Cisco Secure Firewall Management Center を使用したリモートワーカーの多要素認証の設定

初版：2023 年 5 月 25 日

DUO 多要素認証について

Duo Multi-Factor Authentication（MFA）は、デジタルアカウントやシステムへの不正アクセスから保護するためのセキュリティ対策です。ユーザーは、アクセスを許可する前に、2 つ以上の形式の認証を提供する必要があります。通常は、既知の何か（パスワードまたはPIN）と所有している何か（スマートフォンまたはセキュリティトークン）の組み合わせを使用します。

リモートアクセスVPNヘッドエンドを介して接続するリモートワーカーに対して、Cisco Secure Firewall Management Center を使用して MFA を設定できます。

対象読者

この使用例は、主に Cisco Secure Firewall 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 Duo MFA を設定するネットワーク管理者を対象としています。

このドキュメントでは、次の使用例について説明します。

- RADIUS をプライマリ認証サーバーとして使用する Duo MFA。
- プライマリ認証サーバーとして Microsoft Active Directory を使用する Duo MFA。

シナリオ

Nik 氏は組織のネットワーク管理者です。Nik 氏は、従業員がどこからでも組織のネットワークに接続できるように、リモートアクセス VPN の設定を担当しています。いくつかの理由から、リモートワーク環境はサイバー攻撃のリスクを高める可能性があります。ユーザー名とパスワードは、簡単に侵害される可能性があるため、VPNを介してネットワークにアクセスするための唯一の認証識別子にすることはできません。

