を確認します。
  - Key_Agreement：キー共有。

- Data_Encipherment：Key_Encipherment 以外のデータを暗号化します。
- Key_Encipherment：キーを暗号化します。
- Non_Repudiation：一部のアクションを誤って拒否しないように、Key_Cert_sign および CRL_Sign 以外のデジタル署名を確認します。
- Digital_Signature：Non_Repudiation、Key_Cert_Sign、および CRL_Sign 以外のデジタル署名を確認します。

- [拡張キーの使用状況（Extended Key Usage）]：次の拡張キーの使用状況設定を使用します。OID は丸カッコ内に記載してあります。
  - ServerAuth（1.3.6.1.5.5.7.3.1）
  - ClientAuth（1.3.6.1.5.5.7.3.2）
  - CodeSign（1.3.6.1.5.5.7.3.3）
  - EmailProtect（1.3.6.1.5.5.7.3.4）
  - IPSecEndSystem（1.3.6.1.5.5.7.3.5）
  - IPSecTunnel（1.3.6.1.5.5.7.3.6）
  - IPSecUser（1.3.6.1.5.5.7.3.7）
  - TimeStamp（1.3.6.1.5.5.7.3.8）
  - OCSPSign（1.3.6.1.5.5.7.3.9）
  - DVCS（1.3.6.1.5.5.7.3.10）
  - IKE Intermediate

- [カスタム拡張照合キー（最大 10）（Custom Extended Match Key (Max 10)）]：カスタム拡張照合キー（もしあれば）を指定します（最大 10 個）。証明書は入力したすべての指定キーに一致する必要があります。OID 形式でキーを入力します（1.3.6.1.5.5.7.3.11 など）。

（注） カスタム拡張照合キーを 30 文字を超える OID サイズで作成すると、[OK] ボタンのクリック時に拒否されます。OID の最大文字数は、30 文字です。

- [拡張キーの使用状況が設定されている証明書のみを適合（Match only certificates with Extended key usage）]：以前の動作では、証明書識別名（DN）の照合ルールが設定されると、クライアントは特定の EKU OID が設定されている証明書と、EKU が設定されていないすべての証明書とを適合させていました。一貫性を保ちながら、より明確にするため、EKU が設定されていない証明書との適合を拒否できます。デフォルトでは、お客様が予想してい

る従来の動作が保持されます。新しい動作を有効にし、適合を拒否するには、チェックボックスをオンにする必要があります。

- [識別名（最大 10）（Distinguished Name (Max 10)）]：受け入れ可能なクライアント証明書を選択する際に完全一致基準として使用する識別名（DN）を指定します。
  - [名前（Name）]：照合に使用する識別名（DN）。
    - CN：サブジェクトの一般名
    - C：サブジェクトの国
    - DC：ドメイン コンポーネント
    - DNQ：サブジェクトの DN 修飾子
    - EA：サブジェクトの電子メール アドレス
    - GENQ：サブジェクトの GEN 修飾子
    - GN：サブジェクトの名
    - I：サブジェクトのイニシャル
    - L：サブジェクトの都市
    - N：サブジェクトの非構造体名
    - O：サブジェクトの会社
    - OU：サブジェクトの部署
    - SN：サブジェクトの姓
    - SP：サブジェクトの州
    - ST：サブジェクトの州
    - T：サブジェクトの敬称
    - ISSUER-CN：発行元の一般名
    - ISSUER-DC：発行元のコンポーネント
    - ISSUER-SN：発行元の姓
    - ISSUER-GN：発行元の名
    - ISSUER-N：発行元の非構造体名
    - ISSUER-I：発行元のイニシャル
    - ISSUER-GENQ：発行元の GEN 修飾子
    - ISSUER-DNQ：発行元の DN 修飾子
    - ISSUER-C：発行元の国

- ISSUER-L：発行元の都市
- ISSUER-SP：発行元の州
- ISSUER-ST：発行元の州
- ISSUER-O：発行元の会社
- ISSUER-OU：発行元の部署
- ISSUER-T：発行元の敬称
- ISSUER-EA：発行元の電子メール アドレス

- [パターン（Pattern）]：照合する文字列を指定します。 照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

  abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。

- [演算子（Operator）]：この DN で照合する場合に使用する演算子です。
  - [等しい（Equal）]：== と同等
  - [等しくない（Not Equal）]：!= と同等

- [ワイルドカード（Wildcard）]：[有効（Enabled）] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。

- [大文字と小文字を区別（Match Case）]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

関連トピック

証明書照合の設定 （130 ページ）

AnyConnect プロファイル エディタの証明書の登録

証明書登録により、AnyConnect は Simple Certificate Enrollment Protocol（SCEP）を使用してクライアント認証のために証明書をプロビジョニングし、更新できます。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect が、証明書の有効期限の何日前にユーザに対して証明書の失効が近づいていることを警告する日数（RADIUS パスワード管理ではサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。

- [証明書インポート ストア（Certificate Import Store）]：どの Windows 証明書ストアに登録証明書を保存するかを選択します。

- [証明書の内容（Certificate Contents）]：SCEP 登録要求に含める証明書の内容を指定します。
  - Name (CN)：証明書での一般名。
  - Department (OU)：証明書に指定されている部署名。
  - Company (O)：証明書に指定されている会社名。
  - State (ST)：証明書に指定されている州 ID。
  - State (SP)：別の州 ID。
  - Country (C)：証明書に指定されている国 ID。
  - Email (EA)：電子メール アドレス。次の例では、[Email (EA)] は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
  - Domain (DC)：ドメイン コンポーネント。次の例では、[Domain (DC)] は cisco.com に設定されています。
  - SurName (SN)：姓または名。
  - GivenName (GN)：通常は名。
  - UnstructName (N)：定義されていない名前。
  - Initials (I)：ユーザのイニシャル。
  - Qualifier (GEN)：ユーザの世代修飾子。たとえば、「Jr.」や「III」です。
  - Qualifier (DN)：完全 DN の修飾子。
  - City (L)：都市 ID。
  - Title (T)：個人の敬称。たとえば、Ms.、Mrs.、Mr. など。
  - CA Domain：SCEP 登録に使用されます。通常は CA ドメイン。
  - Key size：登録する証明書用に生成された RSA キーのサイズ。

- [証明書取得ボタンを表示（Display Get Certificate Button）]：次の条件下で AnyConnect GUI が [証明書を取得（Get Certificate）] ボタンを表示できるようにします。
  - 証明書は [証明書失効しきい値（Certificate Expiration Threshold）] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
  - 証明書の期限が切れています。
  - 証明書が存在しません。
  - 証明書を照合できません。

関連トピック

証明書登録の設定 （119 ページ）

AnyConnect プロファイル エディタの証明書ピン

前提条件

証明書のピン留めを開始する前のベストプラクティスについては、「証明書のピン留めについて （141 ページ）」を参照してください。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定には、VPN プロファイル エディタを使用します。[グローバル ピン（Global Pins）] セクション内のプリファレンスが有効になっている場合は、サーバ リスト内のホストごとの証明書のみピン留めできます。プリファレンスを有効にすると、クライアントが証明書ピン検証に使用するグローバル ピンのリストを設定できます。[サーバ リスト（Server List）] セクションでのホストごとのピンの追加は、グローバル ピンの追加と同様です。証明書チェーン内の任意の証明書をピン留めでき、証明書は、ピン留めのために必要な情報を計算するため、プロファイル エディタにインポートされます。

[ピンを追加（Add Pin）]：証明書のプロファイル エディタへのインポートおよびピン留めを手引きする証明書ピン留めウィザードが開始します。

ウィンドウの [証明書の詳細（Certificate Details）] 部分では、[件名（Subject）] 列および [発行元（Issuer）] 列を視覚的に確認することができます。

証明書ピン留めウィザード

ピン留めに必要な情報を指定するため、サーバ証明書チェーンからの任意の証明書をプロファイル エディタにインポートすることができます。プロファイル エディタは、次の 3 つの証明書インポート オプションをサポートしています。

- ローカルのファイルを参照：お使いのコンピュータにローカルに存在している証明書を選択します。
- URL からファイルをダウンロード：任意のファイル ホスティング サーバから証明書をダウンロードします。
- PEM 形式の情報をペースト：証明書の開始および終了ヘッダーを含む PEM 形式の情報を挿入します。

（注） インポートできるのは、データ形式が DER、PEM、および PKCS7 の証明書のみです。

AnyConnect プロファイル エディタのモバイル ポリシー

AnyConnect のバージョン 3.0 以降では、Windows Mobile デバイスをサポートしません。Windows Mobile デバイスに関する情報は、『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5』を参照してください。

AnyConnect プロファイル エディタのサーバ リスト

クライアント GUI に表示されるサーバ リストの設定を行うことができます。ユーザは、VPN 接続を確立する際、このリストでサーバを選択することができます。

[サーバ リスト（Server List）] テーブルの列は次のとおりです。

- [ホスト名（Hostname）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアス。
- [ホスト アドレス（Host Address）]：サーバの IP アドレスまたは FQDN。
- [ユーザ グループ（User Group）]：[ホスト アドレス（Host Address）] と組み合わせて使用することによりグループ ベースの URL が構成されます。
- [自動 SCEP ホスト（Automatic SCEP Host）]：クライアント認証に使用する証明書のプロビジョニング用および更新用として指定された Simple Certificate Enrollment Protocol。
- [CA URL]：このサーバが認証局（CA）へ接続する際に使用する URL。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「AnyConnect プロファイル エディタの証明書ピン （50 ページ）」を参照してください。

（注） クライアントは、ピン検証の際に、グローバル ピンおよび対応するホストごとのピンを使用します。ホストごとのピンの設定は、証明書ピン留めウィザードの使用によるグローバル ピンの設定と同様に行います。

[追加/編集（Add/Edit）]：上記のサーバのパラメータを指定できる [サーバ リスト エントリ（Server List Entry）] ダイアログを起動します。

[削除（Delete）]：サーバ リストからサーバを削除します。

[詳細（Details）]：サーバのバックアップ サーバまたは CA URL に関する詳細情報を表示します。

関連トピック

VPN 接続サーバの設定 （71 ページ）

AnyConnect プロファイル エディタのサーバ リストの追加/編集

- [ホスト表示名（Host Display Name）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアスを入力します。
- [FQDN または IP アドレス（FQDN or IP Address）]：サーバの IP アドレスまたは FQDN を指定します。
  - [ホスト アドレス（Host Address）] フィールドに IP アドレスまたは FQDN を指定すると、[ホスト名（Host Name）] フィールドのエントリが AnyConnect Client トレイ フライアウト内の接続ドロップダウン リストに表示されるサーバのラベルになります。
  - [ホスト名（Hostname）] フィールドで FQDN のみを指定し、[ホスト アドレス（Host Address）] フィールドでは IP アドレスを指定しない場合、[ホスト名（Hostname）] フィールドの FQDN が DNS サーバによって解決されます。
  - IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。
- [ユーザ グループ（User Group）]：ユーザ グループを指定します。

  このユーザ グループとホスト アドレスを組み合わせてグループ ベースの URL が構成されます。プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。
- [モバイル専用追加設定（Additional mobile-only settings）]：Apple iOS および Android モバイル デバイスを設定する場合に選択します。
- **バックアップ サーバ リスト**

  ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定することをお勧めします。サーバで障害が発生した場合、クライアントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストの下方向に移動します。

  （注） 逆の面から述べれば、「AnyConnect プロファイル エディタのバックアップ サーバ （44 ページ）」で設定されるバックアップ サーバは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

  - [ホスト アドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは FQDN を指定します。クライアントでは、ホストに接続できない場合には、バックアップ サーバへの接続が試行されます。

- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

- **ロード バランシング サーバ リスト**

  このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつAlways-On機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスはAlways-On機能によりブロックされます。

  - [ホスト アドレス（Host Address）]：ロードバランシング クラスタにあるバックアップ デバイスの IP アドレスまたは FQDN を指定します。
  - [追加（Add）]：ロード バランシング バックアップ サーバ リストにアドレスを追加します。
  - [削除（Delete）]：ロード バランシング バックアップ サーバをリストから削除します。

- [プライマリ プロトコル（Primary Protocol）]：このサーバも接続するプロトコル（SSL または IKEv2 を使用した IPsec）を指定します。デフォルトは SSL です。
  - [標準認証のみ（IOS ゲートウェイ）（Standard Authentication Only (IOS Gateways)）]：プロトコルとして IPsec を選択した場合、このオプションを選択して、IOS サーバへの接続の認証方式を制限できます。

    （注） このサーバが ASA である場合、認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドルタイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

  - [IKE ネゴシエーション中の認証方式（Auth Method During IKE Negotiation）]：標準ベースの認証方式の 1 つを選択します。
    - [IKE ID（IKE Identity）]：標準ベースの EAP 認証方式を選択した場合、このフィールドにグループまたはドメインをクライアントアイデンティティとして入力でき

ます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。デフォルトでは、文字列は *$AnyConnectClient$* です。

- [CA URL]：SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「AnyConnect プロファイル エディタの証明書ピン （50 ページ）」を参照してください。
- [チャレンジ PW のプロンプト（Prompt For Challenge PW）]：有効にすると、証明書をユーザが手動で要求できるようになります。 ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [CA サムプリント（CA Thumbprint）]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注） CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行元の証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

関連トピック

VPN 接続サーバの設定 （71 ページ）

AnyConnect プロファイル エディタのモバイル設定

Apple iOS/Android の設定

- [証明書認証（Certificate Authentication）]：接続エントリに関連付けられた証明書認証ポリシー属性は、証明書がこの接続にどのように処理されるかを指定します。有効な値は次のとおりです。
  - [自動（Automatic）]：AnyConnect は、接続がいつなされるかを認証するクライアント証明書を自動で選択します。この場合、インストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、デバイス ユーザが VPN 接続の確立を試行するたびに実行されます。
  - [手動（Manual）]：AnyConnect は、プロファイルがダウンロードされ、次のいずれかを行うときに、Android デバイスの AnyConnect 証明書ストアで証明書を検索します。

- AnyConnect は、VPN クライアント プロファイルで定められる基準に一致している証明書に基づく証明書を見つけた場合、証明書を接続エントリに割り当て、接続が確立されたときにその証明書を使用します。
- 一致する証明書が見つからない場合、証明書認証ポリシーが [自動（Automatic）] に設定されます。
- 割り当てられた証明書が、何らかの理由で AnyConnect 証明書ストアから削除された場合、AnyConnect は [自動（Automatic）] に証明書認証ポリシーをリセットします。

- [無効（Disabled）]：クライアント証明書は認証に使用されません。

- [プロファイルがインポートされたときにサーバ リスト エントリをアクティブ化（Make this Server List Entry active when profile is imported）]：VPN 接続がデバイスにダウンロードされたら、サーバ リスト エントリをデフォルトとして定義します。この宛先を設定できるのは、1 つのサーバ リストエントリのみです。デフォルトでは、無効に設定されています。

Apple iOS のみの設定

- [3G/WiFi ネットワーク間のローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]：有効（デフォルト）の場合、AnyConnect は、接続が解除された後やデバイスが起動した後、もしくは接続種別（EDGE（2G）、1xRTT（2G）、3G または Wi-Fi など）が変更になった後で、再接続にかかる時間を制限しません。この機能は、ネットワーク全体とのセキュアな接続を維持することで、シームレスなモビリティを提供します。企業への接続が必要で、かつバッテリ寿命の消費が多いアプリケーションには有用です。

  [ネットワーク ローミング（Network Roaming）] が無効で、AnyConnect の接続が切断された場合、必要に応じて最大 20 秒まで再接続を試みます。接続できない場合は、デバイスユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

  （注） ネットワーク ローミングは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響しません。

- [Connect on Demand（証明書の認証が必要）（Connect on Demand (requires certificate authorization)）]：このフィールドでは、Apple iOS で提供される Connect on Demand 機能を設定できます。その他のアプリケーションが、ドメイン ネーム システム（DNS）を使用して解決されるネットワーク接続を開始したときに、毎回チェックされるルールのリストを作成できます。

  [Connect on Demand] は、[証明書認証（Certificate Authentication）] フィールドが [手動（Manual）] または [自動（Automatic）] に設定されている場合にのみ使用できるオプションです。[証明書認証（Certificate Authentication）] フィールドが [無効（Disabled）] に設定されている場合は、このチェックボックスはグレー表示されます。[ドメインまたはホス

トと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

- [ドメインまたはホストと一致（Match Domain or Host）]：ユーザが Connect on Demand ルールを作成するホスト名（host.example.com）、ドメイン名（.example.com）、またはドメインの一部（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。
- [オンデマンドアクション（On Demand Action）]：デバイス ユーザが前の手順で定義されたドメインまたはホストに接続しようとしたときに実行するアクションを次の中から 1 つ指定します。
  - [接続しない（Never Connect）]：このリストのルールに一致しても、iOS は絶対に VPN 接続を開始しません。このリストのルールは他のどのリストよりも優先されます

    （注） Connect On Demand が有効の場合、アプリケーションは自動的にこのリストにサーバアドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。

  - [必要に応じて接続（Connect if Needed）]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続を開始します。
  - [常に接続（Always Connect）]：常時接続動作は、リリースに依存します。
    - Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
    - iOS 7.x では、常時接続はサポートされません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
    - 以降のリリースでは、常時接続は使用されません。設定されたルールは [必要に応じて接続（Connect if Needed）] リストに移動され、それに合わせて動作します。
- [追加または削除（Add or Delete）]：[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドに指定されたルールをルール テーブルに追加するか、または選択したルールをルール テーブルから削除します。

NVM プロファイル エディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、または デュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。

TND が NVM プロファイルに設定されている場合、信頼ネットワーク検出は NVM によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。ただし、TND が NVM プロファイルに明示的に設定されていない場合、NVM は VPN の TND 機能を使用してエンドポイントが信頼ネットワーク内にあるかどうかを判断します。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステム ログに TND の使用状況が表示されます。TND パラメータの設定については、「AnyConnect プロファイル エディタ、プリファレンス（Part 2）（38 ページ）」を参照してください。

- [デスクトップ（Desktop）] または [モバイル（Mobile）]：NVM をデスクトップとモバイル デバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。 モバイルは、将来的にサポートされます。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）]：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [IP アドレス/FQDN（IP Address/FQDN）]：コレクタの IPv4 の IP アドレス/FQDN を指定します。
  - [ポート（Port）]：コレクタがリッスンするポート番号を指定します。
- **キャッシュの設定**
  - [最大サイズ（Max Size）]：データベースが到達できる最大サイズを指定します。以前はキャッシュ サイズに事前設定の制限がありましたが、プロファイル内で設定できるようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

- [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

  日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- [定期的なフロー レポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フロー レポートが定期送信されます。デフォルトで、NVM は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、 *n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンド ユーザへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイムデータとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

  キャッシュデータはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または [すべてのネットワーク（all networks）] を選択します。

- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。

  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにかかる時間が削減されるよう、ブロードキャストパケットおよびマルチキャストパケットの収集はオフになっています。ブロードキャストパケットとマルチキャストパケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。

