Cisco Secure Firewall Management Center を使用した Threat Defense での Secure Client モジュールの設定

初版：2023 年 7 月 31 日

最終更新：2023 年 8 月 1 日

Cisco Secure Firewall Management Center を使用した Threat Defense での Secure Client モジュールの設定

はじめに

Cisco Secure Client は、さまざまな Cisco エンドポイント セキュリティ ソリューションと統合することが可能で、複数の Secure Client モジュールを使ってセキュリティを強化できます。

管理対象ヘッドエンド Threat Defense を使用して、エンドポイントに Secure Client モジュールを配布して管理できます。ユーザーが Threat Defense に接続すると、Secure Client と必要なモジュールがエンドポイントにダウンロードされ、インストールされます。

メリット

Threat Defense を使用して Secure Client モジュールをエンドポイントに配布し管理すると、組織のネットワークを管理するための次の手動アクションが不要になるという大きな利点があります。

- 各エンドポイントでの Secure Client のダウンロードまたはアップグレード。
- 各エンドポイントでの Secure Client モジュールとプロファイルの配布および管理。

対象読者

この使用例は、Management Center を使用して、リモートアクセス VPN で組織のネットワークに接続するリモートワーカー向けに Secure Client モジュールを設定する、ネットワーク管理者を対象としています。

システム要件

次の表に、この機能でサポートされるプラットフォームを示します。

製品	バージョン	このドキュメントで使用されるバージョン
Cisco Secure Firewall Threat Defense（旧称 Firepower Threat Defense/FTD）	6.3 以降	7.3
Cisco Secure Firewall Management Center（旧称 Firepower Management Center/FMC）	6.7 以降	7.3
Cisco Secure Client（旧称 AnyConnect）	4.0 以降	5.0

（注） FMC バージョン 6.4 ～ 6.6 では、FlexConfig を使用して FTD でこれらのモジュールとプロファイルを有効にできます。詳細については、「Configure AnyConnect Modules and Profiles Using FlexConfig」を参照してください。

管理対象 Threat Defense を使用して Secure Client モジュールをインストールする方法

1. 管理者は、必要な Secure Client モジュールのプロファイルを作成します。
2. 管理者は Management Center を使用して次の操作を実行します。
   1. モジュールを設定し、RA VPN グループポリシーにプロファイルを追加します。
   2. 設定を Threat Defense に展開します。
3. ユーザーは、Secure Client を使用して Threat Defense への VPN 接続を開始します。
4. Threat Defense がユーザーを認証します。
5. Secure Client が更新をチェックします。
6. Threat Defense がエンドポイントで Secure Client モジュールとプロファイルを配布します。

さまざまな Secure Client モジュールの相違点

モジュール	説明
AMP イネーブラ	Cisco Secure Endpoint（旧 AMP for Endpoints）をエンドポイントに展開します。 ネットワーク内の潜在的なマルウェア脅威を検出し、検出した脅威を削除して企業を保護します。
ISE ポスチャ	Cisco Identity Services Engine（ISE）を使用してポスチャチェックを実行し、エンドポイントのコンプライアンスを評価します。
ネットワークの可視性	エンドポイントアプリケーションの使用状況をモニターします。 使用状況データは、NetFlow 分析ツールと共有できます。
Umbrella ローミングセキュリティ	Cisco Umbrella ローミング セキュリティ サービスを使用して DNS レイヤセキュリティを提供します。
Network Access Manager	セキュアなレイヤ2ネットワークを提供し、有線およびワイヤレスネットワークにアクセスするためのデバイス認証を実行します。
Start Before Login（SBL）	ユーザーが Windows へのログイン前に企業インフラへの VPN 接続を確立することを可能にします。
Web セキュリティ	HTTP トラフィックを Cisco クラウド Web セキュリティ スキャニング プロキシにルーティングします。
Diagnostic and Reporting Tool（DART）	システムログと他の診断情報を照合して、Secure Client のインストールと接続の問題をトラブルシュートします。
Feedback	使用および有効化する機能とモジュールについての情報を提供します。 この情報により、シスコは Cisco Secure Client の品質、信頼性、パフォーマンス、およびユーザー体験を向上させることができます。

該当するモジュールの詳細については、『Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5』[英語] を参照してください。

前提条件

- 使用するモジュールに応じて、関連する製品を設定します。
- Cisco Software Download Center [英語] からローカルホストに、次の Secure Client 関連パッケージをダウンロードします。
  - 必要なプラットフォーム用の Cisco Secure Client ヘッドエンド展開パッケージ。