そのため、Nik 氏は組織のネットワークに安全にアクセスするために、ユーザー名とパスワードに加えて追加情報を提供することをリモートワーカーに義務づける Duo MFA を使用することにしました。

Duo MFA を使用する利点

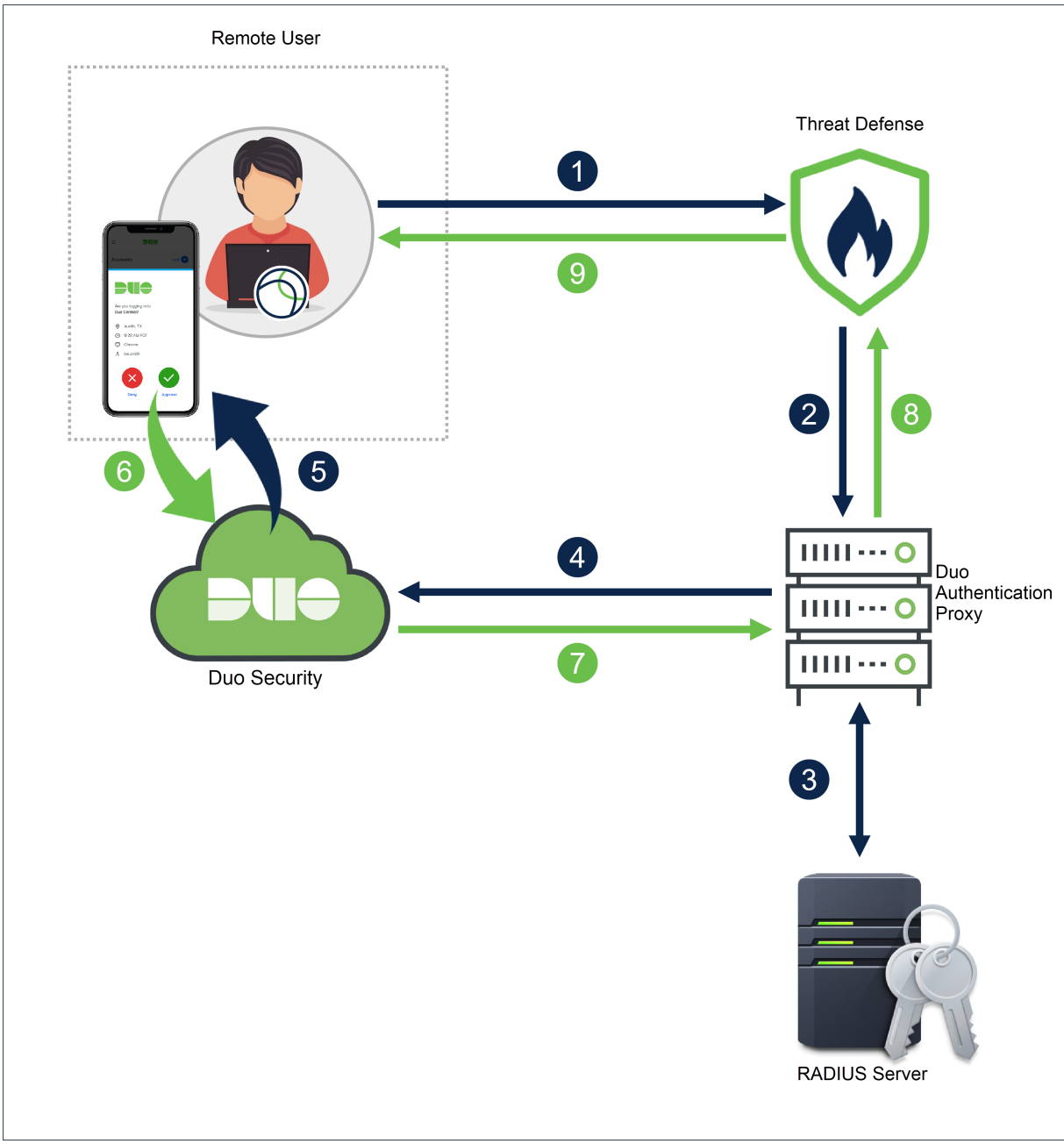
- コンプライアンス要件：多くの業界や組織には、機密データとシステムを保護するために MFA を使用することを義務付けるコンプライアンス要件があります。Duo MFA は、これらの要件を満たすのに役立ちます。Duo は、連邦および公共部門の組織のセキュリティニーズを満たすように調整された FedRAMP Authorized 認証を提供します。
- フィッシング攻撃からの保護：Duo MFA は、攻撃者がリモートワーカーのログイン情報を盗むフィッシング攻撃から保護するのに役立ちます。Duo MFA では、ユーザーがフィッシング攻撃に陥ってパスワードを入力した場合でも、攻撃者はアクセスするために 2 番目の要素を必要とします。
- ユーザーの利便性：Duo MFA は、信頼できるデバイスを記憶するように設定できるため、ユーザーがログインするたびに第 2 要素を入力する必要がなくなります。これにより、セキュリティが維持されるとともに、ユーザーにとって認証プロセスの利便性が高まります。
- 設定が簡単：Duo は、リモートワーカーとその詳細情報を簡単に登録できるクラウドベースのソリューションです。