  - [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。

- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時に

アクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

[追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。

- ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
- それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
- より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
- 選択したコレクション モードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。
- 以前の AnyConnect リリースのプロファイルがそれより後の AnyConnect リリース のプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。
- [名前（Name）] : 作成するポリシーの名前を指定します。
- [ネットワーク タイプ（Network Type）] : 収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。
- [フロー フィルタ ルール（Flow Filter Rule）] : 一連の条件と、すべての条件が満たされたときに実行するアクションを、フローの収集または無視として定義します。最大 25 のルールを設定でき、各ルールに最大 25 の条件を定義できます。[フロー フィルタ ルール（Flow Filter Rule）] リストの右側にある上下ボタンを使用してルールの優先順位を調整し、後続のルールよりも優先的に考慮されるように設定します。[追加（Add）] をクリックし、フロー フィルタ ルールのコンポーネントを設定します。
  - [名前（Name）] : フロー フィルタ ルールの一意の名前。
  - [タイプ（Type）] : 各フィルタ ルールには [収集（Collect）] または [無視（Ignore）] が指定されます。フィルタ ルールが満たされた場合に適用するアクション（[収集（Collect）] または [無視（Ignore）]）を決定します。[収集（Collect）] する場合、条件が満たされるとフローが許可されます。[無視（Ignore）] する場合、フローはドロップされます。

- [条件（Conditions）]：照合する各フィールドのエントリと、合致と見なすのはそのフィールド値が等しいときか等しくないときか、判断する操作を追加します。各操作にはフィールド識別子とそのフィールドに対応する値が含まれます。フィールドの一致では、フィルタ エンジン ルールの設定でルール セットに大文字と小文字を区別しない操作（EqualsIgnoreCase）を適用しない限り、大文字と小文字が区別されます。有効にした後、ルール下で設定された値フィールドへの入力は、大文字と小文字が区別されません。

- **[包含（Include）]/[除外（Exclude）]**
  - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドがすべて収集され、すべてのフィールドがオフにされます。
  - [フィールド（Fields）]：データ収集ポリシーの一部とするフィールドを決定します。 ネットワーク タイプと包含または除外するフィールドに基づいて、NVM はエンドポイント上で該当するデータを収集します。

    AnyConnect リリース 4.4（およびそれ以降）では、インターフェイスの状態と SSID を選択できるようになりました。これによりインターフェイスのネットワーク状態を信頼する/信頼しないを指定します。
  - [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードをプライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。これにより、フィールド情報は実際の値ではなく値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

    包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- Knox のデータ収集ポリシー（モバイルのみ）：モバイルプロファイルを選択した場合にデータ収集ポリシーを指定するオプションです。Knox コンテナのデータ収集ポリシーを作成するには、[範囲（Scope）] の下の [Knox のみ（Knox-Only）] チェックボックスをオンにします。[デバイスの範囲（Device Scope）] で適用されるデータ収集ポリシーは、別の Knox コンテナデータ収集ポリシーが指定されていない限り、Knox コンテナトラフィックの場合も適用されます。データ収集ポリシーを追加または削除するには、前述の「データ収集ポリシー」の説明を参照してください。モバイルプロファイルでは最大 6 つの異なるデータ収集ポリシー（デバイス用に 3 つ、Knox 用に 3 つ）を設定できます。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、NVM が設定されると、ユーザに対して表示されるようになります。リモート ユーザは、NVM アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して NVM を制御します。

- [モバイルネットワークでのエクスポート（Export on Mobile Network）]（オプションおよびモバイルのみ）：デバイスがモバイルネットワークを使用している場合に NVM フローのエクスポートを許可するかどうかを指定します。有効な場合（デフォルト値）、エンドユーザは、[利用許可ポリシー（Acceptable User Policy）] ウィンドウが表示されているとき、または後で AnyConnect Android アプリケーションで **[設定（Settings）]** > **[NVM 設定（NVM-Settings）]** > > **[NVM にモバイルデータを使用する（Use mobile data for NVM）]** チェックボックスをオンにして、管理者を上書きできます。[モバイルネットワークでのエクスポート（Export on Mobile Network）] チェックボックスをオフにすると、デバイスがモバイルネットワークを使用している場合に NVM フローがエクスポートされず、エンドユーザはそれを変更できません。

- [信頼ネットワーク検出（Trusted Network Detection）]：この機能は、エンドポイントが物理的に社内ネットワーク上にあるかどうかを検出します。ネットワークの状態は、いつ NVM データをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために NVM によって使用されます。[設定（Configure）] をクリックして、信頼ネットワーク検出の設定を行います。SSL プローブが設定済みの信頼できるヘッドエンドに送信され、到達可能であれば、証明書で応答します。次に、サムプリント（SHA-256ハッシュ）が抽出され、プロファイル エディタのハッシュ セットと照合されます。一致が見つかった場合はエンドポイントが信頼ネットワーク内にあることを意味します。ただし、ヘッドエンドが到達不能である場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼されていないネットワーク内にあると見なされます。

（注） 内部ネットワーク外から操作している場合、TND は DNS 要求を行い、設定されたサーバへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

TND が NVM プロファイルに設定されておらず、VPN モジュールがインストールされている場合、NVM は Trusted Network Detection の設定を使用して、エンドポイントが信頼ネットワーク内にあるかどうかを判断します。NVM プロファイル エディタの TND 設定には次が含まれます。

1. **https://**：信頼されている各サーバの URL（IP アドレス、FQDN、またはポート アドレス）を入力し、[追加（Add）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

2. [証明書ハッシュ（SHA-256）（Certificate Hash (SHA-256)）]：信頼されているサーバへの SSL 接続が成功した場合、このフィールドは自動的に入力されます。それ以外の場合は、サーバ証明書の SHA-256 ハッシュを入力して [設定（Set）] をクリックすることにより手動で設定できます。

3. [信頼されているサーバのリスト（List of Trusted Servers）]：このプロセスで複数の信頼されているサーバを定義できます（最大値は 10 です）。サーバは、設定されている順序で信頼ネットワーク検出に対して試行されるため、[上に移動（Move Up）] ボタンと [下に移動（Move|Down）] ボタンを使用して順序を調整できます。エンドポイントが最初のサーバに接続できなかった場合は、2 番目のサーバという順序で試行されます。リスト内のすべてのサーバをした後、エンドポイントは 10 秒待機してからもう一度途最終試行を行います。サーバが認証されると、エンドポイントは信頼ネットワーク内で考慮されます。

プロファイルを `NVM_ServiceProfile.xml` として保存します。この名前でプロファイルを保存する必要があります。そうしないと、NVM はデータの収集と送信に失敗します。

AnyConnect ローカル ポリシー

AnyConnectLocalPolicy.xml は、セキュリティ設定を含む、クライアント上の XML ファイルです。このファイルは、ASA によって展開されません。手動でインストールするか、社内のソフトウェア展開システムを使用してユーザ コンピュータに展開する必要があります。ユーザのシステムで既存のローカル ポリシー ファイルに変更を加えた場合は、そのシステムをリブートする必要があります。

ローカル ポリシー パラメータと値

次のパラメータは、VPN ローカル ポリシー エディタおよび `AnyConnectLocalPolicy.xml` ファイル内の要素です。XML 要素は、山カッコで囲んで表示しています。

（注） ファイルを手動で編集し、ポリシーパラメータを省略した場合、この機能にはデフォルトの動作が適用されます。

- <acversion>

  このファイルのすべてのパラメータを解釈できる AnyConnect クライアントの最小バージョンを指定します。このバージョンよりも古いバージョンの AnyConnect を実行しているクライアントがファイルを読み込むと、イベント ログに警告が記録されます。

  形式は acversion="<version number>" です。

- [FIPS モード（FIPS Mode）] <FipsMode>

  クライアントの FIPS モードを有効にします。この設定は、FIPS 標準で承認されているアルゴリズムおよびプロトコルだけを使用するようにクライアントに強制します。

- [ダウンローダのバイパス（Bypass Downloader）] <BypassDownloader>

  オンにすると、ダイナミック コンテンツのローカル バージョンの存在を検出し、アップデートする VPNDownloader.exe モジュールの起動を無効にします。クライアントは、変

換、カスタマイズ、オプション モジュール、コア ソフトウェア更新など、ASA のダイナミック コンテンツをチェックしません。

[ダウンローダのバイパス（Bypass Downloader）] をオンにすると、ASA へのクライアント接続時に、次の 2 つの事態のいずれかが発生します。

- ASA 上の VPN クライアント プロファイルがクライアント上のものと異なる場合、クライアントは接続の試行を中断します。
- ASA に VPN クライアント プロファイルが存在しない場合でもクライアントは VPN 接続を行いますが、クライアントにハードコードされた VPN クライアント プロファイル設定を使用します。

（注） ASA で VPN クライアント プロファイルを設定する場合は、BypassDownloader を true に設定した ASA に接続する前に、クライアントプロファイルをクライアントにインストールしておく必要があります。プロファイルには管理者が定義したポリシーを含めることができるため、BypassDownloader 設定 true は、ASA を使用してクライアントプロファイルを集中管理しない場合に限りお勧めします。

- [CLRチェックの有効化（Enable CRL Check）] <EnableCRLCheck>

この機能は *Windows* デスクトップでのみ実装されます。SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。この設定を有効にすると、AnyConnect はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認します。認証局（CA）によって失効された証明書であることが判明すると、AnyConnect は接続しません。

CRL チェックは、デフォルトでは無効です。AnyConnect が CRL チェックを実行するのは、[CLRチェックの有効化（Enable CRL Check）] がオンである場合（有効な場合）だけであるため、エンド ユーザに対し次のような状況が発生することがあります。

- CRL によって証明書が失効した場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が無効になっている場合でも、セキュア ゲートウェイへの接続は無条件で失敗します。
- 到達できない CRL 配布ポイントなどが原因で CRL を取得できない場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が有効になっていると、セキュア ゲートウェイへの接続は無条件で失敗します。[厳格な証明書トラスト（Strict Certificate Trust）] が無効な場合は、ユーザに対しエラーを無視するように求められることがあります。

（注） AnyConnect は、[常時接続（Always On）] が有効な場合は CRL チェックを実行できません。CRL 配布ポイントがパブリックに到達不能な場合、AnyConnect でサービスの中断が発生することがあります。

- [Web起動の制限（Restrict Web Launch）] <RestrictWebLaunch>

  ユーザは、FIPS 準拠のブラウザを使用して、WebLaunch を開始できません。これを行うためには、AnyConnect トンネルを開始するために使用されるセキュリティ Cookie をクライアントが取得できないようにします。クライアントからユーザに情報メッセージが表示されます。

- [厳格な証明書トラスト（Strict Certificate Trust）] <StrictCertificateTrust>

  選択すると、リモート セキュリティ ゲートウェイを認証するときに、AnyConnect は確認できない証明書を許可しません。ユーザにこれらの証明書を受け入れるように求める代わりに、クライアントは自己署名証明書を使用したセキュリティ ゲートウェイの接続に失敗し、「`Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.`」を表示します。オフにすると、クライアントはユーザに証明書を受け入れるように求めます。これはデフォルトの動作です。

  以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

  - 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザが接続している場合に「中間者」攻撃を防ぐために役立ちます。
  - 完全に検証可能で信頼できる証明書を使用する場合でも、AnyConnect クライアントは、デフォルトでは、未検証の証明書の受け入れをエンドユーザに許可します。エンドユーザが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエンド ユーザに求めます。エンド ユーザによるこの判断を回避するには、厳格な証明書トラストを有効にします。

- [プリファレンス キャッシングの制限（Restrict Preference Caching）] <RestrictPreferenceCaching>

  AnyConnect は機密情報をディスクにキャッシュしないように設計されています。このパラメータを有効にすると、AnyConnect プリファレンスに保存されているすべての種類のユーザ情報に、このポリシーが拡張されます。

  - [クレデンシャル（Credentials）] : ユーザ名および第 2 ユーザ名はキャッシュされません。
  - [サムプリント（Thumbprints）] : クライアントおよびサーバ証明書のサムプリントはキャッシュされません。

- [クレデンシャルとサムプリント（CredentialsAndThumbprints）]：証明書のサムプリントおよびユーザ名はキャッシュされません。
- [すべて（All）]：自動プリファレンスはいずれもキャッシュされません。
- [false]：すべてのプリファレンスがディスクに書き込まれます（デフォルト）。

- [PEM ファイル証明書ストアの除外（Exclude Pem File Cert Store）]（Linux および macOS）<ExcludePemFileCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが PEM ファイル証明書ストアを使用できないようにします。

  FIPS 対応の OpenSSL を使用するストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。PEM ファイル証明書ストアを許可することで、リモートユーザは FIPS 準拠の証明書ストアを使用することになります。

- [Mac のネイティブ証明書ストアの除外（Exclude Mac Native Cert Store）]（macOS のみ）<ExcludeMacNativeCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが Mac ネイティブ（キーチェーン）証明書ストアを使用できないようにします。

- [Firefox の NSS 証明書ストアの除外（Exclude Firefox NSS Cert Store）]（Linux および macOS）<ExcludeFirefoxNSSCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが Firefox NSS 証明書ストアを使用できないようにします。

  ストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。

- [更新ポリシー（Update Policy）] <UpdatePolicy>

  クライアントがどのヘッドエンドからソフトウェア更新またはプロファイル更新を取得できるかを制御します。

  - [任意のサーバからのソフトウェア更新を許可（Allow Software Updates From Any Server）] <AllowSoftwareUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN コア モジュールおよびその他のオプション モジュールのソフトウェア更新を許可または禁止します。

  - [任意のサーバからの VPN プロファイル更新を許可（Allow VPN Profile Updates From AnyServer）]<AllowVPNProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN プロファイル更新を許可または禁止します。

  - [任意のサーバからの管理 VPN プロファイル更新を許可（Allow Management VPN Profile Updates From Any Server）]<AllowManagementVPNProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの管理 VPN プロファイル更新を許可または禁止します。

- [任意のサーバからのサービス プロファイル更新を許可（Allow Service Profile Updates From AnyServer）] <AllowServiceProfileUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのその他のサービス モジュール プロファイル更新を許可または禁止します。

- [任意のサーバからの ISE ポスチャ プロファイル更新を許可（Allow ISE Posture Profile Updates From Any Server）] <AllowISEProfileUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの ISE ポスチャ プロファイル更新を許可または禁止します。

- [任意のサーバからのコンプライアンス モジュール更新を許可（Allow Compliance Module Updates From Any Server）] <AllowComplianceModuleUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのコンプライアンス モジュール更新を許可または禁止します。

- [サーバ名（Server Name）] <ServerName>

  このリストに認証されたサーバを指定します。これらのヘッドエンドには、VPN 接続時にすべての AnyConnect ソフトウェアとプロファイルの完全な更新が許可されます。ServerName には、FQDN、IP アドレス、ドメイン名、またはワイルドカードを含むドメイン名を使用できます。

ローカル ポリシー パラメータの手動変更

手順

ステップ 1 クライアント インストールから、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のコピーを取得します。

表 *1*: オペレーティング システムと *AnyConnect* ローカル ポリシー ファイルのインストール パス

オペレーティング システム	インストール パス
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

ステップ 2 パラメータ設定を編集します。AnyConnectLocalPolicy ファイルを手動で編集するか、AnyConnect プロファイル エディタのインストーラとともに配布される VPN ローカル ポリシー エディタを使用できます。

ステップ 3 ファイルを `AnyConnectLocalPolicy.xml` として保存し、社内のソフトウェア展開システムを使用してこのファイルをリモート コンピュータに展開します。

ステップ 4 ローカル ポリシー ファイルへの変更が反映されるように、リモート コンピュータをリブートします。

MST ファイルでのローカル ポリシー パラメータの有効化

設定できる説明および値については、「ローカル ポリシー パラメータと値」を参照してください。

ローカル ポリシー パラメータを変更するには、MST ファイルを作成します。MST パラメータ名は、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）の次のパラメータに対応しています。

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

（注） AnyConnect インストールは、ユーザ コンピュータ上にある既存のローカル ポリシー ファイルを自動的には上書きしません。クライアント インストーラが新しいポリシー ファイルを作成できるようにするには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

（注） ローカル ポリシー ファイルへのすべての変更には、システムのリブートが必要になります。

Enable FIPS ツールによるローカル ポリシー パラメータの有効化

すべてのオペレーティング システムで、シスコの Enable FIPS ツールを使用して、FIPS が有効な AnyConnect ローカル ポリシー ファイルを作成できます。Enable FIPS ツールはコマンド ライン ツールで、実行するには、Windows では管理者権限が必要です。Linux および macOS では、root ユーザとして実行する必要があります。

Enable FIPS ツールのダウンロード元の詳細については、FIPS クライアント用に受け取ったライセンシング情報を参照してください。

Enable FIPS ツールを実行するには、コンピュータのコマンド ラインから EnableFIPS <arguments> コマンドを入力します。Enable FIPS ツールを使用するときは、次のことに注意してください。

- 引数を何も指定しなかった場合、ツールによって FIPS が有効にされ、vpnagent サービス（Windows）または vpnagent デーモン（macOS および Linux）がリスタートされます。
- 複数の引数はスペースで区切ります。

Windows コンピュータ上で実行する Enable FIPS ツールのコマンド例を次に示します。

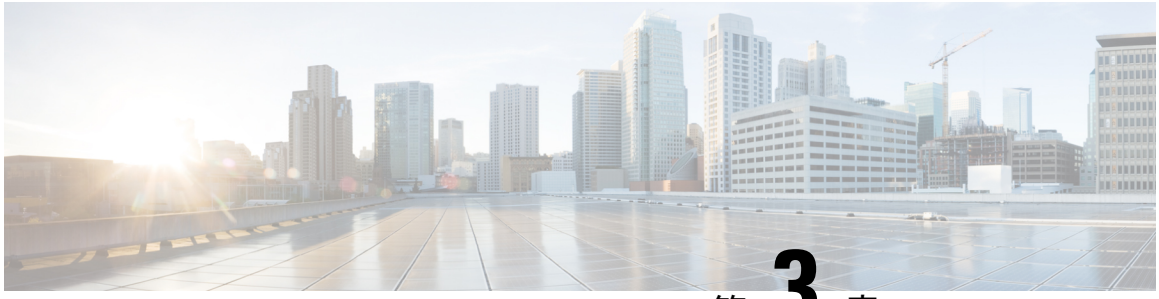
```
EnableFIPS rwl=false sct=true bd=true fm=false
```

Linux または macOS コンピュータ上で実行するコマンド例を次に示します。

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

次の表に、Enable FIPS ツールで設定できるポリシー設定の例を示します。引数は、AnyConnect ローカル ポリシー ファイルのパラメータに対応します。

ポリシー設定	引数および構文
FIPS モード	fm=[true | false]
ダウンローダのバイパス	bd=[true | false]
WebLaunch の制限	rwl=[true | false]
厳格な証明書トラスト	sct=[true | false]
プリファレンス キャッシングの制限	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
FireFox の NSS 証明書ストアの除外（Linux および macOS）	efn=[true | false]
PEM ファイル証明書ストアの除外 （Linux および macOS）	epf=[true | false]
Mac のネイティブ証明書ストアの除外 （macOS のみ）	emn=[true | false]



第 3 章

VPN アクセスの設定

- VPN への接続と接続解除 （69 ページ）
- VPN トラフィックの選択および除外 （107 ページ）
- VPN 認証の管理 （114 ページ）

VPN への接続と接続解除

AnyConnect VPN 接続オプション

AnyConnect クライアントには、自動的に VPN セッションを接続、再接続、または切断するための多数のオプションが用意されています。これらのオプションは、ユーザが VPN に接続するために便利な方法を提供し、同時にネットワーク セキュリティの要件をサポートします。

AnyConnect 接続の開始とリスタート

VPN 接続サーバの設定を行い、ユーザが手動で接続するセキュア ゲートウェイの名前とアドレスを提供します。

便利な自動 VPN 接続を提供するための AnyConnect 機能を次から選択します。

- ログイン前の Windows VPN 接続の自動開始
- AnyConnect 起動時の VPN 接続の自動開始
- VPN 接続の自動リスタート

また、強力なネットワーク セキュリティを適用したり、ネットワーク アクセスを VPN のみに制限したりするために、次の自動 VPN ポリシー オプションの使用を検討してください。