    このパッケージはヘッドエンド用で、すべての Secure Client モジュールが含まれています。Windows の場合、ファイル名は cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg です。
  - Profile Editor：プロファイルを必要とするモジュールのプロファイルを作成します。

    Secure Client には、一部のモジュール用の Secure Client プロファイルが必要です。プロファイルには、モジュールを有効にし、対応するセキュリティサービスに接続するための設定が含まれています。Profile Editor は Windows のみをサポートします。

    次の表に、クライアントプロファイルを必要とするモジュールを示します。

Secure Client モジュール	クライアントプロファイルが必要
AMP イネーブラ	対応
ISE ポスチャ	対応
Network Access Manager	対応
ネットワーク可視性モジュール	対応
Umbrella ローミング セキュア モジュール	対応
Feedback	対応
DART	非対応
Start Before Login	非対応

ライセンス

- Secure Client Premier、Secure Client Advantage、または Secure Client VPN Only のいずれかの Secure Client ライセンスが必要です。
- Management Center Essentials（旧 Base）ライセンスでは、輸出規制対象機能を許可する必要があります。

  Management Center でこの機能を確認するには、**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** の順に選択します。

ガイドライン、ベストプラクティス、および制約事項

- 異なるモジュールは、異なるファイル拡張子を持つプロファイルをサポートします。

  次の表に示すように、正しいファイル拡張子を選択していることを確認します。

モジュール名（**Module Name**）	ファイル拡張子
AMP イネーブラ	*.xml、*.asp
カスタマーエクスペリエンスのフィードバック	*.xml
ISE ポスチャ	*.xml、*.isp
Network Access Manager	*.xml、*.nsp
ネットワークの可視性	*.xml、*.nvmsp
Umbrella ローミングセキュリティ	*.xml、*.json
Web セキュリティ	*.xml、*.wsp、*.wso

- DART を使用してトラブルシューティング データとログを照合し、必要に応じて Cisco TAC と共有します。

  6.7 以降のバージョンのデフォルトでは、DART は新しいリモートアクセス VPN グループポリシーで有効になっていません。6.6 以前のバージョンでは、DART はデフォルトで有効になっています。

- Windows OS で ISE ポスチャモジュールを使用する場合は、ISE ポスチャモジュールを使用する前に、Network Access Manager をインストールする必要があります。

- Cisco ISE 3.0 以降では、エージェントレスポスチャがサポートされています。

- Cisco Umbrella ローミング セキュリティ モジュールを有効にする場合は、RA VPN グループポリシーのスプリットトンネリングで[常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）] オプションを無効にしてください。

- Secure Client VPN プロファイルで SBL を有効にし、Management Center の RA VPN グループポリシーに追加する必要があります。

  Secure Client VPN プロファイルをグループポリシーに追加するには、次の手順を実行します。

  1. RA VPN グループポリシーを編集します。
  2. [Secure Client] タブをクリックし、[プロファイル（Profile）] をクリックします。
  3. [+] をクリックして、Secure Client VPN プロファイルを追加します。
  4. [保存（Save）] をクリックします。

制限事項

- グループポリシーの場合、Client モジュールごとに 1 つのエントリのみを追加できます。モジュールのエントリは編集または削除できます。
- Windows 用 Cisco Secure Client は Cisco Secure Endpoint との完全な統合を提供するため、AMP イネーブラは Cisco Secure Client 5.0 の macOS に対してのみ使用可能です。
- Network Access Manager は、macOS または Linux をサポートしていません。