システムの仕組み

リモートワーカーは、ログイン情報を使用して認証する必要があり、その後に設定された Duo パスコード（プッシュ、電話、パスコード、または SMS）のいずれかを使用する必要があります。

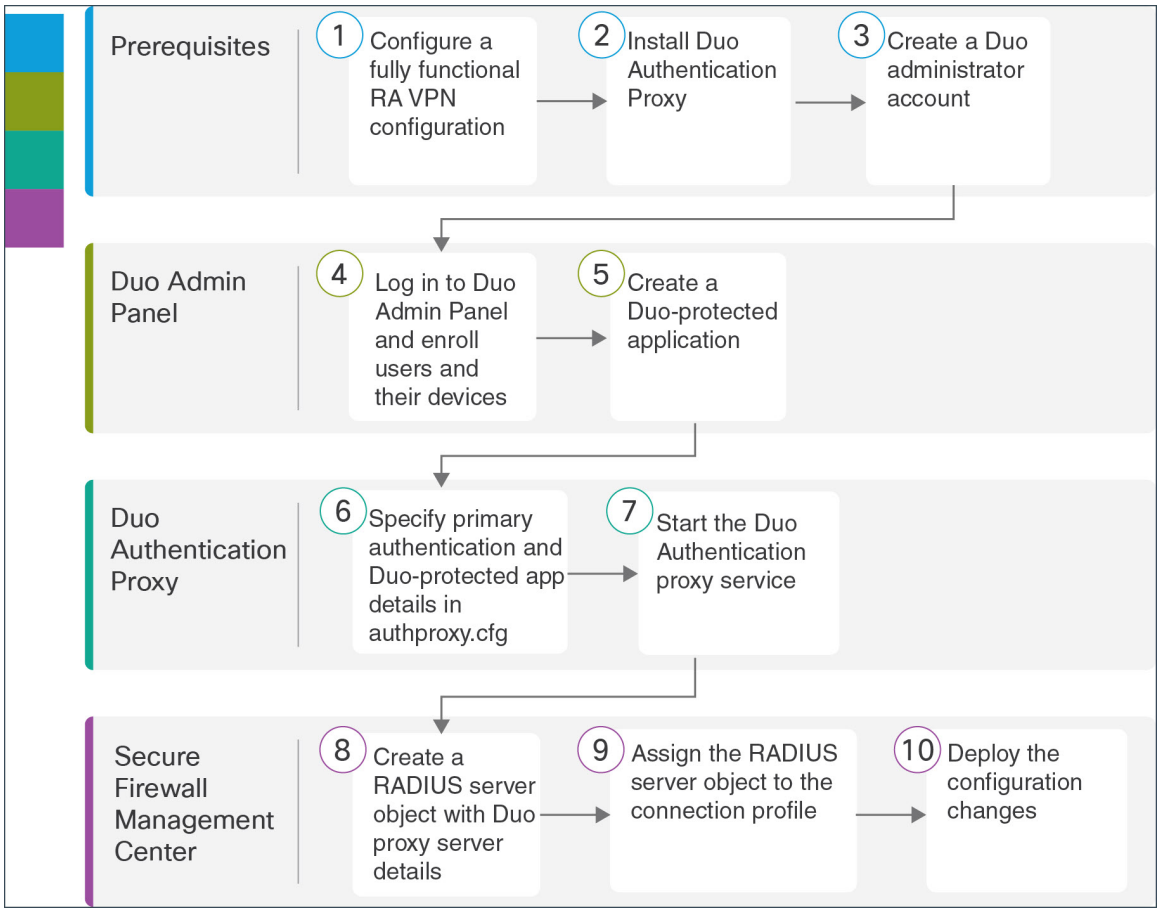
DUO による多要素認証設定は、次のコンポーネントで構成されています。

- Secure Firewall Management Center：リモートアクセス VPN ポリシーを設定し、ライブセッションを監視するためのオンプレミスマネージャです。
- Secure Firepower Threat Defense：リモートワーカーが組織ネットワークに接続するための VPN トンネルを作成します。
- Cisco Secure Client：このユーティリティは、脅威防御デバイスとの VPN セッションを確立するためにリモートワーカーのデバイスにインストールされます。
- [プライマリ認証サーバー（Primary Authentication Server）]：プライマリ認証サーバーは、ユーザーログイン情報を保存するデータベースです。RADIUS または AD サーバーはプライマリ認証エージェントとして設定できます。
- Duo Authentication Proxy：Duo Authentication Proxy は、脅威防御から認証要求を受信してプライマリ認証を実行し、Duo に接続してセカンダリ認証を行うオンプレミスのソフトウェアサービスです。



エンドツーエンドの手順

次の図は、リモートワーカー用に Duo MFA を設定するタスクを示しています。



ステップ	アプリケーション	説明
1	前提条件	完全に機能するリモートアクセス VPN を設定します。「前提条件」を参照してください。
2	前提条件	Duo Authentication Proxy をインストールします「前提条件」を参照してください。
3	前提条件	新しい管理者アカウントを作成します。「前提条件」を参照してください。
4	Duo Admin Panel	Duo Admin Panel でユーザーを追加する でユーザーとデバイスを登録します。
5	Duo Admin Panel	Duo で保護されたアプリケーションを作成して、統合の詳細を生成します。「Duo-Protected アプリケーションの作成」を参照してください。

ステップ	アプリケーション	説明
6	Duo Authentication Proxy	**Duo Authentication Proxy Manager** アプリケーションを設定して、「authproxy.cfg」ファイルを変更します。RADIUS または AD サーバーの詳細を使用した Duo Authentication Proxy の設定を参照してください。
7	Duo Authentication Proxy	Duo Authentication Proxy サービスを開始します。「RADIUS または AD サーバーの詳細を使用した Duo Authentication Proxyの設定」を参照してください。
8	Management Center	RADIUS サーバーオブジェクトを作成します。「Duo の RADIUS サーバーオブジェクトの作成」を参照してください。
9	Management Center	RADIUS サーバーオブジェクトを接続プロファイルに割り当てます。Management Center を使用した接続プロファイルへの Radius サーバーオブジェクトの割り当てを参照してください。
10	Management Center	設定をデバイスに展開します。「Management Center を使用した接続プロファイルへの Radius サーバーオブジェクトの割り当て」を参照してください。