- Trusted Network Detection について
- Always-Onを使用した VPN 接続の必要性
- キャプティブ ポータル ホットスポットの検出と修復の使用

AnyConnect 接続の再ネゴシエートと維持

アクティビティが発生していない場合でも、ASA がユーザに対して AnyConnect VPN 接続を維持する長さを制限できます。VPN セッションがアイドルになった場合、接続を終了するか、または接続を再ネゴシエートできます。

- キープアライブ：ASA はキープアライブ メッセージを定期的に送信します。これらのメッセージは、ASA によって無視されますが、クライアントと ASA の間の、デバイスを使用した接続の維持に役立ちます。

  ASDM または CLI でキープアライブを設定する手順については、『Cisco ASA Series VPN Configuration Guide』の「Enable Keepalive」の項を参照してください。

- デッド ピア検出：ASA および AnyConnect クライアントは、「R-U-There」メッセージを送信します。これらのメッセージは、IPsec のキープアライブ メッセージよりも少ない頻度で送信されます。ASA（ゲートウェイ）および AnyConnect クライアントの両方で DPD メッセージの送信を有効にして、タイムアウト間隔を設定できます。

  - クライアントが ASA の DPD メッセージに応答しない場合、ASA はもう 1 回試行してから、セッションを「再開待機」モードに移行します。このモードでは、ユーザはネットワークをローミングしたり、スリープ モードに移行してから後で接続を回復したりできます。アイドル タイムアウトが発生する前にユーザが再接続しなかった場合、ASA はトンネルを終了します。推奨されるゲートウェイ DPD 間隔は 300 秒です。

  - ASA がクライアントの DPD メッセージに応答しない場合、クライアントはもう 1 回試行してから、トンネルを終了します。推奨されるクライアント DPD 間隔は 30 秒です。

    ASDM 内で DPD を設定する手順については、適切なリリースの『Cisco ASA Series VPN Configuration Guide』の「Configure Dead Peer Detection」の項を参照してください。

- ベスト プラクティス：

  - クライアント DPD を 30 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

  - サーバ DPD を 300 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

  - SSL および IPsec の両方のキー再生成を 1 時間に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [キー再作成（Key Regeneration）]）。

AnyConnect 接続の終了

AnyConnect 接続を終了するには、ユーザはセキュア ゲートウェイに対してエンドポイントを再認証し、新しい VPN 接続を作成する必要があります。

次の接続パラメータは、タイムアウトに基づいて、VPN セッションを終了します。

- 最大接続時間：ユーザの最大接続時間を分単位で設定します。ここで指定した時間が経過すると、システムは接続を終了します。また、無制限の接続時間（デフォルト）を許可することもできます。
- VPN アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。VPN アイドル タイムアウトを設定しない場合は、デフォルトのアイドル タイムアウトが使用されます。
- デフォルト アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。デフォルト値は 30 分（1800 秒）です。

これらのパラメータを設定するには、適切なリリースの『Cisco ASA Series VPN Configuration Guide』の「Specify a VPN Session Idle Timeout for a Group Policy」の項を参照してください。

VPN 接続サーバの設定

AnyConnect VPN サーバ リストは、VPN ユーザが接続するセキュア ゲートウェイを識別するホスト名とホストアドレスのペアで構成されます。ホスト名は、エイリアス、FQDN、または IP アドレスで指定できます。

サーバ リストに追加されたホストは、AnyConnect GUI の [接続先（Connect to）] ドロップダウン リストに表示されます。その後、ユーザはドロップダウン リストから選択して VPN 接続を開始できます。リストの最上位にあるホストはデフォルト サーバで、GUI のドロップダウン リストの先頭に表示されます。ユーザがリストから代替サーバを選択した場合、その選択されたサーバが新しいデフォルト サーバになります。

サーバ リストにサーバを追加すると、その詳細を表示し、サーバ エントリを編集または削除るようになります。サーバ リストにサーバを追加するには、次の手順を実行します。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 サーバのホスト名およびアドレスを設定します。

a) [ホスト表示名（Host Display Name）]、ホストの参照に使用されるエイリアス、FQDN、または IP アドレスを入力します。名前に「&」または「<」文字を使用しないでください。FQDN または IP アドレスを入力した場合、次の手順で [FQDN] または [IP アドレス（IP Address）] を入力する必要はありません。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。

b) （任意）[ホスト表示名（Host Display Name）] に入力していない場合、ホストの [FQDN] または [IP アドレス（IP Address）] を入力します。

c) （任意）[ユーザ グループ（User Group）] を指定します。

AnyConnect は、ユーザ グループとともに FQDN または IP アドレスを使用してグループ URL を形成します。

ステップ 4 [バックアップ サーバ リスト（Backup Server List）] に、バックアップ サーバとしてフォールバックするサーバを入力します。名前に「&」または「<」文字を使用しないでください。

（注） 逆の面から述べれば、[サーバ（Server）] メニューの [バックアップ サーバ（Backup Server）] タブは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

ステップ 5 （任意）[ロード バランシング サーバ リスト（Load Balancing Server List）].に、ロード バランシング サーバ を追加します。名前に「&」または「<」文字を使用しないでください。

このサーバ リスト エントリのホストにセキュリティ アプライアンスのロード バランシング クラスタを指定し、かつ Always-On 機能が有効になっている場合は、このリストにクラスタのロード バランシング デバイスを追加します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは Always-On 機能によりブロックされます。

ステップ 6 クライアントがこの ASA に使用する [プライマリ プロトコル（Primary Protocol）] を指定します。

a) SSL（デフォルト）または IPSec を選択します。

IPsec を指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

b) IPSec を指定した場合は、[標準認証のみ（Standard Authentication Only）] を選択してデフォルトの認証方式（独自の AnyConnect EAP）を無効にし、ドロップダウン リストからいずれかの方式を選択します。

（注） 認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

ステップ 7 （任意）このサーバ用の SCEP を設定します。

a) SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。

b) [チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにして、ユーザが証明書を手動で要求できるようにします。ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。

c) CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します。CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

ステップ 8 [OK] をクリックします。

関連トピック

AnyConnect プロファイル エディタのサーバ リスト （51 ページ）
AnyConnect プロファイル エディタのサーバ リストの追加/編集 （52 ページ）

ログイン前の Windows VPN 接続の自動開始

Start Before Logon について

Start Before Logon（SBL）と呼ばれるこの機能によりユーザは、Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。

SBL がインストールされ、有効になると、[ネットワーク接続（Network Connect）] ボタンは AnyConnect VPN および ネットワーク アクセス マネージャ UI を起動します。

SBL には、ネットワーク アクセス マネージャ タイルも含まれており、ユーザが設定したホーム ネットワーク プロファイルを使用した接続を可能にします。SBL モードで許可されるネットワーク プロファイルには、非 802.1X 認証モードを採用するすべてのメディア タイプ（オープン WEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。

SBL は Windows システムのみで利用でき、Windows のバージョンによって異なるメカニズムを使用して実装されます。

- Windows では、Pre-Login Access Provider（PLAP）が AnyConnect SBL を実装するために使用されます。

  PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [ネットワーク接続（Network Connect）] ボタンでネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

  PLAP は Windows の 32 ビット版と 64 ビット版をサポートします。

SBL を有効にする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループ ポリシーでキャッシュのクレデンシャル使用が許可されない場合）。このシナリオでは、コンピュー

タへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。

- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。SBL を有効にすると、ユーザは、ローカル インフラストラクチャおよび通常はオフィスにいるときに実行されるログイン スクリプトにアクセスできます。これには、ドメインログインスクリプト、グループポリシーオブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。
- インフラストラクチャとの接続が必要な場合があるネットワーキングコンポーネント（MS NAP/CS NAC など）が存在する。

Start Before Logon の制限

- AnyConnect は、高速ユーザ切り替えとの互換性がありません。
- AnyConnect は、サードパーティの Start Before Logon アプリケーションでは起動できません。

Start Before Logon の設定

手順

ステップ 1 AnyConnect Start Before Logon モジュールのインストール。

ステップ 2 AnyConnect プロファイルでの SBL の有効化。

AnyConnect Start Before Logon モジュールのインストール

AnyConnect インストーラは、基盤となるオペレーティング システムを検出し、システム ディレクトリに AnyConnect SBL モジュールから適切な AnyConnect DLL を配置します。Windows 7 または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネント（vpnplap.dll または vpnplap64.dll）をインストールします。

（注） VPNGINA または PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、VPNGINA または PLAP のコンポーネントは無効となり、リモート ユーザの画面に表示されなくなります。

SBL モジュールを事前展開するか、SBL モジュールをダウンロードするように ASA を設定することができます。AnyConnect を事前展開する場合は、Start Before Logon モジュールよりも先にコア クライアント ソフトウェアをインストールする必要があります。MSI ファイルを使

用して AnyConnect コアおよび Start Before Logon コンポーネントを事前展開する場合は、正しい順序で実行する必要があります。

手順

ステップ 1 ASDM で、**[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）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 左側のナビゲーション ペインで **[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]** を選択します。

ステップ 4 [ダウンロードするオプションのクライアント モジュール（Optional Client Module for Download）] 設定の [継承（Inherit）] をオフにします。

ステップ 5 ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

AnyConnect プロファイルでの SBL の有効化

始める前に

- SBL は、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、その他のワイヤレス認証を設定する必要があります。
- ネットワーク アクセス マネージャがインストールされている場合、デバイス接続を展開して、適切な接続を確実に使用できるようにする必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [ログイン前の起動の使用（Use Start Before Logon）] を選択します。

ステップ 3 （任意）リモート ユーザが SBL を制御できるようにする場合は、[ユーザ制御可（User Controllable）] をオンにします。

（注） SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

Start Before Logon のトラブルシューティング

手順

ステップ 1 AnyConnect プロファイルが ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2 以前のプロファイルを削除します（*.xml と指定してハード ドライブ上の格納場所を検索します）。

ステップ 3 Windows の [プログラムの追加と削除（Add/Remove Programs）] を使用して SBL コンポーネントをアンインストールします。コンピュータをリブートして、再テストします。