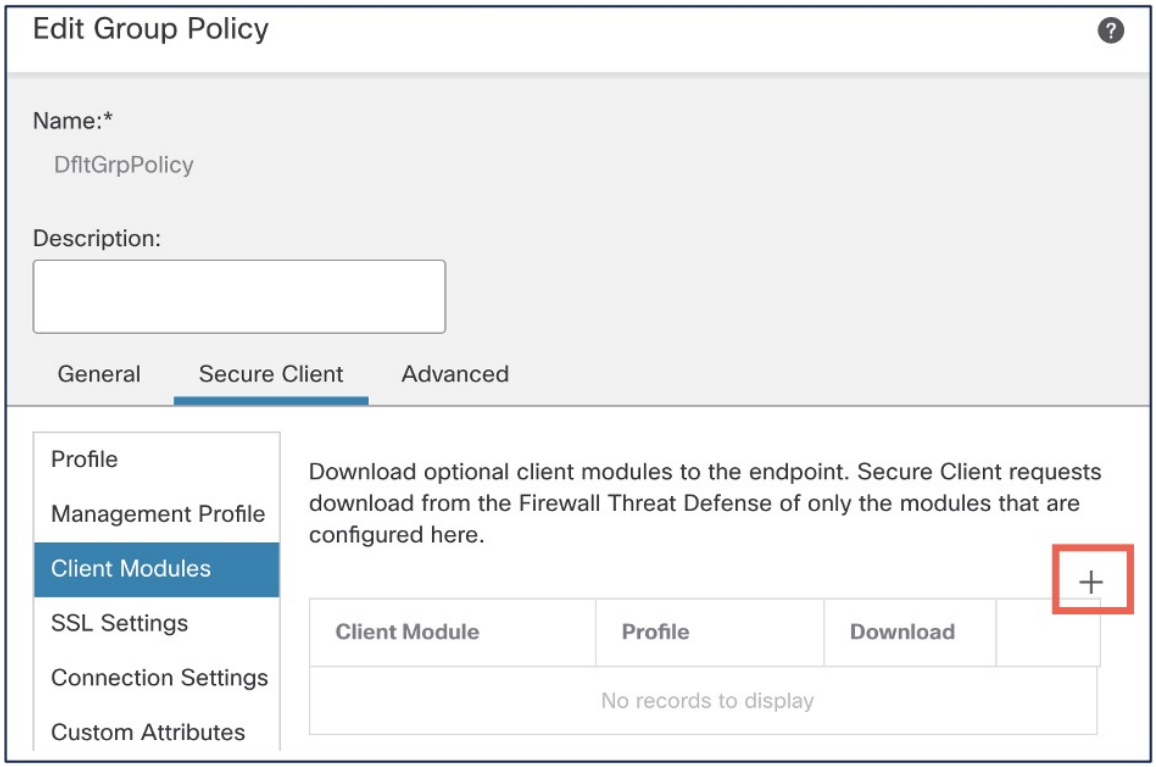
Secure Client モジュールのリモートアクセス VPN グループポリシーの設定

始める前に

Management Center でリモートアクセス VPN ポリシーを設定します。

手順

ステップ 1 Management Center の Web インターフェイスにログインします。
ステップ 2 **[デバイス（Devices）]** > **[リモートアクセス（Remote Access）]**を選択します。
ステップ 3 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。
ステップ 4 接続プロファイルを選択し、[編集（Edit）] をクリックします。
ステップ 5 [グループポリシーの編集（Edit Group Policy）] をクリックします。
ステップ 6 [Secure Client] タブをクリックします。
ステップ 7 [Clientモジュール（Client Module）] をクリックし、[+] をクリックします。



ステップ 8 [Clientモジュール（Client Module）] ドロップダウンリストからモジュールを選択します。

ステップ 9 [ダウンロードするプロファイル（Profile to download）] ドロップダウンリストからモジュールのプロファイルを選択するか、[+] をクリックしてプロファイルを追加します。

ステップ 10 [モジュールダウンロードの有効化（Enable Module Download）] チェックボックスをオンにします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

1. 設定を Threat Defense に展開します。
2. Secure Client を使用して、Threat Defense への VPN 接続を確立します。
3. Secure Client の設定を確認します。