前提条件

次の条件が満たされていることを確認します。

- FMC 管理の脅威防御デバイスでリモートアクセス VPN が設定されている。
- Windows/Linux ホストに Duo Authentication Proxy サーバーがインストールされている。詳細については、『Duo Authentication Proxy Reference』を参照してください。

（注） シームレスな設定のために、Proxy Manager をインストールすることをお勧めします。

- 新しい管理者アカウントが作成されている。『Getting Started with Duo Security』を参照してください。

（注） 新しいアカウントを使用して Duo Admin Panel にログインし、[請求（Billing）] をクリックして、必要なプランにアップグレードします。

Duo Admin Panel でユーザーを追加する

手順

ステップ 1 Duo Admin Panel にログインします。

ステップ 2 組織のユーザーを Duo に登録します。「Enroll Users」を参照してください。

- Duo で指定されたユーザー名は、プライマリ認証サーバーのユーザー名と一致する必要があります。
- Duo Push を使用するには、デバイスに Duo Mobile アプリをインストールしてから、Duo アカウントをアプリに追加する必要があります。

Duo-Protected アプリケーションの作成

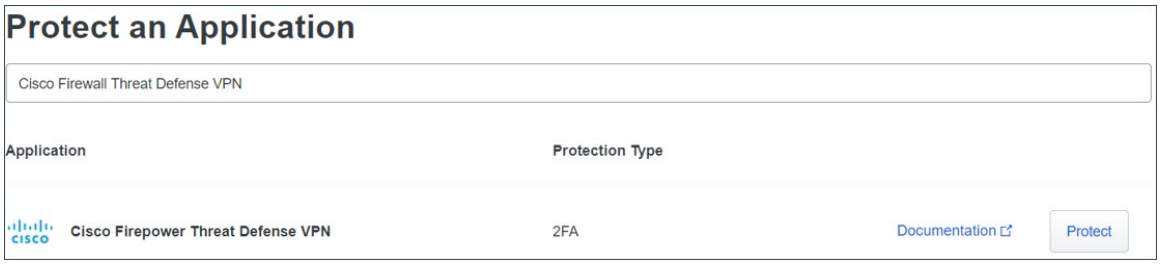
Duo-Protected アプリケーションは、Duo と Cisco Secure Firewall Threat Defense リモートアクセス VPN を統合するサービスです。

手順

ステップ 1 Duo Admin Panel にログインします。

ステップ 2 **[アプリケーション（Applications）]** > **[アプリケーションの保護（Protect an Application）]** を選択します。

ステップ 3 アプリケーションリストで **Cisco Firepower Threat Defense VPN** を探し、[保護（Protect）] をクリックします。



アプリケーションは、**統合キー**、**秘密キー**、および **API ホスト名**を生成します。Duo Authentication Proxy の設定を完了するには、この情報を指定する必要があります。

Duo でのアプリケーションの保護と追加のアプリケーションオプションの詳細については、「Protecting Applications」を参照してください。

ステップ 4 [保存（Save）] が表示されるまでページを下にスクロールします。

ステップ 5 [保存（Save）] をクリックします。

RADIUS または AD サーバーの詳細を使用した Duo Authentication Proxyの設定

RADIUS または Active Directory のいずれかを使用して、プライマリ認証を実行できます。

手順

ステップ 1 Duo Authentication Proxy がインストールされているホストにログインします。

ステップ 2 **Duo Authentication Proxy Manager** アプリケーションを開きます。

削除可能なサンプルコンテンツが含まれている場合があります。

ステップ 3 RADIUS をプライマリ認証サーバーとして使用するには、authoproxy.cfg ファイルを次の設定に変更します。

Configure: authproxy.cfg

```
[main]
debug=true

[radius_client]
host=10.10.0.28
secret=cisco
pass_through_all=true

[radius_server_auto2]
ikey=
skey=
api_host=
radius_ip_1=
radius_secret_1=cisco
client=radius_client
```

[radius_client]	RADIUS をプライマリ認証サーバーとして使用します。
ホスト	プライマリ RADIUS サーバーの IP アドレス。この例では、10.10.0.28 は Cisco ISE サーバーのアドレスです。
secret	認証プロキシと既存の RADIUS サーバーの間で秘密が共有されます。ISE サーバーのインストール時に指定した秘密キーを入力します。