ステップ 4 イベント ビューアでユーザの AnyConnect ログをクリアし、再テストします。

ステップ 5 セキュリティ アプライアンスを再度参照して、AnyConnect を再インストールします。

ステップ 6 いったんリブートします。次回リブート時には、[ログイン前の起動（Start Before Logon）] プロンプトが表示されます。

ステップ 7 DART バンドルを収集し、AnyConnect 管理者に送付します。

ステップ 8 次のエラーが表示された場合は、ユーザの AnyConnect プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application
 Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
 available.
```

ステップ 9 .tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

AnyConnect 起動時の VPN 接続の自動開始

[起動時に自動接続（Auto Connect on Start）] とも呼ばれるこの機能は、AnyConnect が開始されると、VPN クライアント プロファイルで指定されたセキュア ゲートウェイへの VPN 接続を自動的に確立します。

[起動時に自動接続（Auto Connect on Start）] はデフォルトでは無効であり、ユーザはセキュア ゲートウェイを指定または選択する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [起動時に自動接続（Auto Connect on Start）] を選択します。

ステップ 3 （任意）[起動時に自動接続（Auto Connect on Start）] をユーザが制御できるようにするには、[ユーザ制御可（User Controllable）] を選択します。

Windows システムにおける Start Before Logon（PLAP）の設定

Start Before Logon（SBL）機能によって、ユーザが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。

SBL AnyConnect 機能は「Pre-Login Access Provider（PLAP）」と呼ばれます。これは、接続可能なクレデンシャルプロバイダーです。この機能を使用すると、プログラマチック ネットワークの管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログオン前に実行することができます。PLAP では、サポートされている Windows オペレーティング システムすべてに対して SBL 機能を提供します。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

PLAP のインストール

vpnplap.dll および vpnplap64.dll の両コンポーネントは、既存のインストール済み環境の一部になっているため、単一のアドオン SBL パッケージをセキュリティ アプライアンスにロードできます。ロードされると、該当するコンポーネントがターゲット プラットフォームにインストールされます。PLAP はオプションの機能です。インストーラ ソフトウェアは、基盤のオペレーティング システムを検出して該当する DLL をシステム ディレクトリに配置します。Windows 7 以降、または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティングシステムが使用されているかを判別して、該当する PLAP コンポーネントをインストールします。

（注） PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、PLAP のコンポーネントは無効となり、リモート ユーザの画面に表示されなくなります。

PLAP は、インストールされた後でも、SBL がアクティブ化されるようにユーザ プロファイル <profile.xml> ファイルが変更されるまでアクティブ化されません。AnyConnect プロファイルでの SBL の有効化 （75 ページ）を参照してください。アクティブ化後に、ユーザは [ユーザのスイッチ（Switch User）] をクリックし、さらに画面下右側の [ネットワーク接続（Network Connect）] アイコンをクリックして Network Connect コンポーネントを呼び出します。

（注） 誤ってユーザ インターフェイスの画面表示を最小化した場合は、Alt+Tab キーの組み合わせで元に戻ります。

PLAP を使用した Windows PC へのログオン

手順

ステップ 1 Windows のスタート画面で、Ctrl+Alt+Del キーの組み合わせを押します。

[ユーザのスイッチ（Switch User）] ボタンが表示されたログイン ウィンドウが表示されます。

ステップ 2 ユーザが [ユーザのスイッチ（Switch User）] をクリックします。[ネットワーク接続（Network Connect）] ウィンドウが表示されます。AnyConnect 接続によってすでに接続済みのユーザが [ユーザのスイッチ（Switch User）] をクリックしても、VPN 接続は解除されません。[ネットワーク接続（Network Connect）] をクリックすると、元の VPN 接続が終了します。[キャンセル（Cancel）] をクリックすると、VPN 接続が終了します。

ステップ 3 ウィンドウの右下にある [ネットワーク接続（Network Connect）] ボタンをクリックして、AnyConnect を起動します。AnyConnect のログオン ウィンドウが表示されます。

ステップ 4 この GUI を使用して通常どおりログインします。
この例は、AnyConnect がただ 1 つのインストール済み接続プロバイダーであることを前提としたものです。複数のプロバイダーをインストールしている場合は、このウィンドウに表示される項目の中から、ユーザが使用するものをいずれか 1 つ選択する必要があります。

ステップ 5 接続されると、[ネットワーク接続（Network Connect）] ウィンドウとほぼ同じ画面が表示されます。異なるのは、右下隅に表示されるのが Microsoft の [接続解除（Disconnect）] ボタンである点です。このボタンは、正常に接続されたことを通知するためだけのものです。

ステップ 6 各ユーザのログオン用アイコンをクリックします。
接続が確立したら、数分間以内にログオンします。約 2 分のアイドル タイムアウト後にユーザ ログオン セッションがタイムアウトし、AnyConnect PLAP コンポーネントに対して接続解除が発行され、VPN トンネルが接続解除されます。

PLAP を使用した AnyConnect からの接続解除

VPN セッションが正常に確立されると、PLAP コンポーネントは元のウィンドウに戻ります。このときウィンドウの右下隅には [接続解除（Disconnect）] ボタンが表示されます。

[接続解除（Disconnect）] をクリックすると、VPN トンネルが接続解除されます。

トンネルは、[接続解除（Disconnect）] ボタンの操作によって明示的に接続解除される以外に、次のような状況でも接続解除されます。

- ユーザが PLAP を使用して PC にログインした後で [キャンセル（Cancel）] を押した。
- ユーザがシステムへログインする前に PC がシャットダウンした。

- Windows でユーザ ログオン セッションがタイムアウトになり、[ログオンするには CTRL+ALT+DELを押してください（Press CTRL + ALT + DEL to log on）] 画面に戻った。

この動作は、Windows PLAP アーキテクチャの機能であり、AnyConnect の機能ではありません。

VPN 接続の自動リスタート

[自動再接続（Auto Reconnect）] が有効（デフォルト）になっている場合、AnyConnect は初期接続に使用したメディアに関係なく、VPNセッションの中断から回復し、セッションを再確立します。たとえば、有線、ワイヤレス、または3Gのセッションを再確立できます。[自動再接続（Auto Reconnect）] が有効になっている場合は、システムの一時停止またはシステムの再開が発生した場合の再接続動作も指定します。システムの一時停止とは、Windows の「休止状態」や macOS または Linux の「スリープ」など、低電力スタンバイのことです。システムの再開とは、システムの一時停止からの回復のことです。

[自動再接続（Auto Reconnect）] を無効にすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。この機能のデフォルト設定（有効）を使用することを強く推奨します。この設定を無効にすると、不安定な接続では VPN 接続の中断が発生することがあります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [自動再接続（Auto Reconnect）] を選択します。

ステップ 3 自動再接続の動作を選択します。

- [中断時に接続解除（Disconnect On Suspend）]：（デフォルト）AnyConnect では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムの再開後も再接続は試行されません。
- [再開後に再接続（Reconnect After Resume）]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムの再開後は再接続が試行されます。

Trusted Network Detection を使用した接続または接続解除

Trusted Network Detection について

Trusted Network Detection（TND）を使用すると、ユーザが社内ネットワークの中（信頼ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、社内ネットワークの

外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。

TND を使用している場合でも、ユーザが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザが信頼ネットワークに移動した場合だけです。たとえば、ユーザが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

（注） Network Visibility Module の TND 機能を設定するには、「Network Visibility Module」の章のNVM プロファイル エディタ （57 ページ）を参照してください。

TND は AnyConnect VPN クライアント プロファイルで設定します。ASA の設定の変更は必要ありません。AnyConnect が信頼ネットワークと非信頼ネットワークの間の遷移を認識したときに実施するアクションまたはポリシーを指定する必要があります。また、信頼ネットワークおよび信頼サーバを特定する必要があります。

Trusted Network Detection のガイドライン

- TND 機能は AnyConnect GUI を制御し、接続を自動的に開始するため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。
- さらに AnyConnect で Start Before Logon（SBL）が実行されている場合は、ユーザが信頼ネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。
- Always-Onが設定されているかどうかにかかわらず、Trusted Network Detection は、IPv4 ネットワークおよび IPv6 ネットワーク経由での ASA への IPv6 および IPv4 VPN 接続でサポートされています。
- ユーザ コンピュータ上に複数のプロファイルがあると、TND 設定が異なっている場合には問題になることがあります。

  ユーザが過去に TND 対応のプロファイルを受け取っていた場合、システムをリスタートすると、AnyConnect は最後に接続されたセキュリティ アプライアンスへの接続を試みますが、これが目的の動作ではないことがあります。別のセキュリティアプライアンスに接続するには、そのヘッドエンドを手動で接続解除してから、再接続する必要があります。この問題を回避する手段としては、次のような対策が考えられます。

  - 社内ネットワーク上にあるすべての ASA にロードされるクライアント プロファイルで、TND を有効にする。
  - すべての ASA がリストされた 1 つのプロファイルをホスト エントリ セクションに作成し、このプロファイルをすべての ASA にロードする。
  - 複数の異なるプロファイルが必要ない場合は、すべての ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 ASA により上書きされます。

- Linux 上で TND を使用するには、ネットワーク マネージャがインストールされてターゲット（RHEL/Ubuntu）デバイス上で正しく実行されていることと、ネットワーク インターフェイスがネットワーク マネージャによって管理されていることが必要です。

Trusted Network Detection の設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。

ステップ 3 [信頼されたネットワークポリシー（Trusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク（信頼ネットワーク）内に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続解除（Disconnect）]：（デフォルト）クライアントは、信頼ネットワークで VPN 接続を終了します。
- [接続（Connect）]：クライアントは、信頼ネットワークで VPN 接続を開始します。
- [何もしない（Do Nothing）]：クライアントは、信頼ネットワークでアクションを実行しません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection（TND）は無効となります。
- [一時停止（Pause）]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は（VPN セッションを接続解除するのではなく）一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

ステップ 4 [信頼されていないネットワークポリシー（Untrusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク外に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続（Connect）]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。
- [何もしない（Do Nothing）]：クライアントは、非信頼ネットワークの検出時にアクションを実行しません。このオプションを指定すると、Always-On VPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

ステップ 5 [信頼された DNS ドメイン（Trusted DNS Domains）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）を指定します。split-dns リストに複数の DNS サフィックスを追加し、ASA でデフォルト ドメインを指定した場合、複数の DNS サフィックスを割り当てることができます。

AnyConnect クライアントは、次の順序で DNS サフィックスのリストを構築します。

- ヘッド エンドから渡されたドメイン。
- ヘッド エンドから渡されたスプリット DNS リスト。
- パブリック インターフェイスの DNS サフィックス（設定されている場合）。設定されていない場合は、プライマリ DNS サフィックスの親サフィックスを伴うプライマリおよび接続固有のサフィックス（対応するボックスが拡張 TCP/IP 設定でオンの場合）。

照合する DNS サフィックス	TrustedDNSDomains に使用する値
example.com（のみ）	*example.com
example.com と anyconnect.example.com	*.example.com または example.com、anyconnect.example.com
asa.example.com と anyconnect.example.com	*.example.com または asa.example.com、anyconnect.example.com

ステップ 6 [信頼された DNS サーバ（Trusted DNS Servers）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるすべての DNS サーバ アドレス（カンマ区切りの文字列）。たとえば、203.0.113.1,2001:DB8::1 です。IPv4 および IPv6 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされています。

DNS で解決できるヘッドエンド サーバの DNS エントリが必要です。IP アドレスによる接続の場合、mus.cisco.com を解決できる DNS サーバが必要です。mus.cisco.com が DNS で解決できない場合、キャプティブ ポータルの検出が期待どおりに動作しません。

（注） TrustedDNSDomains、TrustedDNSServers、またはその両方を設定できます。TrustedDNSServers を設定する場合は、DNS サーバをすべて入力してください。その結果、サイトはすべて信頼ネットワークの一部になります。

アクティブ インターフェイスは、VPN プロファイルのすべてのルールが一致した場合に、信頼ネットワークに含まれると見なされます。

ステップ 7 信頼できる URL として追加するホスト URL を指定します。信頼できる証明書を使用してアクセス可能なセキュア Web サーバが、信頼できるサーバとして見なされる必要があります。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバが定義されていない場合、このフィールドは無効になります。

Always-Onを使用した VPN 接続の必要性

Always-On VPN について

Always-On操作により、VPNセッションがアクティブでない限り、コンピュータが信頼ネットワーク上にない場合にはインターネット リソースにアクセスできなくなります。この状況で VPN を常に適用すると、コンピュータがセキュリティに対する脅威から保護されます。

Always-Onが有効になっている場合、ユーザがログインした後、および非信頼ネットワークが検出されたときに、VPN セッションが自動的に確立されます。VPN セッションは、ユーザがコンピュータからログアウトするか、（ASA グループ ポリシーに指定された）セッション タイマーまたはアイドル セッション タイマーが期限に達するまではオープンした状態が維持されます。AnyConnect では、セッションがオープンしている場合は、それを再アクティブ化するために接続の再確立が継続して試行され、それ以外の場合は、新しい VPN セッションの確立が継続的に試行されます。

VPN プロファイルでAlways-Onが有効になっている場合、AnyConnect は他のダウンロードされたすべての AnyConnect プロファイルを削除してエンドポイントを保護し、ASA に接続するように設定されているパブリック プロキシを無視します。

Always-Onを有効にする場合は、次の AnyConnect オプションも考慮する必要があります。

- [ユーザにAlways-On VPN セッションの接続解除を許可（Allowing the user to Disconnect the VPN session）]：AnyConnect では、ユーザがAlways-On VPN セッションの接続を解除できます。**Allow VPN Disconnect** を有効にすると、AnyConnect では VPN セッションが確立された時点で [接続解除（Disconnect）] ボタンが表示されます。Always-On VPN を有効にすると、プロファイル エディタでは、[接続解除（Disconnect）] ボタンがデフォルトで有効になります。

  [接続解除（Disconnect）]ボタンを押すと、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。現在のVPNセッションでパフォーマンスが低下したり、VPNセッションの中断後に再接続で問題が発生したりした場合、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

- [接続障害ポリシーの設定（Setting a Connect Failure Policy）]：接続障害ポリシーにより、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかが決まります。「常時接続の接続障害ポリシーの設定」を参照してください。

- [キャプティブ ポータル ホットスポットの処理（Handling Captive Portal Hotspots）]：「キャプティブ ポータル ホットスポットの検出と修復の使用」を参照してください。

Always-On VPN の制限事項

- Always-Onがオンであっても、ユーザがログインしていない場合は、AnyConnect は VPN 接続を確立しません。AnyConnect が VPN 接続を確立するのは、ログイン後に限られます。
- Always-On VPN では、プロキシを介した接続はサポートされていません。

Always-On VPN のガイドライン

脅威に対する保護を強化するためにも、Always-On VPN の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- 認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。ASDM では、[アイデンティティ証明書（Identity Certificates）] パネル（[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] > [アイデンティティ証明書（Identity Certificates）]）に、公開証明書を容易に登録するための [ASA SSL VPN を Entrust で登録（Enroll ASA SSL VPN with Entrust）] ボタンが用意されています。
- フェールオーバー モードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- Always-On が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより、Always-Onポリシーを無視することができます。Always-Onの安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。
- Windows コンピュータ上の Cisco サブフォルダ（通常は `C:\ProgramData`）へのアクセスを制限します。
- 限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、AnyConnect プロファイル ファイルを削除できるため、Always-On機能を無効にすることができます。
- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。macOS ユーザに対してもこれに相当するものを事前に展開します。

Always-On VPN の設定

手順

ステップ 1 AnyConnect VPN クライアント プロファイルでのAlways-Onの設定 （85 ページ）。
ステップ 2 （任意）サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加。
ステップ 3 （任意）常時接続 VPN からのユーザの除外。

AnyConnect VPN クライアント プロファイルでのAlways-Onの設定

始める前に

Always-On VPN を使用するには、ASA 上に有効な信頼できるサーバ証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。また、サーバ証明書が厳格な証明書トラストモードを通過できるようにすると、Always-On VPN プロファイルのダウンロードを防止して不正なサーバへの VPN 接続をロックできます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。
ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。
ステップ 3 Trusted Network Detection の設定 （81 ページ）
ステップ 4 [常時接続（Always On）] を選択します。
ステップ 5 （任意）[VPN の接続解除を許可（Allow VPN Disconnect）] を選択または選択解除します。
ステップ 6 （任意）接続障害ポリシーの設定。
ステップ 7 （任意）キャプティブ ポータル修復の設定。

サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加

Always-On VPN は、AnyConnect VPN セッションのロード バランシングに影響を与えます。Always-On VPN を無効にした状態では、クライアントからロード バランシング クラスタ内のプライマリ デバイスに接続すると、クライアントはプライマリ デバイスから任意のバックアップ クラスタ メンバーにリダイレクションされます。Always-On を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがプライマリ デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロード バランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 ロードバランシング クラスタのプライマリ デバイスであるサーバを選択し、[編集（Edit）] をクリックします。

ステップ 3 いずれかのロード バランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

常時接続 VPN からのユーザの除外

Always-Onポリシーに優先して適用される除外規定を設定できます。たとえば、特定のユーザに対して他社との VPN セッションを確立できるようにしつつ、企業外資産に対してはAlways-On VPN ポリシーを除外するという場合があります。

ASA のグループ ポリシーおよびダイナミック アクセス ポリシーで設定された除外規定は Always-On ポリシーを上書きします。ポリシーの割り当てに使用される一致基準に従って例外を指定します。AnyConnect ポリシーでは Always-On が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

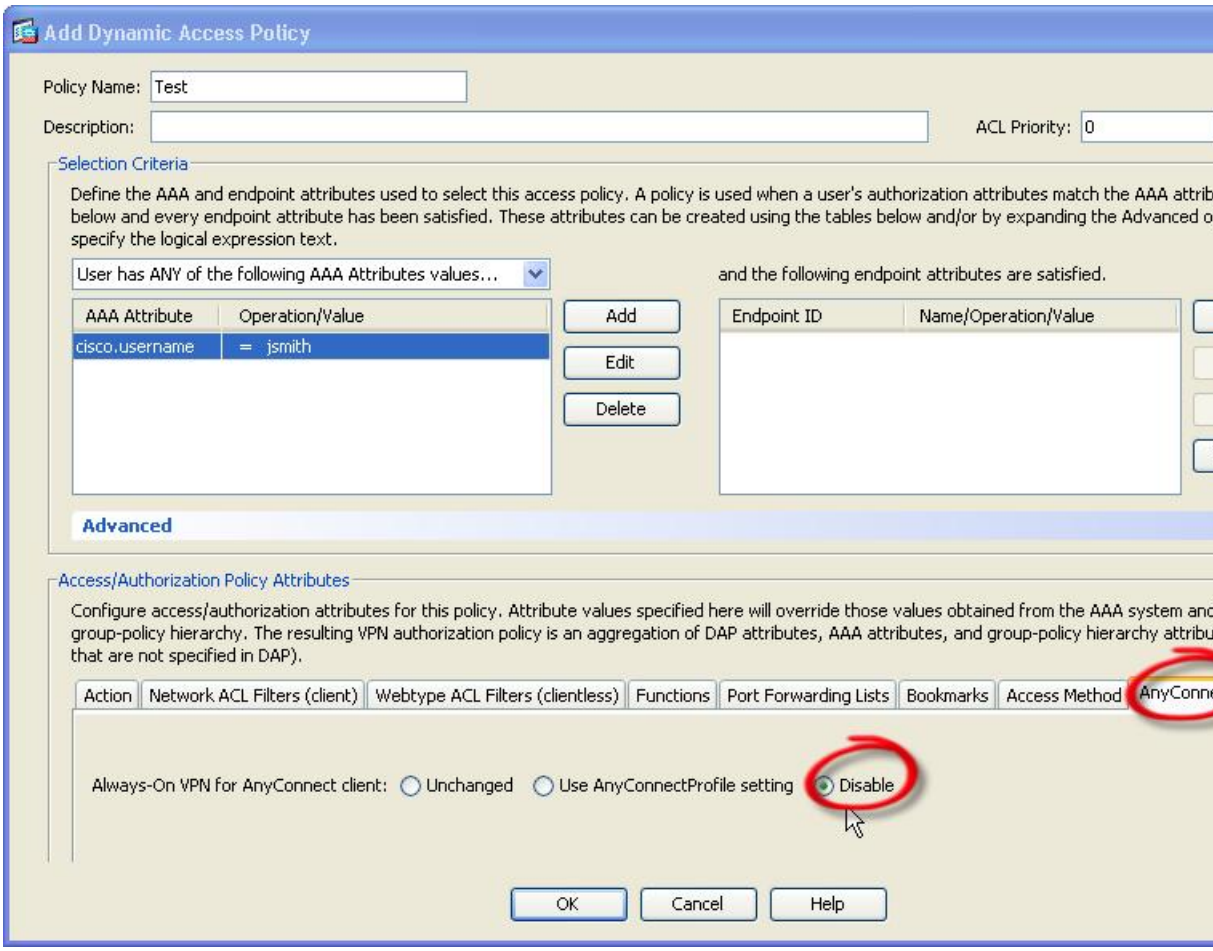
この手順では、AAA エンドポイント条件を使用して企業外資産にセッションを照合するダイナミック アクセス ポリシーを設定します。

手順

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）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

ステップ 2 ユーザをAlways-On VPN から除外する条件を設定します。たとえば、[選択基準（Selection Criteria）] 領域を使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3 [ダイナミック アクセス ポリシーの追加（Add Dynamic Access Policy）] ウィンドウまたは [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] ウィンドウの下半分にある [AnyConnect] タブをクリックします。



ステップ 4 [AnyConnect クライアントのAlways-On VPN（Always-On VPN for AnyConnect client）] の横にある [無効（Disable）] をクリックします。

常時接続の接続障害ポリシーの設定

接続障害ポリシーについて

接続障害ポリシーは、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかを決定します。これは、セキュア ゲートウェイに到達不能な場合、または AnyConnect がキャプティブ ポータル ホットスポットの存在を検出できない場合に発生する可能性があります。

オープン ポリシーは、最大限のネットワーク アクセスを許可します。これにより、インターネット リソースやその他のローカル ネットワーク リソースへのアクセスが必要なタスクをユーザが継続して実行できるようにします。

クローズド ポリシーは、VPN セッションが確立されるまで、すべてのネットワーク接続を無効にします。AnyConnect では、エンドポイントから、コンピュータが接続を許可されている

セキュア ゲートウェイ宛以外のトラフィックをすべてブロックするパケット フィルタを有効にすることで、この制限が実現されています。

AnyConnect では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。

接続障害ポリシーを設定するためのガイドライン

最大限のネットワーク アクセス権を許可するオープン ポリシーを使用する場合は、次の点を考慮してください。

- VPNセッションが確立されるまでセキュリティと保護は提供されません。したがって、エンドポイント デバイスが Web ベースのマルウェアに感染したり、センシティブ データが漏えいしたりする可能性があります。
- [接続解除（Disconnect）] ボタンが有効で、かつユーザが [接続解除（Disconnect）] をクリックした場合は、オープン接続障害ポリシーは適用されません。

VPNセッションが確立されるまですべてのネットワーク接続を無効にする終了ポリシーを使用する場合は、次の点を考慮してください。

- ユーザが VPN の外部へのインターネット アクセスを必要とする場合に、クローズド ポリシーを適用すると、生産性が低下する可能性があります。
- クローズドの目的は、エンドポイントを保護するプライベート ネットワークのリソースが使用できない場合に、ネットワークの脅威から企業資産を保護することです。スプリット トンネリングによって許可されたプリンタやテザー デバイスなどのローカル リソースを除き、すべてのネットワーク アクセスが禁止されるため、エンドポイントは Web ベースのマルウェアとセンシティブ データ漏えいから常に保護されます。
- このオプションは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する組織向きです。
- クローズドポリシーは、特に有効にしない限り、キャプティブ ポータルを修復しません。
- クライアント プロファイルで [最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] が有効になっている場合は、直近の VPN セッションにより適用されたローカル リソース ルールを適用できます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。
- AnyConnect ソフトウェアのアップグレード中、Always-Onが有効であると、ネットワークはクローズド ポリシーに関係なくブロックが解除され、開かれます。
- クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープン ポリシーを使用してAlways-Onを展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

⚠

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。接続障害クローズドポリシーは、細心の注意を払って実装してください。

接続障害ポリシーの設定

Always-On 機能を有効にする場合にのみ、接続障害ポリシーを設定します。デフォルトでは、接続障害ポリシーはクローズされており、VPN が到達不能な場合にはインターネットにアクセスできません。この状況でインターネットへのアクセスを許可するには、オープンするように接続障害ポリシーを設定する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [Connect Failure Policy（接続エラーポリシー）] パラメータを次のいずれかに設定します。

- [クローズド（Closed）]：（デフォルト）セキュア ゲートウェイに接続できない場合、ネットワーク アクセスが制限されます。
- [オープン（Open）]：クライアントがセキュア ゲートウェイに接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。

ステップ 3 クローズド ポリシーを指定した場合は、次の手順を実行します。

a) キャプティブ ポータル修復の設定。

b) ネットワーク アクセスが無効になっている間、最後の VPN セッションのローカル デバイス ルールを保持する場合は、[最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] を選択します。

キャプティブ ポータル ホットスポットの検出と修復の使用

キャプティブ ポータルについて

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、キャプティブ ポータルと呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。キャプティブ ポータルの検出はこの制限を認識することであり、キャ

プティブ ポータル修復はネットワーク アクセスを取得するためにキャプティブ ポータルのホットスポット要件を満たすプロセスです。

キャプティブ ポータルは、VPN 接続が開始されると AnyConnect によって自動的に検出され、追加設定は必要ありません。また、AnyConnect は、キャプティブ ポータルの検出中にブラウザの設定を変更せず、キャプティブ ポータルを自動的に修復しません。修復は、エンド ユーザが実行します。AnyConnect は、現在の設定に応じてキャプティブ ポータルの検出に対応します。

- Always-On が無効の場合、または Always-On が有効で接続障害ポリシーが開いている場合、各接続試行時に次のメッセージが表示されます。

  ```
  The service provider in your current location is restricting access to the Internet.
   You need to log on with the service provider before you can establish a VPN session.
   You can try this by visiting any website with your browser.
  ```

  エンドユーザは、ホットスポットプロバイダーの要件を満たすことで、キャプティブポータル修復を実行する必要があります。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

- Always-On が有効で、接続障害ポリシーが閉じている場合、キャプティブ ポータル修復を明示的に有効にする必要があります。有効の場合、エンドユーザは修復を前述のように実行できます。無効の場合、各接続試行時に次のメッセージが表示され、VPN に接続できません。

  ```
  The service provider in your current location is restricting access to the Internet.
   The AnyConnect protection settings must be lowered for you to log on with the service
   provider. Your current enterprise security policy does not allow this.
  ```

キャプティブ ポータル修復の設定

Always-On 機能を有効にし、接続障害ポリシーをクローズドに設定する場合にのみ、キャプティブ ポータル修復を設定します。この場合、キャプティブ ポータルのために VPN に接続できないときは、キャプティブ ポータル修復を設定すると、AnyConnect は VPN に接続できます。

（注） このプラットフォームでは常時接続がサポートされていないため、キャプティブ ポータルの修復の設定は Linux に適用されません。したがって、プロファイル エディタでの [キャプティブ ポータルの修復を常に許可（Allow Captive Portal Remediation Aloways On）] の設定に関係なく、Linux ユーザはキャプティブ ポータルを修復できます。

接続障害ポリシーがオープンに設定されているか、または Always-On が有効でない場合、ユーザはネットワーク アクセスが制限されないため、AnyConnect VPN クライアント プロファイルに特定の設定がなくてもキャプティブ ポータルを修復できます。

デフォルトでは、セキュリティを最大化するために、常時接続をサポートしているプラットフォーム（Windows と macOS）上ではキャプティブ ポータルの修復は無効になっています。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [キャプティブ ポータルの修復を許可（Allow Captive Portal Remediation）] .を選択します。

この設定は、クローズ接続障害ポリシーによるネットワーク アクセス制限を解除します。

ステップ 3 修復タイムアウトを指定します。

AnyConnect がネットワーク アクセス制限を解除する時間（分単位）を入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

キャプティブ ポータルの修復の強化（Windows のみ）

キャプティブ ポータルの修復が強化され、AnyConnect によって制限されているネットワーク アクセス（常時接続などのよる）を伴うキャプティブ ポータルが検出されるたびに、AnyConnect の組み込みブラウザが修復に使用されます。その他のアプリケーションは、AnyConnect ブラウザでのキャプティブ ポータルの修復が保留中の間、ネットワーク アクセスがブロックされたままになります。ユーザは AnyConnect ブラウザを閉じて、外部ブラウザにフェールオーバーできます（プロファイルで有効になっている場合）。これにより、AnyConnect は通常のキャプティブ ポータルの修復動作に戻ります。その場合に、次のメッセージが表示されます。

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

キャプティブ ポータルが検出されたものの、ネットワーク アクセスが AnyConnect によって制限されている場合、AnyConnect ブラウザが自動的に起動し、ユーザに修復を求める次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the internet. You
 need to log on with the service provider before you establish a VPN session, using the
 AnyConnect browser.
```