Secure Client モジュール設定の確認

Threat Defense で

Secure Client モジュールの設定を表示するには、Threat Defense CLI で次のコマンドを使用します。

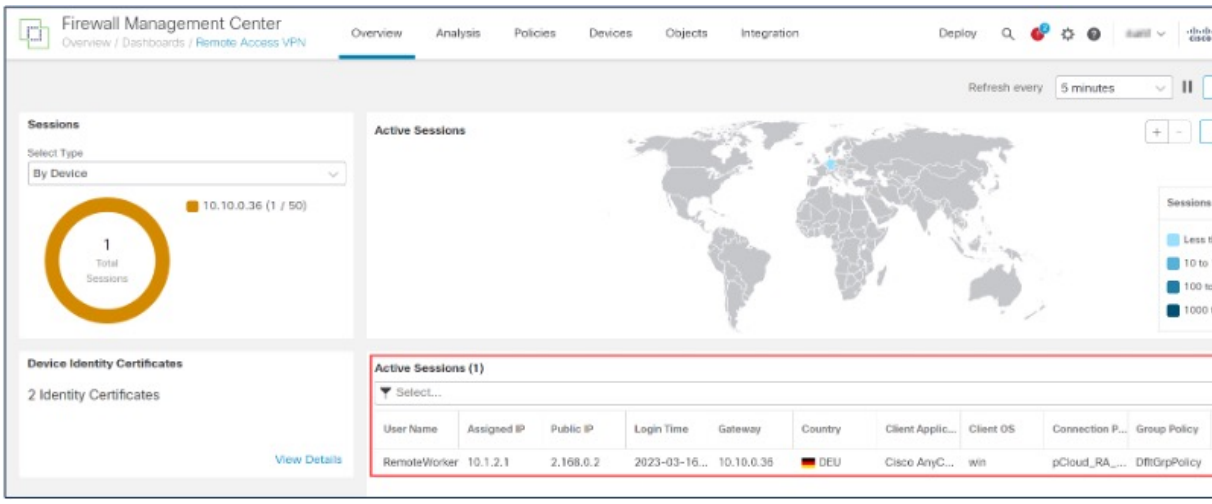
コマンド	説明
show disk0:	プロファイルとその設定を表示します。
show run webvpn	Secure Client 設定の詳細を表示します。
show run group-policy <group_policy_name>	Secure Client の RA VPN グループポリシーの詳細を表示します。
show vpn-sessiondb anyconnect	アクティブな Secure Client VPN セッションの詳細を表示します。

エンドポイントで

1. Secure Client を使用して、Threat Defense への VPN 接続を確立します。
2. 設定されたモジュールがダウンロードされ、Secure Client の一部としてインストールされているかどうかを確認します。
3. 「Profile Locations for all Operating Systems」[英語] で指定されている場所でプロファイルが使用可能かどうかを確認します。

Management Center で

リモートアクセス VPN ダッシュボードを使用して、Management Center でアクティブなリモートアクセス VPN セッションをモニターできます（**[概要（Overview）] > [リモートアクセス（Remote Access）] > [VPN]**）。ユーザーセッションに関連した問題を特定し、ネットワークとユーザーの問題を軽減できます。



Secure Client モジュールの設定例

- Secure Client Umbrella モジュールおよび Management Center を使用したエンドポイントへの DNS レイヤセキュリティの提供 （9 ページ）
- エンドポイントでの DART モジュールの設定
- Assess Endpoint Compliance Using Cisco Secure Client ISE Posture Module and Cisco Secure Firewall Management Center [英語]

Secure Client Umbrella モジュールおよび Management Center を使用したエンドポイントへの DNS レイヤセキュリティの提供

はじめる前に

次の条件が満たされていることを確認します。

- Cisco Umbrella ダッシュボードへのアクセス。
- Secure Client パッケージをローカルホストにダウンロード済み。
- Management Center でリモートアクセス VPN を設定済み。
- Management Center 上の Secure Client のバージョンがエンドポイント上のバージョンよりも新しい。
- RA VPN グループポリシーのスプリットトンネリングで、[常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）] オプションを無効にします。

手順

ステップ	タスク	詳細
1	Cisco Umbrella ダッシュボードからローカルホストに Secure Client Umbrella モジュールプロファイルをダウンロードします。	Cisco Umbrella ダッシュボードからの Secure Client Umbrella モジュールプロファイルのダウンロード（10 ページ）
2	Management Center のリモートアクセス VPN グループポリシーで Cisco Umbrella モジュールとプロファイルを設定します。	Secure Client モジュールのリモートアクセス VPN グループポリシーの設定 （6 ページ）
3	設定を Threat Defense に展開します。	Management Center メニューバーで、[展開（Deploy）] をクリックしてから、[展開（Deployment）] を選択します。

Cisco Umbrella ダッシュボードからの Secure Client Umbrella モジュールプロファイルのダウンロード

Cisco Umbrella（OrgInfo.json）ファイルには、Cisco Umbrella サービスサブスクリプションに関する特定の情報が含まれているため、セキュリティ ローミング モジュールはレポートする場所と適用するポリシーを認識できます。