[radius_server_auto2]	—
ikey	Duo-Protected アプリケーションの作成時に生成された Duo 統合キーを入力します。
skey	Duo-Protected アプリケーションの作成時に生成された秘密キーを入力します。
api_host	Duo-Protected アプリケーションの作成時に生成された Duo API ホスト名を入力します。
radius_ip_1	Threat Defense SSL VPN デバイスの IP アドレス。
radius_secret_1	プロキシと脅威防御 SSL VPN デバイス間で共有される秘密。
クライアント	radius_client プライマリ認証に RADIUS を使用する。[radius_client] セクションが設定されていることを確認します。

追加のオプション設定については、「RADIUS configuration」を参照してください。

ステップ 4 AD サーバーをプライマリ認証サーバーとして使用するには、authoproxy.cfg ファイルを次の設定に変更します。

Configure: authproxy.cfg

```
1  [main]
2  debug=true
3
4  [ad_client]
5  host=10.10.0.41
6  service_account_username=administrator
7  service_account_password=[redacted]
8  search_dn=DC=cnsdoc,DC=acme,DC=com
9
10 [radius_server_auto]
11 ikey=[redacted]
12 skey=[redacted]
13 api_host=[redacted]
14 radius_ip_1=[redacted]
15 radius_secret_1=cisco
16 client=ad_client
```

[ad_client]	AD をプライマリ認証サーバーとして使用します。

ホスト	ドメインコントローラまたはディレクトリサーバーの IP アドレスまたはホスト名。この例では、10.10.0.41 は AD サーバーのアドレスです。
service_account_username	ディレクトリにバインドして検索を実行する権限を持つドメインアカウントのユーザー名。読み取り専用アクセス権を持つサービスアカウントを作成することをお勧めします。
service_account_password	service_account_username に対応するパスワード。
search_dn	ログインを許可するすべてのユーザーを含む Active Directory/LDAP コンテナまたは組織単位（OU）の LDAP 識別名（DN）。
[radius_server_auto]	Duo-Protected アプリケーションの詳細。
ikey	Duo-Protected アプリケーションの作成時に生成された Duo 統合キーを入力します。
skey	Duo-Protected アプリケーションの作成時に生成された秘密キーを入力します。
api_host	Duo-Protected アプリケーションの作成時に生成された Duo API ホスト名を入力します。
radius_ip_1	Threat Defense SSL VPN デバイスの IP アドレス。
radius_secret_1	プロキシと脅威防御 SSL VPN デバイス間で共有される秘密。
クライアント	ad_client プライマリ認証にアクティブディレクトリを使用する。[ad_client] セクションが設定されていることを確認します。

追加のオプション設定については、「Active Directory configuration」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 プロキシマネージャウィンドウの上部にある [サービスの開始（Start Service）] ボタンをクリックして、サービスを開始します。

ステップ 7 **[検証（Validate）]** をクリックして、設定をテストします。ウィンドウで設定の問題が報告された場合は、ログファイルを読んでトラブルシューティングを行う必要があります。「Duo Authentication Proxy 設定のトラブルシューティング」を参照してください。