キャプティブ ポータルの修復の設定ブラウザのフェールオーバー

キャプティブ ポータルの修復のために AnyConnect ブラウザが起動するたびに適用されるようにブラウザのフェールオーバーを設定することができます。ブラウザのフェールオーバーを設定することで、ユーザは AnyConnect ブラウザを閉じた後に外部ブラウザを介してキャプティブ ポータルを修復できます。

キャプティブ ポータルの修復のために起動した AnyConnect ブラウザには、サーバ セキュリティ証明書に関して厳密なセキュリティ設定が備わっています。キャプティブ ポータルの修復中は、信頼されていないサーバ証明書は受け入れられません。信頼できないサーバ証明書が検出されると、対応する HTTPS URL が AnyConnect ブラウザによってロードされず、修復プロセスがブロックされる可能性があります。キャプティブ ポータルの修復中に信頼できないサーバ証明書が受け入れられる場合は、キャプティブ ポータルの修復ブラウザのフェールオーバーを有効にしてユーザがキャプティブ ポータルを修復できるようにする必要があります。有効に

すると、ユーザはAnyConnectブラウザを閉じ、（AnyConnectは通常のキャプティブ ポータルの修復動作に戻るため）外部ブラウザを使用して修復を継続することができます。

始める前に

Windows でのみサポートされています。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 エンド ユーザが（AnyConnect ブラウザを閉じた後）キャプティブ ポータルの修復に外部ブラウザを使用させる場合は、[キャプティブ ポータルの修復ブラウザのフェールオーバー（Captive Portal Remediation Browser Failover）] をオンにします。デフォルトでは、エンド ユーザは AnyConnect ブラウザを使用してキャプティブ ポータルの修復のみを行えます。つまり、ユーザは強化されたキャプティブ ポータルの修復を無効にすることはできません。

キャプティブ ポータルの検出と修復のトラブルシューティング

次のような状況では、誤ってキャプティブ ポータルと見なされる場合があります。

- AnyConnectが、サーバ名が正しくない証明書（CN）を持ったASAに接続しようとしている場合、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。

  これを回避するには、ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアント プロファイルの ASA サーバの名前と一致する必要があります。

- ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる ASA への接続に応答すると、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。これは、ユーザが内部ネットワークに存在し、ファイアウォールを介して ASA に接続している場合に発生する可能性があります。

  企業内から ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。ASA への HTTP/HTTPS アクセスは許可するか、完全にブロック（ブラック ホール化とも呼ばれます）し、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、次のことを試すようにユーザに指示してください。

- 修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP フォン クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。

  キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、DoS 攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

- ネットワーク インターフェイスを無効にした後、再度有効にします。このアクションにより、キャプティブ ポータルの検出が再試行されます。

- コンピュータを再起動します。

AnyConnect over L2TP または PPTP の設定

一部の国の ISP では、Layer 2 Tunneling Protocol（L2TP）や Point-to-Point Tunneling Protocol（PPTP）のサポートが必要です。

セキュア ゲートウェイを宛先としたトラフィックを Point-to-Point Tunneling Protocol（PPP）接続上で送信するため、AnyConnect は外部トンネルが生成したポイントツーポイント アダプタを使用します。PPP 接続上で VPN トンネルを確立する場合、クライアントでは ASA より先を宛先としてトンネリングされたトラフィックから、この ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、除外ルートを特定する方法を指定する場合は、AnyConnect プロファイルの [PPP 除外（PPP Exclusion）] 設定を使用します。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [PPP 除外（PPP Exclusion）] でその方式を選択します。また、このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザがこの設定を表示および変更できるようにします。

- [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。

- [上書き（Override）]：同様に PPP 除外を有効にします。自動検出で PPP サーバの IP アドレスを取得できず、[PPP 除外（PPP Exclusion）] の [ユーザ制御可（User Controllable）] の値が true である場合は、次項の説明に従ってこの設定を使用するよう、ユーザに指示してください。

- [無効（Disabled）]：PPP 除外は適用されません。

ステップ 3 [PPP 除外サーバ IP（PPP Exclusion Server IP）] フィールドに、接続に使用する PPP サーバの IP アドレスを入力します。このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザが preferences.xml ファイルを利用して PPP サーバの IP アドレスを変更できるようにします。

次のタスク

preferences.xml ファイルの変更については、「ユーザに対する PPP 除外上書きの指示」の項を参照してください。

ユーザに対する PPP 除外上書きの指示

自動検出が機能しない場合に、PPP除外フィールドをユーザ設定可能に設定すると、ユーザはローカル コンピュータ上で AnyConnect プリファレンス ファイルを編集することにより、これらの設定を上書きすることができます。

手順

ステップ 1 メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows：%LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。次に例を示します。
- macOS：/Users/username/.anyconnect
- Linux：/home/username/.anyconnect

ステップ 2 PPPExclusion の詳細を `<ControllablePreferences>` の下に挿入して、Override 値と PPP サーバの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3 ファイルを保存します。

ステップ 4 AnyConnect を終了して、リスタートします。

管理 VPN トンネルの使用

管理 VPN トンネルについて

管理VPNトンネルにより、エンドユーザによってVPN接続が確立されるときだけでなく、クライアント システムの電源が入るたびに社内ネットワークの接続が確保されます。オフィスネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログイン スクリプトに対するメリットもあります。

管理 VPN トンネルはエンド ユーザに対し透過的であるため、ユーザ アプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

管理トンネル機能が有効として検出されると、制限付きのユーザアカウント（ciscoacvpnuser）が作成され、最小権限の原則が適用されます。このアカウントは、AnyConnect のアンインストール中、またはインストールのアップグレード中に削除されます。

ログインが低速であるとユーザから報告された場合、管理トンネルが適切に設定されていない可能性があります。「管理 VPN トンネルの設定 （97 ページ）」で、この機能を有効にするのに必要な設定手順について説明します。この設定を行ったにもかかわらず、社内ネットワークへの接続ができない症状が出ている場合は、「管理 VPN トンネル接続問題のトラブルシューティング」を参照してください。

管理 VPN トンネルの互換性と要件

- ASDM 9.0.1（またはそれ以降）および ASDM 7.10.1（またはそれ以降）が必要です。
- ユーザ ログインの前後にユーザによって開始された VPN トンネルが切断されるたびに接続します。

（注） 信頼ネットワーク検出（TND）機能によって信頼ネットワークが検出されるか、AnyConnect ソフトウェア アップデートが進行中の場合、管理 VPN トンネルは確立されません。

- ユーザ ログインの前後にユーザが VPN トンネルを開始するたびに切断します。
- マシン ストア証明書認証のみを使用します。
- ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンドユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作をオーバーライドする場合は、「Tunnel-All 設定をサポートするカスタム属性の設定 （100 ページ）」を参照してください。
- サーバ証明書に対して厳密な証明書のチェックを実行します。サーバー証明書のルート CA 証明書は、マシン証明書ストア（Windows の場合はコンピュータ証明書ストア、macOS

の場合はシステム キーチェーンまたはシステム ファイル証明書ストア）に存在する必要があります。

- バックアップ サーバ リストで作業します。
- 現在 Windows および macOS でのみ入手可能です。以降のリリースでは、Linux のサポートが追加されます。

管理 VPN トンネルの非互換性と制限

- 管理 VPN プロファイルはプロキシ設定の値 [ネイティブ（Native）] をサポートしていません。この制限は、管理 VPN トンネルはユーザがログインしていなくても開始できるため、 Windows クライアントにのみ適用されます。 そのため、ユーザ固有のブラウザ プロキシ設定に依存することはできません。
- 管理 VPN プロファイルは、VPN サーバからプッシュされるプライベート プロキシ設定をサポートしません。管理 VPN トンネルはエンド ユーザに対して透過的であることを目的としているため、ユーザ固有の設定またはシステム プロキシ設定は変更されません。
- ユーザの VPN トンネルが非アクティブになるたびに管理 VPN トンネルが確立されるため、Always On 機能と互換性はありません。ただし、すべてのトラフィックをトンネリングするように管理トンネル接続のグループ ポリシーを設定して、ユーザの VPN トンネルが非アクティブの間にトラフィックが物理インターフェイスによってリークされないようにすることができます。「Tunnel-All 設定をサポートするカスタム属性の設定 （100 ページ）」を参照してください。
- キャプティブ ポータルの修復は、AnyConnect UI が実行中でユーザがログインしている間、管理 VPN トンネル機能が有効になっていなかったかのようであるときにのみ実行されます。
- 管理VPNプロファイルの設定は、管理VPNトンネルがアクティブのときにのみAnyConnectで適用されます。管理VPNトンネルが切断されると、ユーザのVPNトンネルプロファイル設定のみが適用されます。このため、管理VPNトンネルはユーザのVPNトンネルプロファイルの信頼ネットワーク検出（TND）設定（つまり、設定済みの信頼できないネットワーク ポリシーに関係なく TND が無効化されるか、「信頼できないネットワーク」が検出された場合）に従って開始されます。また、管理VPNプロファイルにおける TND 接続アクションは（管理 VPN トンネルがアクティブである場合にのみに適用）、管理 VPN トンネルがエンド ユーザに対して透過的であるように常にユーザの VPN トンネルに適用されます。ユーザエクスペリエンスに一貫性をもたせるために、ユーザと管理の両方のVPNトンネル プロファイルで同じ TND 設定を使用することをお勧めします。

管理 VPN プロファイルによって適用される必須設定

特定のプロファイル設定は管理 VPN トンネルがアクティブである間は必須です。有効なプロファイルの設定をサポートするために、対応する UI 制御を無効にすることで、AnyConnect 管理VPNプロファイルエディタにより必須設定が適用されます。主に、ユーザのインタラクションを排除してトンネルの中断を最小限に抑えるために、管理トンネルの接続中に次の設定値が上書きされます。

- *AllowManualHostInput: false*：管理トンネル (ヘッドレス クライアント) に関連しません。

- *AlwaysOn: false*：管理トンネルが切断されるたびにユーザのトンネル プロファイル設定が適用されるため、関連しません。
- *AutoConnectOnStart: false*：以前に接続されたホストに対する起動時の自動接続用 UI クライアントにのみ関連します。
- *AutomaticCertSelection: true*：証明書の選択ポップアップを回避します。
- *AutoReconnect: true*：ネットワークの変更時に管理トンネルが終了するのを回避します。
- *AutoReconnectBehavior: ReconnectAfterResume*：ネットワークの変更時に管理トンネルの終了を回避します。
- *AutoUpdate: false*：管理トンネル接続中にソフトウェア アップデートは実行されません。
- *BlockUntrustedServers: true*： 信頼できないサーバ証明書のプロンプトを回避します。
- *CertificateStore: MachineStore*：管理トンネル認証はログイン ユーザなしでも成功する必要があります。
- *CertificateStoreOverride: true*：Windows でのマシン証明書認証に必要です。
- *EnableAutomaticServerSelection: false*：管理 VPN プロファイルではホスト エントリは 1 つのみです。
- *EnableScripting: false*：AnyConnect カスタマイゼーション スクリプト（接続時または切断時に呼び出される）は管理トンネル接続中は実行されません。
- *MinimizeOnConnect:false*：管理トンネル（ヘッドレス クライアント）に関連しません。
- *RetainVPNOnLogoff:true*: 管理トンネルはユーザがログオフしてもアクティブなままである必要があります。
- *ShowPreConnect Message*：管理トンネル（ヘッドレス クライアント）に関連しません。
- *UserEnforcement: AnyUser*：特定のユーザがログインしたときに管理トンネルが切断されないようにします。
- *UseStartBeforeLogon:False*：ユーザ トンネルにのみ適用されます。
- *WindowsVPNEstablishment: AllowRemote* ユーザ：どのユーザ タイプ（ローカルまたはリモート）がログインしても管理トンネルが影響されないようにします。

また、AnyConnect では、管理トンネルの接続中は、WindowsLogonEnforcement および SCEP 関連の設定はプロファイル設定として適用されません。

管理 VPN トンネルの設定

ユーザがログインしていなくても管理トンネル接続が発生する場合があるため、マシン ストア証明書認証のみがサポートされます。したがって、少なくとも 1 つの関連するクライアント証明書がクライアント ホストのマシン証明書ストアで使用できる必要があります。

管理 VPN トンネルのトンネル グループの設定

トンネル グループの認証方法は、ASDM で**[設定（Configuration）] > [リモート アクセス（Remote Access）] > [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）] > [追加/編集（Add/Edit）]** に移動し、[証明書のみ（certificate only）] として設定する必要があります。次に、[詳細設定（Advanced）] > [グループ エイリアス/グループ URL（Group Alias/Group URL）] でグループ URL を設定してから、次に 「管理 VPN トンネルのプロファイルの作成 （98 ページ）」 の説明に従って管理 VPN プロファイルで指定します。

このトンネル グループのグループ ポリシーには、トンネル グループで設定されたクライアント アドレスの割り当てを使用するすべての IP プロトコルに対して split include トンネリングが設定されている必要があります（ASDM から [下記のネットワーク リストをトンネル（Tunnel Network List Below）] **[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）] > [グループ ポリシー（Group Policies）] > [編集（Edit）] > [詳細設定（Advanced）** > **[スプリット トンネリング（Split Tunneling）]を選択）。**> Tunnel-All 設定をサポートするカスタム属性の設定 （100 ページ）「」では、その他のスプリット トンネリング設定のサポートを有効にする方法について説明します。両方の IP プロトコルに対するトンネル グループでクライアント アドレスの割り当てが設定されていない場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] を有効にし、クライアント アドレスの割り当てのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。

管理 VPN トンネルのプロファイルの作成

特定のクライアント デバイスには、1 つの管理 VPN プロファイルのみを展開できます。管理 VPN プロファイルは固定名（VpnMgmtTunProfile.xml）で専用ディレクトリ（Windows では %ProgramData%\Cisco\Cisco AnyConnect Secure MobilityClient\Profile\MgmtTun、macOS では /opt/cisco/anyconnect/profile/mgmttun）に格納されます。管理 VPN プロファイルには、「管理 VPN トンネルのトンネル グループの設定 （98 ページ）」セクションに従って設定されたトンネル グループを指しているゼロまたは 1 つのホスト エントリを使用できます。（トンネル確立中のプロファイルの更新時に）この機能を自動的に無効にするには、管理 VPN プロファイルでゼロのホスト エントリを設定する必要があります。

始める前に

管理 VPN トンネルのトンネル グループの設定 （98 ページ）を完了します。

手順

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 クライアント プロファイル（AnyConnect Client Profile）] の順に移動します。

ステップ 2 [追加（Add）] をクリックすると、[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profiles）] ウィンドウが表示されます。

ステップ 3 プロファイルの使用方法として、[AnyConnect 管理 VPN プロファイル（AnyConnect Management VPN Profile）] を選択します。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profiles）] 画面でフィールドを読み込む方法の詳細については、『Cisco ASA Series VPN ASDM Configuration Guide』の「Configure AnyConnect Client Profiles」セクションを参照してください。

ステップ 4 「管理 VPN トンネルのトンネル グループの設定 （98 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックして管理 VPN プロファイルを作成してから、[編集（Edit）] をクリックして設定します。以降の更新に対しても同様に行います。

（オプション）すでに設定済みの管理 VPN プロファイルをアップロードする

すでに設定済みの管理 VPN プロファイル（スタンドアロン AnyConnect 管理 VPN プロファイル エディタを使用して編集または作成された、AnyConnect システムからコピーされた、または別の ASA からエクスポートされた）を ASA にアップロードする必要がある場合があります。

手順

ステップ 1 ASDM で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ウィンドウから [追加（Add）]、[アップロード（Upload）] をクリックします。.
ファイルのアップロードの接続先の場所を選択するには、 *vpnm* 拡張子付きのプロファイルを選択することを確認します。

ステップ 2 プロファイル名を提供し、プロファイルの使用率のドロップダウン メニューから **AnyConnect 管理 VPN プロファイル**を選択します。

ステップ 3 「管理 VPN トンネルのトンネル グループの設定 （98 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックし、管理 VPN プロファイルを作成します。

グループ ポリシーへの管理 VPN プロファイルの関連付け

管理トンネル接続に使用するトンネル グループに関連付けられているグループ ポリシーに管理 VPN プロファイルを追加する必要があります。

（注） 同様に、ユーザ トンネル接続に使用する正規のトンネル グループにマッピングされたグループ ポリシーに管理 VPN プロファイルを追加することもできます。ユーザが接続すると、グループ ポリシーにすでにマッピングされているユーザ VPN トンネルとともに管理 VPN プロファイルがダウンロードされ、管理 VPN トンネル機能が有効になります。

また、アウト オブ バンドで管理 VPN プロファイルを展開することができます。その場合、VpnMgmtTunProfile.xml という名前が付いていることを確認し、上記の管理 VPN プロファイル ディレクトリにコピーして、Cisco AnyConnect セキュア モビリティ エージェント サービスを再起動（またはリブート）します。

始める前に

「管理 VPN トンネルのトンネル グループの設定 （98 ページ）」と「管理 VPN トンネルのプロファイルの作成 （98 ページ）」を完了します。

手順

ステップ 1 ASDM で **[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]** に移動します。

ステップ 2 ダウンロードするクライアント プロファイルで、[追加（Add）] をクリックし、「管理 VPN トンネルのプロファイルの作成 （98 ページ）」セクションで作成または更新された管理 VPN プロファイルを選択します。

Tunnel-All 設定をサポートするカスタム属性の設定

管理 VPN トンネルでは、ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンド ユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作は管理トンネル接続で使用されているグループ ポリシーで次のカスタム属性を設定することによりオーバーライドできます（[CreateCustom 属性 ASDM（CreateCustom Attribute ASDM）] ウィンドウ：**[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）] > [グループ ポリシー（Group Policies）] > [編集（Edit）] > [詳細設定（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）] > [追加（Add）]**）。

属性名と値の両方を *true* に設定すると、両方の IP プロトコルの設定が tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、 AnyConnect は管理トンネルの接続に進みます。

管理 VPN プロファイルの更新の制限

管理 VPN プロファイルの更新を新しい AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）設定を使用した特定の信頼できるサーバ リストに制限しても、ユーザが任意のサーバから VPN プロファイルを更新するのを許可することができます。この設定は、[ローカル ポリシー パラメータと値（AnyConnect VPN Local Policy Editor）] を使用して [任意のサーバからの管理 VPN プロファイル更新を許可（Allow Management VPN Profile Updates From AnyServer）] チェック ボックスをオンにすることで編集できます。

たとえば、管理 VPN プロファイルの更新が VPN サーバ TrustedServer からのみ許可される場合、このチェック ボックスはオフになっており、TrustedServer は信頼できるサーバ リストに追加されます。（TrustedServer を該当する VPN プロファイルのサーバ エントリに存在する FQDN または IP アドレスと置き換えてください）。

管理 VPN トンネル接続問題のトラブルシューティング

クライアント ホストがリモートから到達できない場合、さまざまなシナリオが発生して管理 VPN トンネルの切断や確立できない状況の原因となっている可能性があります。次のシナリオでは、AnyConnect VPN GUI と CLI に管理接続状態が統計情報のエントリとして反映されます。