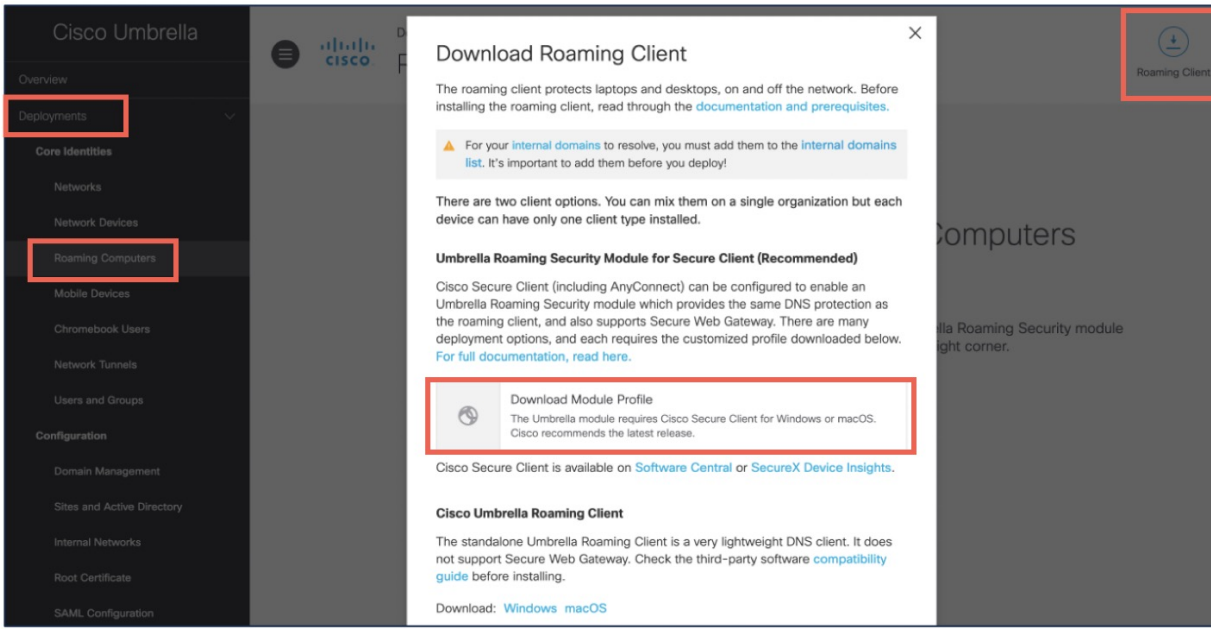
手順

ステップ 1 Cisco Umbrella にログインします。

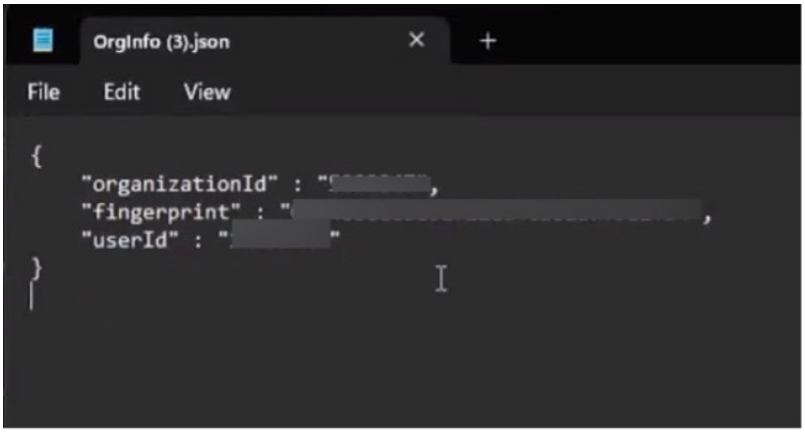
ステップ 2 **[展開（Deployments）] > [ローミングコンピュータ（Roaming Computers）]** を選択します。