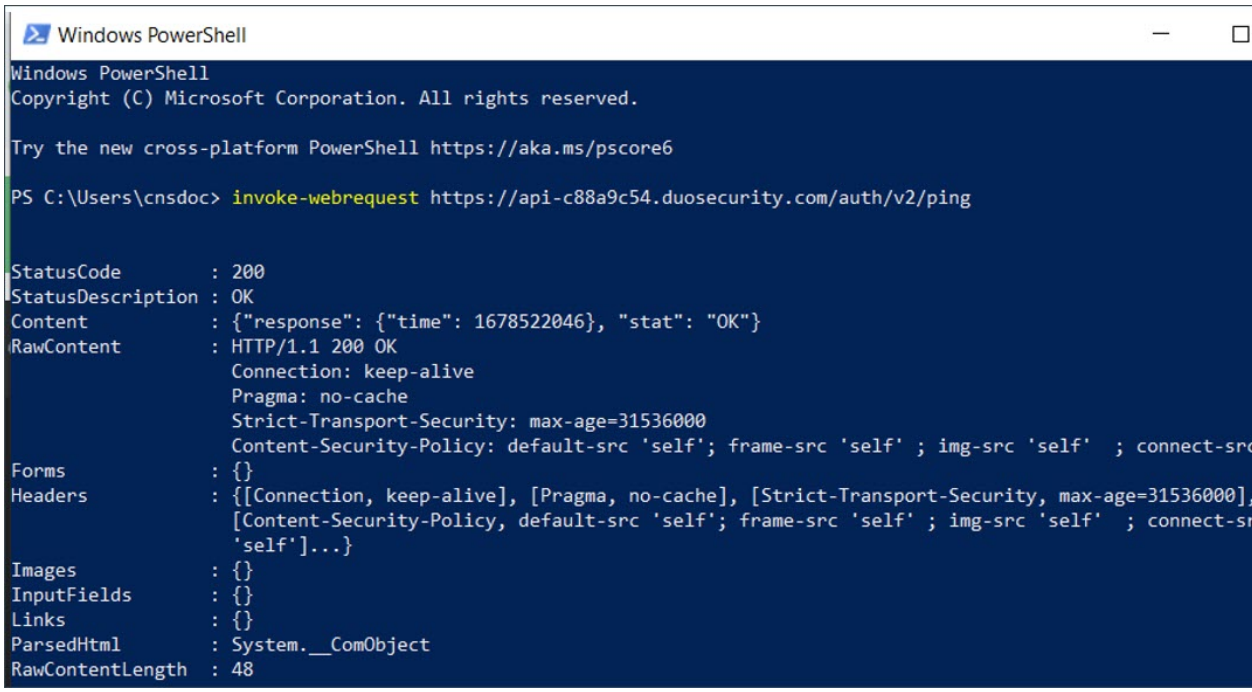
Duo Authentication Proxy 設定の確認

手順

ステップ 1 Windows ホストで PowerShell アプリケーションを起動します。Linux ホストで同じコマンドを実行できます。

ステップ 2 **Invoke-webrequest https://api-host/auth/v2/ping** コマンドを実行します。api-host を、Duo-Protected アプリケーションから生成された Duo API ホスト名に置き換えます。

設定が正しい場合は、同様の応答が表示されます。



Duo の RADIUS サーバーオブジェクトの作成

Duo Authentication Proxy がインストールされている Windows/Linux マシンに関する情報を使用して、RADIUS サーバーオブジェクトを作成する必要があります。このオブジェクトは、AAA サーバー設定ページで認証サーバーとして使用します。

手順

ステップ 1 脅威防御ヘッドエンドを管理する Management Center にログインします。

ステップ 2 Duo プロキシサーバーの詳細を使用してDuo RADIUS サーバーオブジェクトを作成します。

1. **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）] > [RADIUSサーバーグループを追加（Add RADIUS Server Group）]** を選択します。
2. 次の詳細を入力します。

フィールド	値
名前（Name）	オブジェクトのわかりやすい名前（「DuoRADIUS」など）。
Group Accounting Mode	[シングル（Single）] のままにします。
再試行間隔（Retry Interval）	[10] のままにします。
レルム（Realm）	必須ではありません。
認可のみ有効化 **一時的なアカウント更新の有効化** **ダイナミック認証の有効化**	有効化しないでください。

3. [+] をクリックして、RADIUS サーバーを追加します。
4. [IPアドレス/ホスト名（IP Address/Hostname）] に、Duo Authentication Proxy がインストールされている Windows/Linux マシンの IP アドレスを入力します。
5. [認証ポート（Authentication Port）] は 1812 のままにします。
6. 管理対象デバイス（クライアント）と RADIUS サーバー間でデータを暗号化するための共有秘密を入力します。このフィールドで定義した共有秘密キーは、[RADIUS認証設定（RADIUS Authentication Settings）] ページの RADIUS サーバーのキーと一致している必要があります。[キーの確認（Confirm Key）] フィールドでもう一度キーを入力します。
7. [ルーテッド（Routed）] または [特定のインターフェイス（Specific Interface）] を選択します。ここでの選択は、脅威防御から Duo RADIUS AAA サーバーへの接続がどのように確立されるかによって異なります。
8. 変更を保存します。

Management Center を使用した接続プロファイルへの Radius サーバーオブジェクトの割り当て

手順

ステップ 1 Management Center で、**[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 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