- [切断（無効）（Disconnected (disabled)）]：機能は無効です。
- [切断（信頼ネットワーク）（Disconnected (trusted network)）]：TND が信頼ネットワークを検出したため、管理トンネルは確立されません。
- [切断（アクティブ ユーザ トンネル）（Disconnected (user tunnel active)）]：ユーザ トンネルは現在保留中 です（つまり、管理トンネルを切断しています）。
- [切断（プロセスの起動に失敗）（Disconnected (process launch failed)）]：管理トンネル接続の試行時にプロセスの起動エラーが発生しました。
- [切断（接続に失敗）（Disconnected (connect failed)）]：管理トンネルの確立時に接続障害が発生しました。
- [切断された（無効な VPN 設定）（Disconnected (invalid VPN configuration)）]：管理トンネルの確立時に無効なスプリット トンネリング設定が発生しました。追加情報については、「Tunnel-All 設定をサポートするカスタム属性の設定 （100 ページ）」を参照してください。
- [切断（ソフトウェア アップデートが保留中）（Diconnected (software update pending)）]：AnyConnect ソフトウェア アップデートは現在保留中です（つまり、管理トンネルを切断しています）。
- [切断（Disconnected）]：管理トンネルを確立しようとしているか、その他の理由により確立できませんでした。

管理 VPN トンネル経由の接続の欠落をトラブルシューティングする場合は（クライアント ホストで確立されることを想定）、次を確認します。

- 管理 VPN 接続の状態を AnyConnect UI の [統計出力のエクスポート（Export Stats output）] の [統計（Statistics）] タブをで確認するか、CLI で [接続情報/管理接続状態（Connection Information/Management Connection State）] を確認します。管理接続状態が予期せずに [切断（disconnected）] と表示され、提供された説明が不十分な場合、詳細なトラブルシューティングについて DART ツールを使用した AnyConnect ログをキャプチャします。
- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、証明書認証で設定されたトンネル グループを指す、1 つのホスト エントリで管理 VPN プロファイルが設定されていることを確認します。関連付けられているグループ ポリシーに 1 つのプロファイル（管理 VPN プロファイル）が設定されている必要があります。

（注） 関連付けられているグループ ポリシーでバナーを有効にすることはできません。管理のトンネル接続中にユーザのインタラクションはサポートされていません。

- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、正規のユーザ トンネル接続で使用されるトンネル グループに関連付けられているグループ ポリシー内で管理 VPN プロファイルが設定されていることを確認します。ユーザがそのトンネル グループに接続すると、管理 VPN プロファイルがダウンロードされ、この機能が有効になります。

（注） また、管理 VPN プロファイルをアウト オブ バンドで展開できます。

- UI の統計行に [管理接続状態：切断（接続に失敗）（Management Connection State: Disconnected (connect failed)）] と表示される場合、次に示すように、管理トンネル接続はユーザのインタラクションが必要な場合に常に失敗することに注意してください。
  - サーバ証明書が信頼されない場合。サーバ証明書のルート CA 証明書は、マシン証明書ストア内に存在する必要があります。
  - （マシン ストア証明書に関連する）秘密キーがパスワードで保護されている場合、対応するクライアント証明書は管理トンネル接続で使用できません。秘密キーのパスワードを入力するようユーザにプロンプトを表示できないため、クライアント証明書は使用できません。
  - macOS システム キーチェーン プライベート キーが、AnyConnect VPN エージェント実行可能ファイル（vpnagentd）にプロンプトを表示せずにアクセスを許可するように設定されていない場合、秘密鍵にアクセスするための資格情報をユーザに要求することができないため、対応するクライアント証明書は管理トンネル接続では使用できません。
  - グループ ポリシーがバナーを使用して設定されている場合。

AnyConnect プロキシ接続の設定

AnyConnect プロキシ接続について

AnyConnect は、ローカル プロキシ、パブリック プロキシ、プライベート プロキシで VPN セッションをサポートしています。

- ローカル プロキシ接続：

ローカル プロキシは、AnyConnect と同じ PC 上で動作し、トランスペアレント プロキシとして使用されることもあります。トランスペアレント プロキシ サービスの例として、一部のワイヤレスデータ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェア（Kaspersky など）に搭載のネットワーク コンポーネントなどがあります。

ローカル プロキシの使用は、AnyConnect VPN クライアント プロファイルで有効または無効にします。「ローカル プロキシ接続の許可」を参照してください。

- パブリック プロキシ接続：

  通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。Windows がパブリック プロキシを使用するように設定されている場合、AnyConnect はその接続を使用します。パブリック プロキシは macOS と Linux でネイティブと上書きの両方をサポートしています。

  パブリック プロキシの設定については、パブリック プロキシ接続の設定（Windows）に関する説明を参照してください。

- プライベート プロキシ接続：

  プライベートプロキシサーバは、企業の使用ポリシーに基づいて企業ユーザが特定の Web サイト（たとえば、アダルト、ギャンブル、ゲームなどのサイト）にアクセスできないようにするために社内ネットワークで使用されます。

  トンネルの確立後にブラウザにプライベート プロキシ設定をダウンロードするようにグループ ポリシーを設定します。VPN セッションが終了すると、設定は元の状態に復元されます。プライベート プロキシ接続の設定 （106 ページ）を参照してください。

（注） プロキシ サーバを経由する AnyConnect SBL 接続は、Windows オペレーティング システムのバージョン、システム（マシン）の設定、またはその他のサードパーティ プロキシ ソフトウェア機能に依存します。このため、Microsoft または使用するすべてのサードパーティ プロキシ アプリケーションによって提供される、システム全体のプロキシ設定を参照してください。

VPN クライアント プロファイルによるクライアント プロキシの制御

VPN クライアント プロファイルでは、クライアント システムのプロキシ接続をブロックしたり、リダイレクトしたりできます。Windows および Linux の場合、パブリック プロキシ サーバのアドレスを自分で設定したり、ユーザに設定を許可したりできます。

VPN クライアントプロファイルにプロキシ設定を設定する方法の詳細については、「AnyConnect プロファイル エディタ、プリファレンス（Part 2）」を参照してください。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

ASA の一部のバージョンでは、AnyConnect セッションが確立された後も、プロキシ サーバを経由するクライアントレス ポータル アクセスをサポートするために、AnyConnect 設定が必要です。AnyConnect では、この設定が行われるように、プロキシ自動設定（PAC）ファイルを使用してクライアント側プロキシ設定が修正されます。AnyConnect でこのファイルが生成されるのは、ASA でプライベート側プロキシ設定が指定されていない場合だけです。

AnyConnect プロキシ接続の要件

プロキシ接続の OS サポートは次のようになります。

プロキシ接続タイプ	Windows	macOS	Linux
ローカル プロキシ	○	○（上書きおよびネイティブ）	○
プライベートプロキシ	○（Internet Explorer）	○（システム プロキシ設定として設定）	×
パブリック プロキシ	○（IE および上書き）	○（上書きおよびネイティブ	○（上書きおよびネイティブ）

プロキシ接続の制限

- IPv6 プロキシは、プロキシ接続のどのタイプでもサポートされません。
- プロキシ経由の接続は、Always-On機能が有効になっている場合にはサポートされません。
- ローカル プロキシへのアクセスを許可するには、VPN クライアント プロファイルが必要です。

ローカル プロキシ接続の許可

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [ローカル プロキシ接続を許可（Allow Local Proxy Connections）] を選択（デフォルト）または選択解除します。ローカル プロキシはデフォルトで無効になっています。

パブリック プロキシ

パブリック プロキシはWindowsおよびLinuxの各プラットフォームでサポートされています。プロキシ サーバは、クライアント プロファイルで設定されるプリファレンスに基づいて選択

されます。プロキシ オーバーライドの場合、AnyConnect はプロファイルからプロキシ サーバを取得します。リリース 4.1 では、Linux および macOS でのネイティブ プロキシ設定とともに Mac でのプロキシ サポートが追加されました。

Linux では、AnyConnect の実行前にネイティブ プロキシ設定がエクスポートされます。設定を変更した場合は、再起動が必要です。

プロキシ サーバの認証には、ユーザ名とパスワードが必要です。AnyConnect は、プロキシ サーバが認証を必要とするように設定されている場合、基本認証および NTLM 認証をサポートします。AnyConnect ダイアログが認証プロセスを管理します。プロキシ サーバに対する認証に成功すると、AnyConnect は ASA ユーザ名およびパスワードの入力を求めます。

パブリック プロキシ接続の設定（Windows）

Windows でパブリック プロキシ接続を設定するには、次の手順を実行します。

手順

ステップ 1 Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。

ステップ 2 [接続（Connections）] タブを選択し、[LAN 設定（LAN Settings）] ボタンをクリックします。

ステップ 3 プロキシ サーバを使用するように LAN を設定し、プロキシ サーバの IP アドレスを入力します。

パブリック プロキシ接続の設定（macOS）

手順

ステップ 1 システム設定に移動し、接続している適切なインターフェイスを選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 新しいウィンドウで [プロキシ（Proxies）] タブを選択します。

ステップ 4 HTTPS プロキシを有効にします。

ステップ 5 右側のパネルの [セキュアプロキシサーバ（Secure Proxy Server）] フィールドに、プロキシ サーバのアドレスを入力します。

パブリック プロキシ接続の設定（Linux）

Linux でパブリック プロキシ接続を設定するには、環境変数を設定します。

プライベート プロキシ接続の設定

手順

ステップ 1 ASA グループ ポリシーにプライベート プロキシ情報を設定します。『Cisco ASA Series VPN Configuration Guide』の「Configuring a Browser Proxy for an Internal Group Policy」の項を参照してください。

（注） macOS 環境では、（VPN 接続時に）ASA からプッシュダウンされたプロキシ情報は、端末を開いて **scutil --proxy** を発行するまで、ブラウザに表示されません。

ステップ 2 （任意）ブラウザのプロキシ設定を無視するためのクライアントの設定。

ステップ 3 （任意）Internet Explorer の [接続（Connections ）] タブのロックダウン。

ブラウザのプロキシ設定を無視するためのクライアントの設定

AnyConnect プロファイルでは、ユーザの PC 上で Microsoft Internet Explorer または Safari のプロキシ設定が無視されるようにポリシーを指定できます。これにより、ユーザは社内ネットワークの外部からトンネルを確立できなくなり、AnyConnect は望ましくないまたは違法なプロキシ サーバ経由で接続できなくなります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [プロキシ設定（Proxy Settings）] ドロップダウン リストで、[プロキシを無視（Ignore Proxy）] を選択します。[プロキシを無視（Ignore Proxy）] を選択すると、クライアントはすべてのプロキシ設定を無視します。ASA からダウンロードされるプロキシに対してアクションが実行されません。

Internet Explorer の [接続（Connections ）] タブのロックダウン

ある条件下では、AnyConnect により、Internet Explorer の [ツール（Tools ）] > [インターネット オプション] > [接続（Connections ）] タブが非表示にされます。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックダウンは接続解除すると反転され、このタブに適用される管理者定義のポリシーの方が優先されます。このロックダウンは、次のいずれかの条件で行われます。

- ASA の設定で、[接続（Connections ）] タブのロックダウンが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。

- Windows のグループ ポリシーにより、以前に [接続（Connections ）] タブがロックダウンされている（ロックダウンしない ASA グループ ポリシー設定の上書き）。

グループ ポリシーで、プロキシのロックダウンを許可する、または許可しないように ASA を設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

手順

ステップ 1 ASDM で、**[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）]** > **[グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 ナビゲーション ペインで、**[詳細（Advanced）]** > **[ブラウザ プロキシ（Browser Proxy）]** に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4 **[プロキシ ロックダウン（Proxy Lockdown）]** をクリックして、その他のプロキシ設定を表示します。

ステップ 5 プロキシのロックダウンを有効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections ）] タブを非表示にするには、**[継承（Inherit）]** をオフにして **[はい（Yes）]** を選択します。または、プロキシのロックダウンを無効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections ）] タブを表示するには、**[いいえ（No）]** を選択します。

ステップ 6 **[OK]** をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7 **[適用（Apply）]** をクリックして、グループ ポリシーの変更を保存します。

プロキシ設定の確認

- Windows の場合：次の場所でレジストリのプロキシ設定を検索します。

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- macOS の場合：ターミナル ウィンドウを開き、次を入力します。

```
scutil --proxy
```

VPN トラフィックの選択および除外

VPN をバイパスするための IPv4 または IPv6 トラフィックの設定

ASA が IPv6 トラフィックのみを待機している場合は AnyConnect クライアントが IPv4 トラフィックをどのように管理するかを設定し、ASA がクライアント バイパス プロトコル設定を

使用して IPv4 トラフィックのみを待機している場合は AnyConnect クライアントが IPv6 トラフィックをどのように管理するかを設定できます。

AnyConnect クライアントで ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

クライアント バイパス プロトコルが IP プロトコルに対して有効であり、かつ、あるアドレス プールがそのプロトコルに対して設定されていない（つまり、そのプロトコルの IP アドレスが ASA によってクライアントに割り当てられていない）場合、そのプロトコルを使用する IP トラフィックはVPNトンネルを介して送信されません。これは、トンネル外で送信されます。

クライアント バイパス プロトコルが無効であり、かつ、あるアドレス プールがそのプロトコル用に設定されていない場合、VPN トンネルが確立された後、クライアントではその IP プロトコルのすべてのトラフィックをドロップします。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定します。エンドポイントが IPv6 アドレスへの到達を試みた場合、クライアント バイパス プロトコルが無効になっていると、IPv6 トラフィックはドロップされます。クライアント バイパス プロトコルが有効になっていると、IPv6 トラフィックはクライアントからクリア テキストで送信されます。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうかが ASA に通知されないため、ASA は常にクライアント バイパス プロトコル設定をプッシュダウンします。

クライアント バイパス プロトコルを ASA でグループ ポリシーに設定します。

手順

ステップ 1 ASDM で、**[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）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 **[詳細（Advanced）] > [AnyConnect]** を選択します。

ステップ 4 デフォルト グループ ポリシー以外のグループ ポリシーの場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] の隣にある [継承（Inherit）] チェックボックスをオフにします。

ステップ 5 次のオプションのいずれかを選択します。

- ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[無効（Disable）] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[有効（Enable）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定

『Cisco ASA Series Configuration Guide』の「Client Firewall with Local Printer and Tethered Device Support」の項を参照してください。

スプリット トンネリングの設定

スプリット トンネリングは、[ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定します。『Cisco ASA Series VPN Configuration Guide』の「Configure Split Tunneling for AnyConnect Traffic」の項を参照してください。

ASDM でグループ ポリシーに変更を加えたら、[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）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

ダイナミック スプリット トンネリングについて

ダイナミック スプリット トンネリングは、ASDM グループ ポリシー設定で [次のネットワークリストを除外（Exclude Network List Below）] または [次のネットワークリストをトンネリング（Tunnel Network List Below）] オプションを使用して設定される現在のスプリット トンネリング オプションを強化するために設計されました。スプリット トンネリングを定義するために通常使用される静的な包含または除外と違い、ダイナミック スプリット トンネリングでの包含または除外は、特定のサービスに関するトラフィックを VPN トンネリングから除外するまたは VPN トンネリングに包含する必要があるシナリオに対応しています。IP プロトコルごとに個別のスプリット トンネリング設定を構成できます。たとえば、IPv4 にダイナミック スプリット包含トンネリング（IPv4 スプリット包含ドメインやダイナミック スプリット包含ドメインなど）を有効にし、IPv6 にダイナミック スプリット除外トンネリング（IPv6 トンネルオール ドメインやダイナミック スプリット除外ドメインなど）を有効にできます。さらに、AnyConnect リリース 4.6 では、拡張ダイナミック スプリット トンネリングが追加されました。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方が拡張ドメイン名の一致に指定されています。

ダイナミック スプリット除外トンネリング：複数のクラウド ベースのサービスが同じ IP プールにホストされており、ユーザの場所またはクラウド上のコンピュータ資源の負荷に応じて異なる IP アドレスへと解決される場合があります。そのようなサービスのうち 1 つだけを VPN トンネルから除外したい場合、管理者が静的な除外を使用してそのためのポリシーを定義するのは、特に ISP NAT、6to4、4to6 などのネットワーク変換スキームも考慮される場合は困難です。ダイナミック スプリット除外トンネリングでは、トンネルの確立後に、ホストの DNS ド

メイン名に基づいて動的にスプリット除外トンネリングをプロビジョニングできます。たとえば、VPN管理者は、実行時にexample.comをVPNトンネルから除外するように設定できます。VPNトンネルがアップしているときにアプリケーションがmail.example.comに接続しようとすると、VPNクライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、トンネル外部への接続を許可します。

拡張ダイナミック スプリット除外トンネリング：ダイナミック スプリット除外トンネリングがダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方で設定されている場合、VPNトンネルから動的に除外されたトラフィックは少なくとも1つのダイナミック スプリット除外ドメインに一致する必要がありますが、ダイナミック スプリット包含ドメインに一致する必要はありません。たとえば、VPN管理者がダイナミック スプリット除外ドメインexample.comとダイナミック スプリット包含ドメインmail.example.comを設定した場合、mail.example.com以外のすべてのexample.comトラフィックはトンネリングから除外されます。

ダイナミックスプリット包含トンネリング：ダイナミックスプリット包含トンネリングでは、トンネルの確立後に、ホストのDNSドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。たとえば、VPN管理者は、実行時にdomain.comをVPNトンネルに含めるように設定できます。VPNトンネルがアップしているときにアプリケーションがwww.domain.comに接続しようとすると、VPNクライアントは、自動的にシステムルーティング テーブルとフィルタを変更し、VPNトンネル内部での接続を許可します。

拡張ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、VPNトンネルに動的に包含されたトラフィックは少なくとも1つのダイナミック スプリット包含ドメインに一致する必要がありますが、ダイナミック スプリット除外ドメインに一致する必要はありません。たとえば、VPN管理者がdomain.comをスプリット包含ドメインとして、www.domain.comをスプリット除外ドメインとして設定した場合、www.domain.com以外のすべてのdomain.comトラフィックがトンネリングされます。

（注） ダイナミック スプリット トンネリングは、Linuxではサポートされていません。

スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性

静的な除外と動的な除外は共存可能です。スタティック スプリット トンネリングはトンネルの確立時に適用され、ダイナミック スプリット トンネリングは、トンネルが接続済みとなっているときにドメインへのトラフィックが発生すると適用されます。

ダイナミック スプリット除外トンネリング

ダイナミック スプリット除外トンネリングは、「tunnel all」、「split include」、および「split exclude」トンネリングに適用されます。

- すべてのネットワークをトンネリングする：VPNトンネルからの除外は、すべて動的です。

- 特定のネットワークを除外する：事前設定された静的な除外に動的な除外が追加されます。
- 特定のネットワークを包含する：除外されるホスト名の IP アドレスのうち、スプリットを含むネットワークと重複する場合のみ、動的な除外が適用されます。それ以外の場合、トラフィックは VPN トンネルからすでに除外されているため、動的な除外は行われません。

拡張ダイナミック スプリット除外トンネリングは、「tunnel all」および「split exclude」トンネリングに適用されます。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方、およびスプリット包含トンネリングが設定されている場合、その結果の設定は拡張ダイナミック スプリット包含トンネリングになります。

ダイナミック スプリット包含トンネリング

ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

拡張ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

（注） Umbrella ローミング セキュリティによる保護は、スタティックまたはダイナミック スプリット トンネリングのいずれかが有効になっていると、アクティブになります。Umbrella クラウド リゾルバは、到達可能であり、かつ、VPN トンネルによるプローブが可能である場合を除き、VPN トンネルから静的に包含または除外することが必要となる場合があります。

スプリット トンネリング設定をともなう重複シナリオの結果

動的な包含または除外の対象は、まだ包含または除外されていない IP アドレスのみです。静的トンネリングおよび何らかの形式の動的トンネリングの両方が適用されており、新たな包含または除外を強制する必要がある場合、すでに適用された包含または除外との衝突が発生する可能性があります。動的な除外（除外されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、除外において考慮されるのは、まだ除外されていないアドレスのみです。同様に、動的な包含（包含されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、包含において考慮されるのは、まだ包含されていないアドレスのみです。