ステップ 3 [ローミングクライアント（Roaming Client）] アイコンをクリックします。

ステップ 4 [モジュールプロファイルのダウンロード（Download Module Profile）] をクリックします。



OrgInfo.json ファイルの例を次に示します。



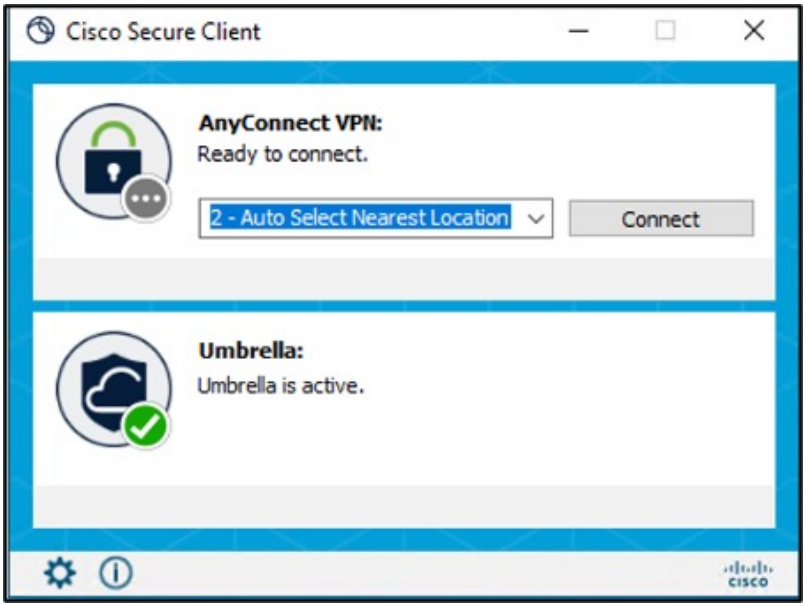
Cisco Umbrella モジュール設定の確認

Threat Defense で

- **sh vpn-sessiondb anyconnect** コマンドを使用して、Secure Client 接続が成功したことを確認します。
- リモートアクセス VPN グループポリシーの詳細を表示するには、**sh run group-policy** コマンドを使用します。