（注） 新しいリモートアクセス VPN ポリシーを作成するときに、RADIUS サーバーオブジェクトを割り当てることができます。

ステップ 3 リモートアクセス VPN 設定で、プライマリ認証方式を [Duo RADIUS] に変更します。

a) [接続プロファイル（Connection Profile）] を選択し、[編集（Edit）] をクリックします。
b) [AAA] タブをクリックします。
c) [認証サーバー（Authentication Server）] リストで、作成した Duo RADIUS サーバーオブジェクトを選択します。
d) 変更を保存します。

ステップ 4 設定変更を展開します。『Cisco Secure Firewall Management Center Device Configuration Guide, XY』の「**Configuration Deployment**」の章にある「Deploy Configuration Changes」の項を参照してください。

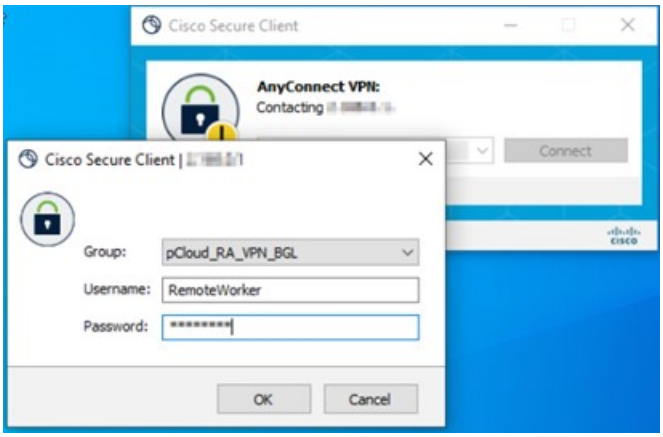
接続のテスト

手順

ステップ 1 Cisco Secure AnyConnect クライアントを起動し Duo RADIUS または Active Directory 認証を使用している VPN プロファイルを選択します。

ステップ 2 ユーザー名とパスワードを入力し、[OK] をクリックします。

自動パスコード、プッシュ、SMS、または電話を受信します。



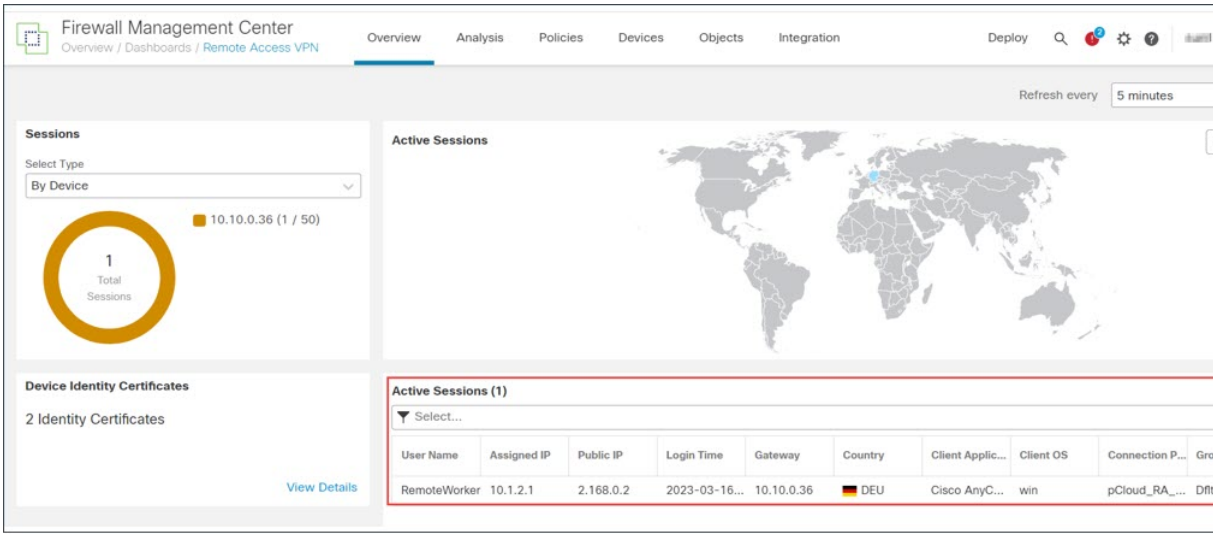
ステップ 3 Duo 認証要求を承認します。クライアントは VPN に接続されます。

Management Center でのリモートアクセス VPN ライブセッションのモニタリング

Management Center はダッシュボードを提供し、デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイムデータをモニターします。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