静的なパブリック ルート（セキュア ゲートウェイ ルートなどのスプリット除外ルートやクリティカル ルートなど）は、ダイナミック スプリット包含ルートよりも優先されます。そのため、動的な包含の少なくとも 1 つの IP アドレスが静的なパブリック ルートと一致する場合、動的な包含は強制されません。

同様に、静的スプリット包含ルートはダイナミック スプリット除外ルートよりも優先されます。そのため、動的な除外の少なくとも 1 つの IP アドレスが静的スプリット包含ルートと一致する場合、動的な除外は強制されません。

ダイナミック スプリット トンネリングの使用状況の通知

VPN トンネルの接続中は、ダイナミック スプリット トンネリングに何が設定されているかをいくつかの方法で確認できます。

- [統計（Statistics）] タブ：ASN グループ ポリシーで設定されている VPN トンネルから除外された、または VPN トンネルに包含されたドメイン名を含むダイナミック トンネル除外およびダイナミック トンネル包含が表示されます。
- [エクスポート統計（Export Stats）] : VPN トンネリングから除外された、または VPN トンネリングに包含されたドメイン名と、IPv4 と IPv6 の両方のトンネル モードを含むファイルが生成されます。ダイナミック ルートもエクスポートされた統計に含まれます。
- [ルートの詳細（Route Details）] タブ：除外または包含された各 IP アドレスに対応するホスト名を持つ IPv4 および IPv6 ダイナミック スプリット除外および包含ルートが表示されます。

（注） AnyConnect UI には、AnyConnect VPN が実現する保護されたルートまたは保護されていないルートが、IP プロトコルにつき最大 200 個表示されます。ルートの数が 200 を超えると、切り捨てが発生します。すべてのルートを表示するには、Windows では **route print** を実行し、Linux または macOS では **netstat -rn** を実行します。

- VPN の設定ログ メッセージ：VPN トンネルから除外された、または VPN トンネルに包含されたドメインの数が示されます。

スプリット DNS

スプリット DNS が [ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定されている場合、AnyConnect は、特定の DNS クエリーをプライベート DNS サーバ（同様にグループ ポリシーに設定）にトンネルします。他の DNS クエリーはすべて DNS 解決のためのクライアント オペレーティング システムの DNS リゾルバにクリア テキストで送信されます。スプリット DNS が設定されていない場合、AnyConnect はすべての DNS クエリーをトンネルします。

スプリット DNS の要件

スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

AnyConnect スプリット DNS は、Windows と macOS プラットフォームでサポートされています。

macOS の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

スプリット DNS の設定

グループ ポリシーにスプリット DNS を設定するには、次の手順を実行します。

手順

ステップ 1 少なくとも 1 つの DNS サーバを設定します。

『Cisco ASA Series VPN Configuration Guide』の「*Configure Server Attributes for an Internal Group Policy*」の項を参照してください。

指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバとオーバーラップしていないことを確認します。オーバーラップしていると、名前解決が正しく動作せず、クエリーがドロップされる可能性があります。

ステップ 2 Split-Include トンネリングを設定します。

[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）] > [グループ ポリシー（Group Policies）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] ペインで、[次のトンネル ネットワーク リスト（Tunnel Network List Below）] を選択し、[ネットワーク リスト（Network List）] にトンネルするアドレスを指定します。

スプリット DNS は、[次のネットワーク リストを除外（Exclude Network List Below）] スプリット トンネリング ポリシーをサポートしません。[次のトンネル ネットワーク リスト（Tunnel Network List Below）] スプリット トンネリング ポリシーを使用して、スプリット DNS を設定します。

ステップ 3 スプリット DNS を設定します。

[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）] > [グループ ポリシー（Group Policies）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] ペインで、[トンネルですべての DNS ルックアップを送信する（Send All DNS lookups through tunnel）] をオフにし、クエリーがトンネルされるドメインの名前を [DNS 名（DNS Names）] に指定します。

次のタスク

ASDM でグループ ポリシーに変更を加えたら、[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）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

AnyConnect ログを使用したスプリット DNS の確認

スプリット DNS が有効であることを確認するには、AnyConnect のログで、「Received VPN Session Configuration Settings」が含まれたエントリを検索します。このエントリは、スプリット DNS が有効であることを示します。IPv4 と IPv6 のスプリット DNS 用に別々のログ エントリがあります。

スプリット DNS を使用しているドメインの確認

ドメイン名解決には、オペレーティング システムの DNS リゾルバに依存するあらゆるツールまたはアプリケーションを使用できます。たとえば、ping または Web ブラウザを使用してスプリット DNS ソリューションをテストできます。nslookup または dig などのその他のツールは、OS DNS リゾルバを回避します。

クライアントを使用して、どのドメインがスプリット DNS に使用されているかを確認する手順は次のとおりです。

手順

ステップ 1 **ipconfig/all** を実行して、DNS サフィックス検索リストの横にリストされたドメインを記録します。

ステップ 2 VPN 接続を確立し、DNS サフィックス検索リストの横にリストされたドメインを再度確認します。

トンネルを確立した後に追加されたドメインは、スプリット DNS で使用されるドメインです。

（注） このプロセスは、ASA からプッシュされたドメインと、クライアント ホストで設定済みのドメインがオーバーラップしていないことを前提としています。

VPN 認証の管理

重要なセキュリティ上の考慮事項

- セキュア ゲートウェイ上での自己署名証明書の使用はお勧めしません。理由は、ユーザが誤って不正なサーバ上の証明書を信頼するようにブラウザを設定する可能性があるため、

また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

- 以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

  を設定するには、ローカル ポリシー パラメータと値（62 ページ）の「ローカル ポリシー パラメータと値」の項を参照してください。

サーバ証明書処理の設定

サーバ証明書の確認

- （Windows のみ）SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。プロファイルエディタで有効にすると、AnyConnect はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認します。認証局によって失効された証明書であることが判明すると、AnyConnect は接続しません。詳細は、ローカル ポリシー パラメータと値（62 ページ）を参照してください。

- サーバ証明書が設定された ASA にユーザが接続する場合、信頼チェーン（ルートや中間など）に問題があっても、その証明書を信頼し、インポートするためのチェックボックスは表示されます。証明書にそれ以外の問題がある場合、そのチェックボックスは表示されません。

- FQDN によって実行される SSL 接続では、FQDN を使用した初期検証に失敗した場合、名前検証のために FQDN が IP アドレスに解決されず、セカンダリ サーバの証明書検証が行われません。

- IPSec および SSL 接続では、サーバ証明書にキーの使用状況が含まれる場合、属性に DigitalSignature および（KeyAgreement または KeyEncipherment）が含まれている必要があります。サーバ証明書に EKU が含まれている場合は、属性に serverAuth（SSL および IPSec の場合）または ikeIntermediate（IPsec の場合のみ）が含まれている必要があります。サーバ証明書がなくても、KU または EKU を受け入れることができることに注意してください。

- IPsec および SSL 接続は、サーバ証明書で名前の検証を実行します。IPsec および SSL 名前検証のために次のルールが適用されます。

  - 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、あっても関連する属性が含まれていない場合、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。このルール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。

- OS X の場合、期限切れの証明書は、キーチェーン アクセスで [有効期限の切れた証明書を表示（Show Expired Certificates）] が設定されている場合にのみ表示されます。期限切れの証明書は、ユーザの混乱を招く可能性があるため、デフォルトでは表示されません。

無効なサーバ証明書の処理

非信頼ネットワーク上のモバイル ユーザを狙った攻撃の増加に対応して、シスコは重大なセキュリティ違反を防ぐため、クライアントのセキュリティ保護を強化しました。デフォルトのクライアントの動作は、中間者攻撃に対する追加の防御レイヤを提供するように変更されました。

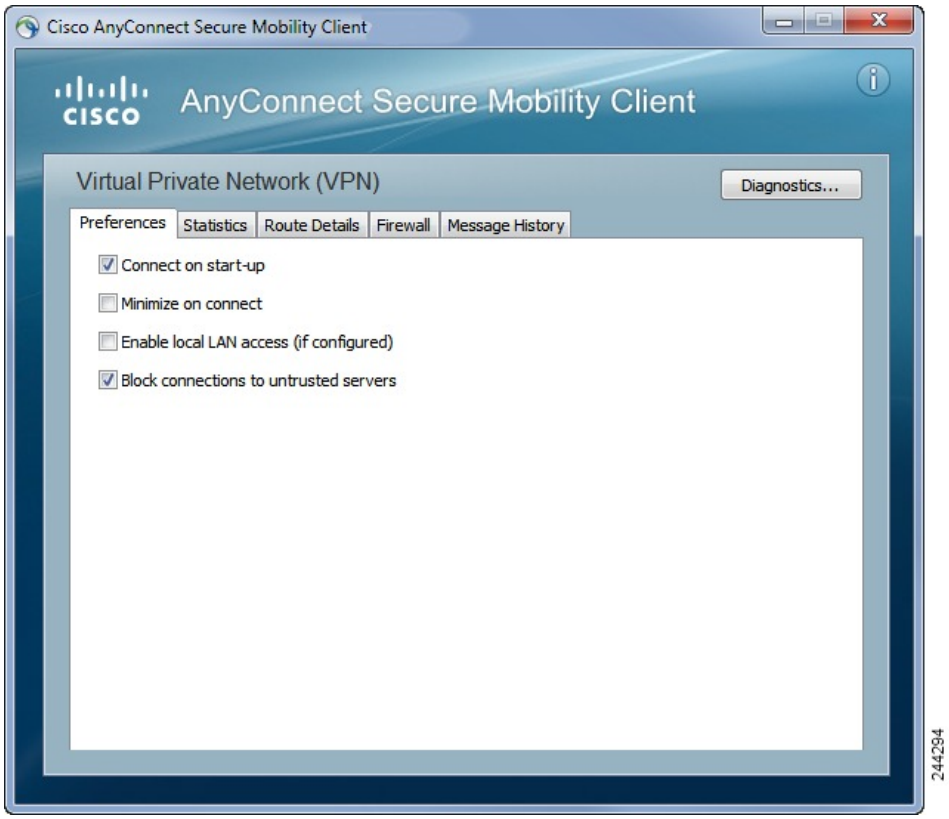
ユーザ対話

ユーザがセキュア ゲートウェイに接続しようとしたときに証明書エラーがある場合（期限切れ、無効な日付、キーの誤用、または CN の不一致による）、[設定の変更（Change Settings）] および [安全を確保（Keep Me Safe）] ボタンを含む赤色のダイアログがユーザに表示されます。

（注） Linux のダイアログは、このマニュアルに示すものと異なる場合があります。

- [安全を確保（Keep Me Safe）] をクリックすると、接続が解除されます。

- [設定の変更（Change Settings）] をクリックすると、AnyConnect の [詳細（Advanced）] > [VPN] > [プリファレンス（Preferences）] ダイアログが開きます。ここで、ユーザは非信頼サーバへの接続を有効にできます。現在の接続の試行がキャンセルされます。



ユーザが、[信頼されていないサーバへの接続をブロック（Block connections to untrusted servers）] をオフにして、証明書に関する問題が CA が信頼できないことのみである場合、次回ユーザがこのセキュア ゲートウェイに接続しようとするときは、ユーザに証明書ブロック エラーのダイアログは表示されず、次のダイアログのみが表示されます。

ユーザが [常にこの VPN サーバを信頼し、証明書をインポートする（Always trust this VPN server and import the certificate）] をオンにしている場合、このセキュア ゲートウェイへの今後の接続時に、ユーザの続行を確認するプロンプトは表示されません。

（注） ユーザが、AnyConnect の [詳細（Advanced）] > [VPN] > [設定（Preferences）] で [信頼されていないサーバへの接続をブロック（Block connections to untrusted servers）] をオンにしている場合、または、ユーザの設定が注意事項と制約事項の項で説明されているモードのリストのいずれかの条件と一致する場合、AnyConnect は無効なサーバ証明書を拒否します。

改善されたセキュリティ動作

クライアントが無効なサーバ証明書を受け入れると、その証明書はクライアントの証明書ストアに保存されます。以前は、証明書のサムプリントだけが保存されました。ユーザが無効なサーバ証明書を常に信頼してインポートすることを選択した場合のみ、無効な証明書が保存されることに注意してください。

エンドユーザの安全性が自動的に損なわれる管理上の優先操作はありません。先行するセキュリティ上の判断をエンド ユーザから完全に排除するには、ユーザのローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] を有効にします。[厳格な証明書トラスト（Strict Certificate Trust）] が有効である場合、ユーザにはエラー メッセージが表示され、接続が失敗します。ユーザ プロンプトは表示されません。

ローカル ポリシー ファイルでの厳格な証明書トラストの有効化については、ローカルポリシーパラメータと値 （62 ページ）の「AnyConnect ローカル ポリシー パラメータと値」の項を参照してください。

注意事項と制約事項

無効なサーバ証明書は、次の場合に拒否されます。

- AnyConnect VPN クライアント プロファイルで [常時接続（Always On）] が有効になっており、適用されたグループ ポリシーまたは DAP によりオフにされていない。
- クライアントに、厳格な証明書トラストが有効なローカル ポリシーがある。
- AnyConnect でログイン前の起動が設定されている。
- マシン証明書ストアからのクライアント証明書が認証に使用されている。

Certificate-Only 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。

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロ

セスによる証明書が ASA に提供されたときに、このグループにユーザを配置するようにできます。

（注） 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。

手順

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）] 領域で、[証明書（Certificate）] 方式を有効にします。

ステップ 3 [OK] をクリックし、変更を適用します。

証明書登録の設定

Cisco AnyConnect Secure Mobility Clientは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一部として証明書をプロビジョニングおよび更新します。SCEP を使用した証明書の登録は、ASA への AnyConnect IPsec および SSL VPN 接続で次のようにサポートされます。

- SCEP プロキシ：ASA はクライアントと認証局（CA）間の SCEP 要求と応答のプロキシとして機能します。
  - クライアントが CA に直接アクセスしないため、CA は、AnyConnect クライアントではなく ASA にアクセスできる必要があります。
  - 登録は、クライアントにより常に自動的に開始されます。ユーザの介入は必要ありません。

関連トピック

AnyConnect プロファイル エディタの証明書の登録 （48 ページ）

SCEP プロキシの登録と動作

次の手順では、AnyConnect および ASA が SCEP プロキシ用に設定されている場合に、証明書が取得され、証明書ベースの接続が確立された方法について説明します。

1. ユーザは、証明書と AAA 認証の両方用に設定された接続プロファイルを使用して、ASA ヘッドエンドに接続します。ASA は、クライアントからの認証用に証明書と AAA クレデンシャルを要求します。
2. ユーザが AAA クレデンシャルを入力しますが、有効な証明書は使用可能ではありません。この状況は、入力された AAA クレデンシャルを使用してトンネルが確立された後で、クライアントが自動 SCEP 登録要求を送信するトリガーになります。
3. ASA が CA に対して登録要求を転送し、CA の応答をクライアントに返します。
4. SCEP 登録が成功すると、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは、証明書認証を使用して、ASA トンネル グループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは自分の管理者に連絡する必要があります。

他の SCEP プロキシの動作上の考慮事項：

- そうするように設定されている場合、ユーザが介入することなく、期限切れになる前に証明書がクライアントにより自動的に更新されます。
- SCEP プロキシ登録は、SSL と IPSec トンネルの両方の証明書認証に SSL を使用します。

認証局の要件

- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- 一部の CA について、セキュリティを強化するために、電子メールで登録パスワードをユーザに送信するように設定できます。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。このパスワードはその後、AnyConnect クライアントプロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

証明書登録のガイドライン

- ASA へのクライアントレス（ブラウザベース）VPN アクセスは、SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）がサポートされます。
- ASA ロード バランシングは、SCEP 登録でサポートされます。
- ASA は、クライアントから受信した要求を記録しますが、登録が失敗した理由は表示しません。接続の問題は、CA またはクライアントでデバッグされる必要があります。
- 証明書のみの認証および ASA での証明書マッピング：

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が ASA に提供されたときに、このトンネル グループにユーザを配置するようにできます。

- ポリシーを適用するための登録接続の特定：

  ASA で、登録接続を捕捉し、選択された DAP レコードの適切なポリシーを適用するために、aaa.cisco.sceprequired 属性が使用されます。

- Windows 証明書の警告：

  Windows クライアントが最初に認証局から証明書を取得しようとした際に、警告される可能性があります。プロンプトが表示されたら、[はい（Yes）] をクリックしてください。これにより、ルート証明書をインポートできます。クライアント証明書との接続に影響しません。

SCEP プロキシ証明書登録の設定

SCEP プロキシ登録用 VPN クライアント プロファイルの設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの証明書の登録」を参照してください。

（注）
- %machineid% を使用した場合は、デスクトップ クライアントに Hostscan/Posture がロードされます。
- モバイル クライアントの場合、証明書フィールドのうち少なくとも 1 つを指定する必要があります。

SCEP プロキシ登録をサポートするための ASA の設定

SCEP プロキシのため、1 つの ASA 接続プロファイルは、証明書登録および認証された VPN 接続をサポートします。

手順

ステップ 1 グループ ポリシー（例：cert_group）を作成します。次のフィールドを設定します。

- [一般（General）] で、[SCEP フォワーディング URL（SCEP Forwarding URL）] に CA への URL を入力します。
- [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアント プロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、SCEP プロキシ用に設定されたクライアント プロファイルを指定します。たとえば、ac_vpn_scep_proxy クライアント プロファイルを指定します。

ステップ 2 証明書の登録および接続を認証した証明書（例：cert_tunnel）用の接続プロファイルを作成します。

- [認証（Authentication）]：Both（AAA および Certificate）。
- デフォルトのグループ ポリシー：cert_group。
- [詳細（Advanced）] > [一般（General）] で、[この接続プロファイルへの SCEP 登録を有効にする（Enable SCEP Enrollment for this Connction Profile）] をオンにします。
- [詳細（Advanced）] > [グループエイリアス/グループ URL（GroupAlias/Group URL）] で、この接続プロファイルのグループ（cert_group）が含まれるグループ URL を作成します。

SCEP 用の Windows 2008 Server の認証局の設定

認証局ソフトウェアが Windows 2008 サーバで実行されている場合、AnyConnect で SCEP がサポートされるように次のいずれかの設定変更を行う必要があります。

認証局での SCEP パスワードの無効化

次の手順は、クライアントが SCEP 登録の前にアウトオブバンドパスワードを提供せずに済むように、SCEP チャレンジ パスワードを無効にする方法について説明します。

手順

ステップ 1 認証局サーバで、レジストリ エディタを起動します。これを行うには、**[スタート（Start）]** > **[ファイル名を指定して実行（Run）]** を選択し、**regedit** と入力して [OK] をクリックします。

ステップ 2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword に移動します。

EnforcePassword キーが存在しない場合は、新しいキーとして作成します。

ステップ 3 EnforcePassword を編集し、「0」に設定します。存在しない場合は、REG-DWORD として作成します。

ステップ 4 regedit を終了し、認証局サーバをリブートします。

認証局での SCEP テンプレートの設定

以下の手順では、証明書のテンプレートを作成する方法、およびこれをデフォルト SCEP テンプレートとして割り当てる方法について説明します。

手順

ステップ 1 サーバ マネージャを起動します。これは、[スタート（Start）] > [管理ツール（Admin Tools）] > [サーバ マネージャー（Server Manager）] を選択することで実行できます。

ステップ 2 [役割（Expand Roles）] > [証明書サービス（Certificate Services）]（または [Active Directory 証明書サービス（AD Certificate Services）]）を展開します。