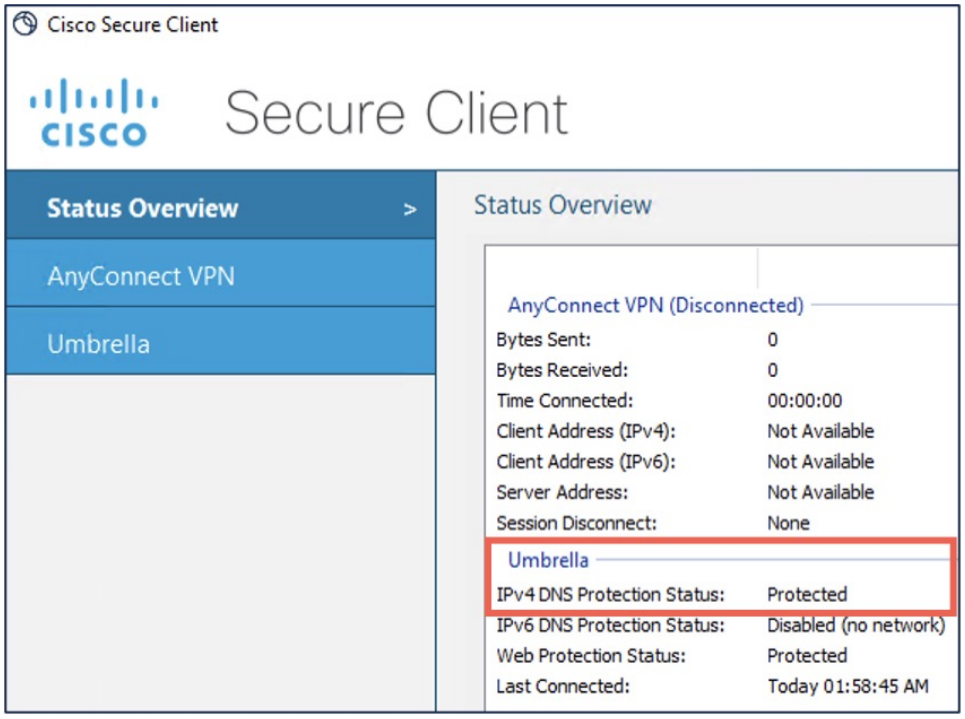
エンドポイントで

1. VPN 接続が成功したかどうか、および Cisco Umbrella モジュールがエンドポイントにダウンロードされているかどうかを確認します。



2. [統計（Statistics）] アイコンをクリックし、[ステータスの概要（Status Overview）] タブをクリックします。

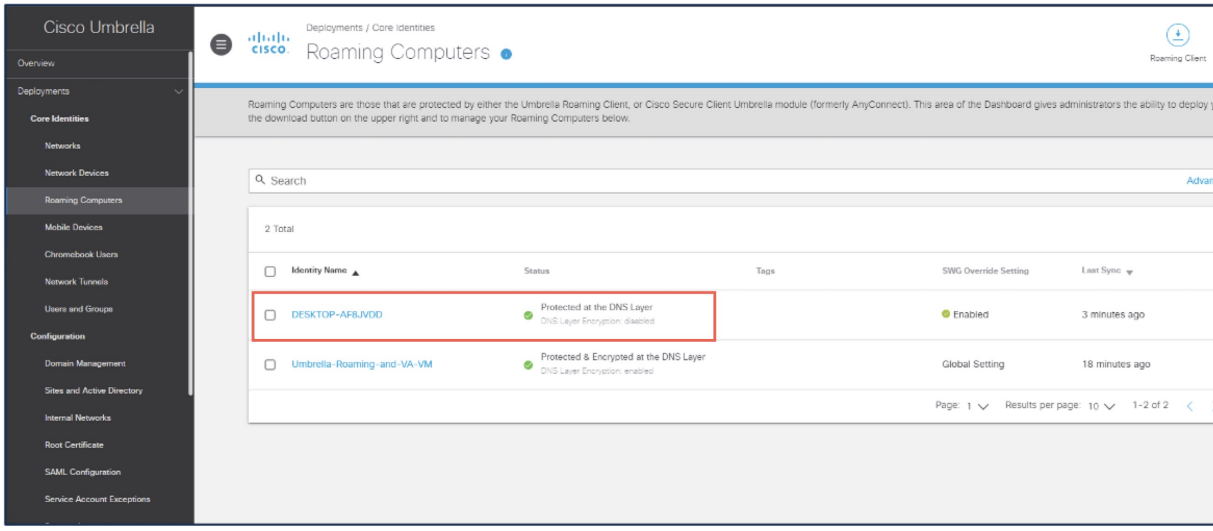
   IPv4/IPv6 DNS 保護ステータスは「保護済み（Protected）」です。



Cisco Umbrella で

[展開（Deployments）] > [ローミングコンピュータ（Roaming Computers）] を選択します。

エンドポイントのステータスは「DNS レイヤで保護済み（Protected at the DNS Layer）」です。



エンドポイントでの DART モジュールの設定

手順

ステップ 1 Secure Client パッケージをローカルホストにダウンロードします。Cisco Software Download Center [英語] を参照してください。

ステップ 2 Management Center でリモートアクセス VPN を設定します。

ステップ 3 Management Center の RA VPN グループポリシーで DART モジュールを設定します。「Secure Client モジュールのリモートアクセス VPN グループポリシーの設定」を参照してください。