ステップ 3 CA の名前 > [証明書テンプレート（Certificate Templates）] に移動します。

ステップ 4 [証明書テンプレート（Certificate Templates）] > [管理（Manage）] を右クリックします。

ステップ 5 [証明書テンプレート コンソール（Cert Templates Console）] から、ユーザ テンプレートを右クリックして [複製（Duplicate）] を選択します。

ステップ 6 新しいテンプレートの [Windows Server 2008] バージョンを選択して、[OK] をクリックします。

ステップ 7 テンプレートの表示名を、NDES IPsec SSL など、具体的な説明に変更します。

ステップ 8 サイトの有効期間を調整します。ほとんどのサイトでは、証明書の期限切れを避けるために 3 年以上を選択します。

ステップ 9 [暗号化（Cryptography）] タブで、展開の最小キー サイズを設定します。

ステップ 10 [サブジェクト名（Subject Name）] タブで、[要求に含まれる（Supply in Request）] を選択します。

ステップ 11 [拡張機能（Extensions）] タブで、[アプリケーションのポリシー（Application Policies ）] に少なくとも次が含まれるように設定します。

- クライアント認証
- IP セキュリティ末端システム
- IP セキュリティ IKE 中間
- IP セキュリティ トンネル終端
- IP セキュリティ ユーザ

これらの値は、SSL または IPSec に有効です。

ステップ 12 [適用（Apply）] をクリックして、次に [OK] をクリックして新しいテンプレートを保存します。

ステップ 13 サーバ マネージャから [証明書サービス（Certificate Services）] に移動して CA の名前を選択し、[証明書テンプレート（Certificate Templates）] を右クリックします。[新規（New ）] > [発

行する証明書テンプレート（Certificate Template to Issue）] を選択し、作成した新しいテンプレートを選択します（この例では NDES-IPSec-SSL）。次に、[OK] をクリックします。

ステップ 14 レジストリを編集します。これは、[スタート（Start）]>[ファイル名を指定して実行（Run）] で regedit と入力し、[OK] をクリックすることで実行できます。

ステップ 15 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP に移動します。

ステップ 16 次の 3 つのキーの値を、NDES-IPSec-SSL に設定します。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

ステップ 17 [保存（Save）] をクリックして、認証局サーバをリブートします。

証明書失効通知の設定

認証証明書が間もなく期限切れになることをユーザに警告するよう AnyConnect を設定します。[証明書失効しきい値（Certificate Expiration Threshold）] の設定では、AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを指定します。AnyConnect は、証明書が実際に期限切れか、新しい証明書が取得されるまで、ユーザが接続するたびに警告します。

（注） RADIUS 登録では、[証明書失効しきい値（Certificate Expiration Threshold）] 機能は使用できません。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 [証明書失効しきい値（Certificate Expiration Threshold）] を指定します。

AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを示す数字です。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 4 [OK] をクリックします。

証明書選択の設定

次の手順では、クライアントシステムで証明書を検索する方法および証明書を選択する方法を設定する、AnyConnect プロファイル内のすべての場所を示します。いずれの手順も必須ではなく、条件を指定しなかった場合、AnyConnect はデフォルトのキー照合を使用します。

Windows では、AnyConnect はブラウザの証明書ストアを読み取ります。Linux の場合、プライバシー強化メール（PEM）形式のファイルストアを作成する必要があります。macOS の場合、プライバシー強化メール（PEM）形式のファイルストアまたはキーチェーンを使用できます。

手順

ステップ 1 Windows および macOS の場合：使用する証明書ストアの設定 （125 ページ）

VPN クライアント プロファイルに AnyConnect で使用される証明書ストアを指定します。

ステップ 2 Windows のみ：Windows ユーザに認証証明書の選択を求めるプロンプトの表示 （128 ページ）

ユーザに有効な証明書のリストを示すように AnyConnect を設定し、ユーザがセッションの認証にその証明書を選択できるようにします。

ステップ 3 macOS および Linux 環境の場合：macOS および Linux での PEM 証明書ストアの作成 （129 ページ）

ステップ 4 macOS および Linux 環境の場合：VPN ローカル ポリシー プロファイルで除外する証明書ストアを選択します。

ステップ 5 証明書照合の設定 （130 ページ）

ストアの証明書を検索する場合に、AnyConnect が照合を試みるキーを設定します。キー（拡張キー）を指定し、カスタム拡張キーを追加できます。また、AnyConnect が照合する識別名に演算子の値のパターンを指定できます。

使用する証明書ストアの設定

Windows および macOS では、AnyConnect が VPN クライアント プロファイルで使用するための別の証明書ストアが提供されます。1 つまたは複数の証明書認証の組み合わせが可能で、複数の証明書認証の選択肢のうち特定の VPN 接続において許容されるものをクライアントに指定するようにセキュア ゲートウェイを設定できます。たとえば、ローカル ポリシー ファイルで ExcludeMacNativeCertStore を true に設定（AnyConnect がユーザ ファイル証明書ストアやシステム ファイル証明書ストアなどのファイル証明書ストアのみを使用するよう強制）し、プロファイル ベースの証明書ストアを [ログイン（Login）] に設定（AnyConnect が、ユーザ ファイル ストアに加え、ログイン キーチェーンおよびダイナミック スマートカード キーチェーンなどの証明書ストアのみを使用するよう強制）すると、その組み合わせによるフィルタリングにより、AnyConnect は、厳格にユーザ ファイル証明書ストアを使用するようになります。

コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。通常、Windows

ユーザには管理者権限がありません。[証明書ストアの上書き（Certificate Store Override）] を選択すると、ユーザに管理者権限がない場合でも、AnyConnect はマシン ストアにアクセスできます。

（注） マシン ストアのアクセス制御は、Windows のバージョンとセキュリティ設定によって異なる場合があります。このため、ユーザは管理者権限を持つ場合にも、マシン ストアの証明書を使用できない可能性があります。この場合、[証明書ストアの上書き（Certificate Store Override）] を選択してマシン ストアへのアクセスを許可します。

次の表に、検索対象の [証明書ストア（Certificate Store）] および [証明書ストアの上書き（Certificate Store Override）] のオン/オフに基づいて AnyConnect がクライアントで証明書を検索する方法について説明します。

[証明書ストア（Certificate Store）] の設定	**[証明書ストアの上書き（Certificate Store Override）] の設定**	**AnyConnect の検索方法**
[すべて（All）]（Windows 用）	オフ	AnyConnect は、すべての証明書ストアを検索します。ユーザに管理者権限がない場合、AnyConnect は、マシン ストアにアクセスできません。 この設定は、デフォルトです。この設定は、ほとんどの状況に適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
[すべて（All）]（Windows 用）	オン	AnyConnect は、すべての証明書ストアを検索します。ユーザに管理者権限がない場合、AnyConnect は、マシン ストアにアクセスできます。
[すべて（All）]（macOS 用）	オン	AnyConnect は、利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。

[証明書ストア（Certificate Store）] の設定	[証明書ストアの上書き（Certificate Store Override）] の設定	AnyConnect の検索方法
[ユーザ（User）]（Windows 用）	適用せず	AnyConnect は、ユーザ証明書ストア内のみ検索します。管理者権限のないユーザがこの証明書ストアにアクセスできるため、証明書ストアの上書きは適用されません。
[システム（System）]（macOS 用）	オン	AnyConnect は macOS システム キーチェーンとシステム ファイル/PEM ストアからの証明書のみを使用します。macOS システム キーチェーンとシステム ファイル/PEM ストアからの証明書のみを使用します。
[ログイン（Log in）]（macOS 用）	オン	AnyConnect は、ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

複数証明書認証の使用

始める前に

- デスクトップ プラットフォーム（Windows、OS X、Linux）でのみサポートされます。
- VPN プロファイルで AutomaticCertSelection を有効にしている必要があります。
- VPNプロファイルで設定した証明書照合設定によって、複数証明書認証で使用できる証明書が制限されます。

（注） SCEP はサポートされていません。

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- 1 マシンおよび 1 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] に設定し、ステップ 2 の説明に従って CertficateStoreOverride を有効にします。
- 2 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] または [ユーザ（User）] に設定しますが、ステップ 2 の説明に従って CertificateStoreOverrideはそのままにします。

ステップ 2 ユーザに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、を選択します。

基本的な証明書認証の使用

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- [すべて（All）] :（デフォルト）すべての証明書ストアを使用して証明書を検索するよう AnyConnect クライアントに指示します。
- [マシン（Machine）] : 証明書ルックアップを Windows ローカル マシン証明書ストアに制限するように AnyConnect クライアントに指示します。
- [ユーザ（User）] : 証明書ルックアップをローカル ユーザ証明書ストアに制限するように AnyConnect クライアントに指示します。

ステップ 2 ユーザに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、を選択します。

Windows ユーザに認証証明書の選択を求めるプロンプトの表示

ユーザに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザが選択できるように AnyConnect を設定できます。期限切れの証明書は必ずしも無効として見なされるわけではありません。たとえばSCEP を使用している場合、サーバが新しい証明書をクライアントに発行することがあります。期限切れの証明書を削除すると、クライアントがまったく接続できなくなることがあります。この場合、手動による介入とアウトオブバンド証明書配布が必要になります。AnyConnect では、設定されている証明書一致ルールに基づき、セキュリティ関連プロパティ（キーの使用状況、キーのタイプと強度など）に基づいて、クライアント証明書が制限されるだけです。この設定は Windows でのみ使用できます。デフォルトでは、ユーザによる証明書の選択は無効です。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 証明書の選択を有効にするには、[証明書選択を無効にする（Disable Certificate Selection）] チェックボックスをオフにします。

ステップ 3 **[詳細（Advanced）] > [VPN] > [プリファレンス（Preferences）]** ペインでユーザが自動証明書の選択のオン/オフを切り替えられるようにする場合を除き、[ユーザ制御可（User Controllable）] チェックボックスをオフにします。

macOS および Linux での PEM 証明書ストアの作成

AnyConnect では、プライバシー強化メール（PEM）形式のファイル ストアからの証明書取得がサポートされています。AnyConnect はリモート コンピュータのファイル システムから PEM 形式の証明書ファイルを読み取り、確認と署名を行います。

始める前に

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子 .pem で終わっていること。
- すべての秘密キー ファイルは、拡張子 .key で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること（client.pem と client.key など）。

ヒント　PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

PEM ファイル証明書ストアを作成する場合は、次に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca （注）　.cisco/ はホーム ディレクトリにあります。	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

マシン証明書は、ルート ディレクトリ以外は PEM ファイル証明書と同じです。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外は、パス、フォルダ、および証明書のタイプが適用されます。

証明書照合の設定

AnyConnect では、特定のキーのセットに一致するこれらの証明書に証明書の検索を限定できます。証明書照合は、[証明書照合（Certificate Matching）] ペインの AnyConnect VPN クライアント プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- [キーの使用状況（Key Usage）]
- [拡張キーの使用状況（Extended Key Usage）]
- [識別名（Distinguished Name）]

関連トピック

AnyConnect プロファイル エディタの証明書照合 （45 ページ）

キーの使用状況の設定

[キーの使用状況（Key Usage）] キーを選択すると、AnyConnect で使用できる証明書が、選択したキーの少なくとも 1 つを持つ証明書に制限されます。サポート対象のセットは、VPN クライアント プロファイルの [キーの使用状況（Key Usage）] リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

拡張キーの使用状況の設定

[拡張キーの使用状況（Extended Key Usage）] キーを選択すると、AnyConnect で使用できる証明書がこれらのキーを持つ証明書に限定されます。次の表は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

制約	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キーの設定

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。

証明書識別名の設定

[識別名（Distinguished Name）] の表には、クライアントが使用できる証明書を指定の条件に一致する証明書に限定する証明書 ID、および一致条件が含まれています。条件をリストに追加したり、追加した条件の内容と照合するための値またはワイルドカードを設定したりするには、[追加（Add）] ボタンをクリックします。

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry

ID	説明
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

[識別名（Distinguished Name）] には、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。[識別名（Distinguished Name）] の一致では、証明書に指定の文字列が含まれている必要があるかどうか、および文字列にワイルドカードを許可するかどうかを指定します。

SAML を使用した VPN 認証

最初のセッション認証にASAリリース9.7.1と統合されたSAML 2.0を使用できます。AnyConnect 4.6 では、組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わります。SAML 認証用に設定されたトンネル グループに接続するときに、AnyConnect は組み込みブラウザ ウィンドウを開いて認証プロセスを完了します。SAML 試行のたびに新しいブラウザ セッションが使用され、ブラウザ セッションは AnyConnect に固有のものとなります（セッション状態は、他のどのブラウザとも共有されません）。各 SAML 認証試行はセッション状態なしで始まりますが、試行間で永続クッキーが保持されます。

プラットフォーム固有の要件

組み込みブラウザでSAMLを使用するためには、次のシステム要件を満たす必要があります。

- Windows：Windows 7（またはそれ以降）、Internet Explorer 11（またはそれ以降）
- macOS：macOS 10.10（またはそれ以降）（AnyConnect は、macOS 10.11 以降を公式にサポートしています）
- Linux：WebKitGTK+ 2.1x（それ以降）、Red Hat 7.4（それ以降）および Ubuntu 16.04（それ以降）の公式パッケージ

アップグレード プロセス

ネイティブ（外部）ブラウザ搭載の SAML 2.0 は、AnyConnect 4.4 と AnyConnect 4.5、および ASA リリース 9.7.x、9.8.x、および 9.9.1 で使用できます。組み込みブラウザを搭載した新しい拡張バージョンを使用するには、AnyConnect 4.6 および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

組み込みブラウザ SAML 統合を備えたヘッドエンドまたはクライアント デバイスをアップグレードまたは展開するときには、次のシナリオに注意してください。

- AnyConnect 4.6 を最初に展開した場合は、他に何も操作しなくても、ネイティブ（外部）ブラウザと組み込みブラウザの両方の SAML 統合が想定どおりに機能します。AnyConnect を最初に展開するときでも、AnyConnect 4.6 は既存の ASA バージョンも更新された ASA バージョンもサポートします。
- 更新された ASA バージョン（組み込みブラウザ SAML 統合を搭載）を最初に展開する場合は、続いて AnyConnect をアップグレードする必要があります。デフォルトでは、更新された ASA リリースは、AnyConnect 4.6 よりも前のリリースのネイティブ（外部）ブラウザ SAML 統合と後方互換性がないためです。認証後に既存の AnyConnect 4.4 または 4.5 クライアントのアップグレードが発生し、このアップグレードを行うためには、トンネル グループ設定で **saml external-browser** コマンドを有効にする必要があります。

SAML を使用する場合は、次の注意事項に従ってください。

- フェールオーバーモードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- 信頼できないサーバ証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、AnyConnect プロファイル エディタ、プリファレンス（Part 1）（33 ページ）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の AnyConnect は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッション クッキーを使用してログオン状態を追跡している場合には、毎回ユーザの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] > [シングルサインオンサーバ（Single Sign On Servers）] >** の [強制再認証（Force Re-Authentication）] は、AnyConnect が開始した SAML 認証には影響しません。

設定の詳細については、適切なリリース（9.7 以降）の『Cisco ASA Series VPN Configuration Guide』の「SSO Using SAML 2.0」の項を参照してください。

SDI トークン（SoftID）統合を使用した VPN 認証

AnyConnect は、Windows 7 x86（32 ビット）および x64（64 ビット）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。

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。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。

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 PIN（個人識別番号）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。

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、セキュア 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。一方で、デフォルト トンネル グループが NTLM 認証を使用する場合、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、「ユーザ名およびパスコードまたはソフトウェア トークンPINを入力してください（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、フィール

ド ラベルが [PIN] になります。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 [Passcode] のフィールドが表示されます。

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。

- Automatic：クライアントはまず 1 つの方式を試行し、それが失敗したら別の方式を試行します。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、成功した方式が新しい 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方式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、デフォルトの方式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:] 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 [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。

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
- 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。

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 0 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。

新規 PIN の作成

現行の PIN がない場合、システム設定に応じて、次の条件のいずれかを満たすことが、SDI サーバによって要求されます。

- 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）。
- ユーザは新規 PIN を作成する必要がある。
- 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。

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。

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。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。

ユーザが新しく PIN を作成するように選択した場合、AnyConnect にこの PIN を入力するためのダイアログボックスが表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。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。

「next passcode」チャレンジと「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。

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。

リモート ユーザからは、ネイティブ SDI と RADIUS SDI は同一です。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が、認証中に必要な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 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、クライアントからの必要な情報と要求される情報の順序は同じです。

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が、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 ASA の設定

SDI 固有の RADIUS 応答メッセージを解釈し、適切なアクションを AnyConnect ユーザに求めるように ASA を設定するには、SDI サーバとの直接通信をシミュレートする方法で RADIUS 応答メッセージを転送するように接続プロファイル（トンネル グループ）を設定する必要があります。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。

手順

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 [AnyConnect 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）] をオンにします。

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。

次の表に、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ます。

（注） ASA 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。Cisco 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。

セキュリティ アプライアンスは、テーブル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であるとします。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照合します。

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。

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
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。

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

証明書のピン留めについて

AnyConnect の証明書のピン留めは、サーバ証明書チェーンが実際に接続しているサーバから来たものであるか検出するのに役立ちます。この機能は VPN プロファイル設定に基づくもので、AnyConnect サーバ証明書検証ポリシーへの追加機能です。AnyConnect のローカル ポリシー ファイルでの厳格な証明書トラストの設定は、証明書のピン留めチェックに影響しません。ピンは、VPN プロファイルで、グローバルにまたはホストごとに設定できます。プライマリ ホストについて設定されたピンは、サーバ リスト内のバックアップ ホストに対しても有効です。証明書のピン留めチェックを実行するプリファレンスをユーザが制御することはできません。ピン検証が失敗すると、VPN 接続が終了します。

（注） AnyConnect は、プリファレンスが有効になっており、接続サーバの VPN プロファイルにピンがあるときのみ、ピン検証を実行します。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定は、VPN プロファイル エディタ（AnyConnect プロファイル エディタの証明書ピン （50 ページ））で行うことができます。

証明書のピン留めを設定および維持するにあたっては、注意が必要です。プリファレンスを設定するときは、次の推奨事項を考慮してください。

- ルート証明書および/または中間証明書をピン留めする。理由は、これらはオペレーティング システムにおいて CA ベンダーによって十分に管理されているためです。

- CA が侵害された場合のバックアップとなるよう、別の CA からの複数のルート証明書および/または中間証明書をピン留めする。
- CA の移行が容易になるよう、複数のルート証明書および/または中間証明書をピン留めする。
- リーフ証明書がピン留めされている場合は、証明書の更新時に公開キーを保持するため、同一の証明書署名要求を使用する。
- サーバ リスト内のすべての接続ホストをピン留めする。

グローバル ピンとホストごとのピン

証明書ピンは、グローバルまたはホストごとに設定できます。大部分の接続ホストに対して有効なピンは、グローバル ピンとして設定されます。ルート証明書、中間証明機関の証明書、およびワイルドカード リーフ証明書は、VPN プロファイルのグローバル ピンの下に設定することを推奨します。1 つの接続ホストに対してのみ有効なピンは、ホストごとのピンと見なされます。リーフ証明書、自己署名の証明書は、VPNプロファイルのホストごとのピンの下に設定することを推奨します。

（注） AnyConnect は、ピン検証において、対応する接続サーバのグローバル ピンおよびホストごとのピンをチェックします。

（注） 複数の VPN プロファイルにまたがるグローバル ピンは、マージされません。ピンは、VPN 接続のためのファイル接続サーバから厳格に考慮されます。

（注） ホストごとの証明書のピン留めができるのは、[グローバル ピン（Global Pins）] セクションで証明書ピン留めのプリファレンスが有効になっている場合のみです。