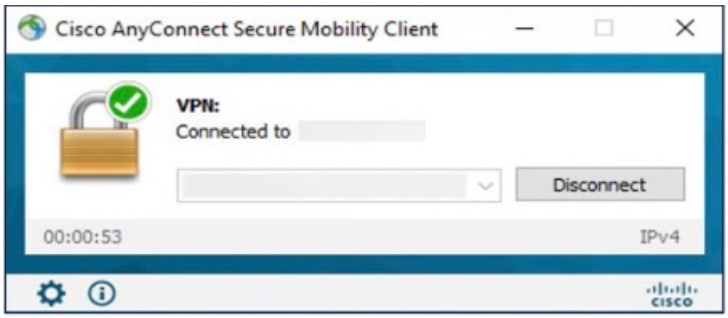
ステップ 4 設定を Threat Defense に展開します。

Management Center メニューバーで、[展開（Deploy）] をクリックしてから、[展開（Deployment）] を選択します。

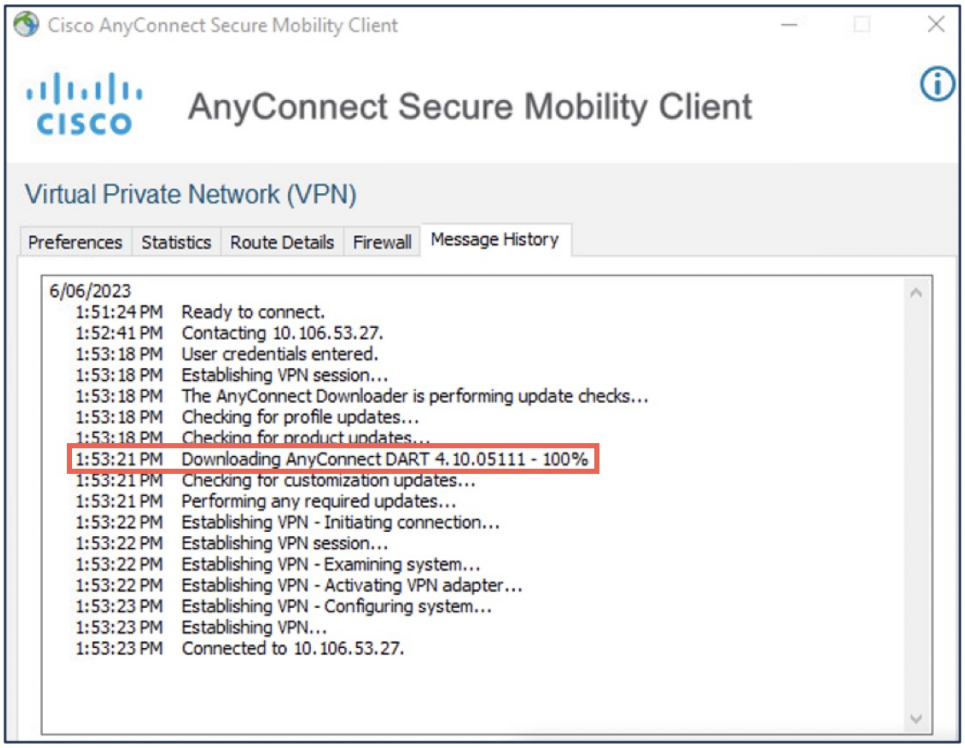
DART 設定の確認

エンドポイントで

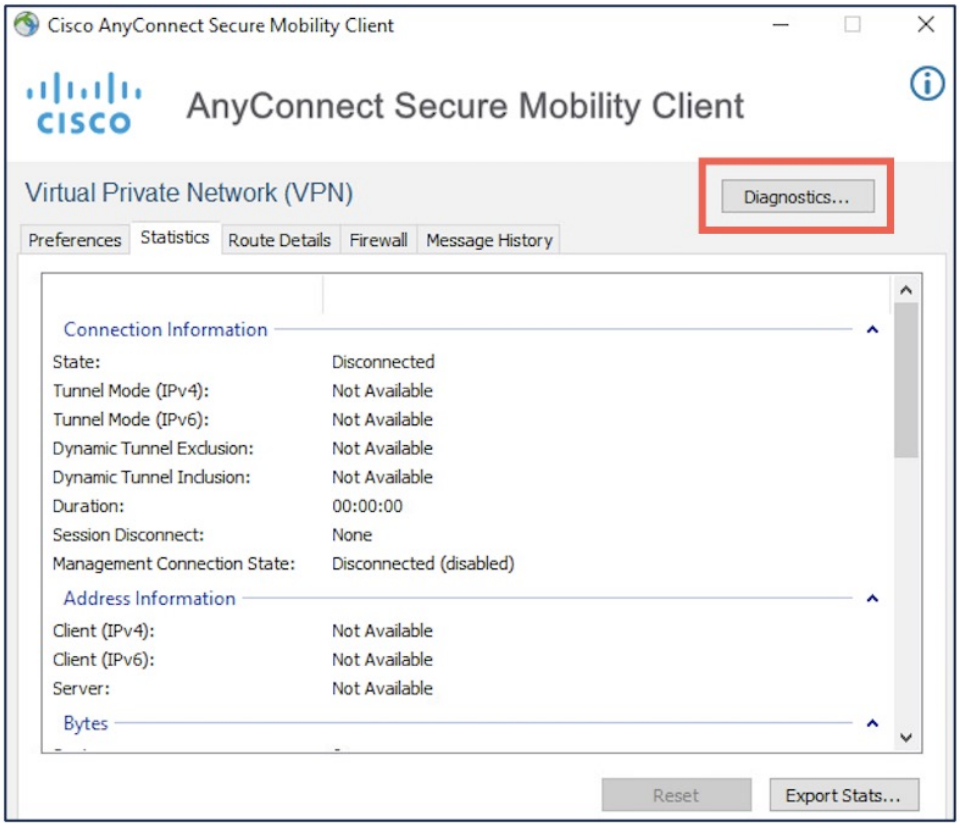
1. VPN 接続が成功したかどうかを確認します。



2. DART モジュールがエンドポイントにダウンロードされているかどうかを確認します。



3. ダウンロードが成功したら、AnyConnect クライアントを再起動します。
4. [統計（Statistics）] アイコンをクリックします。
5. [診断（Diagnostics）] をクリックします。



6. DART ウィザードを使用して DART モジュールを使用します。

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

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