Management Center で、**[概要（Overview）] > [リモートアクセス VPN（Remote Access VPN）]** の順に選択します。

アクティブなセッションがダッシュボードに表示されます。



Duo Authentication Proxy 設定のトラブルシューティング

ログファイルを読んで、設定の問題を解決します。

- https://learn.microsoft.com/en-us/answers/questions/149890/unable-to-bind-or-log-into-ldap-using-specific-cre [英語]
- https://duo.com/docs/authproxy-reference#using-the-support-tool [英語]
- https://help.duo.com/s/article/1126?language=en_US [英語]
- https://help.duo.com/s/article/4758?language=en_US [英語]

リモートワーカーが VPN に接続できない

このセクションでは、リモートワーカーが直面している接続の問題を修復するための診断手順について説明します。

- Duo Admin Panel がユーザー認証ログを受信しているかどうかを確認します。「Duo Admin Panel で認証ログレポートを表示する」を参照してください。
- リモートワーカーが Duo から通知を受信しているかどうかを確認します。「Duo Push でユーザー設定を確認する」を参照してください。
- 脅威防御がプライマリ認証サーバーに到達できるかどうかを確認します。「認証サーバーと脅威防御の接続の決定」を参照してください。

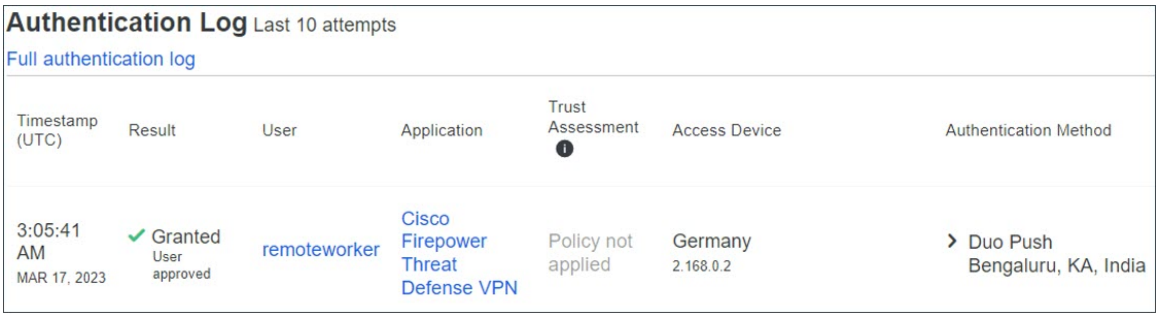
（注） 一般的なリモートアクセス VPN 関連の問題については、「VPN Monitoring and Troubleshooting」を参照してください。

Duo Admin Panel で認証ログレポートを表示する

Duo Admin Panel には、ユーザーの MFA 認証が成功したか失敗したかを示すダッシュボードが表示されます。これらのログでは、ユーザー名、場所、時間、認証要素のタイプなどを使用して、ユーザーがどこでどのように認証したかが示されます。

手順

ステップ 1 Duo Admin Panel にログインします。
ステップ 2 [ダッシュボード（Dashboard）] をクリックします。
ステップ 3 [認証ログ（Authentication Log）] セクションで、認証ログを確認できます。



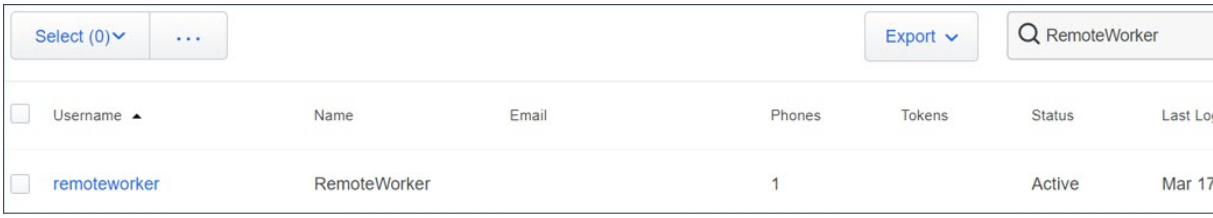
Duo Push でユーザー設定を確認する

Duo Admin Panel からリモートワーカーのスマートフォンに Duo プッシュトークンを送信して、詳細が正しく設定されているかどうかを確認できます。

手順

ステップ 1 Duo Admin Panel にログインします。

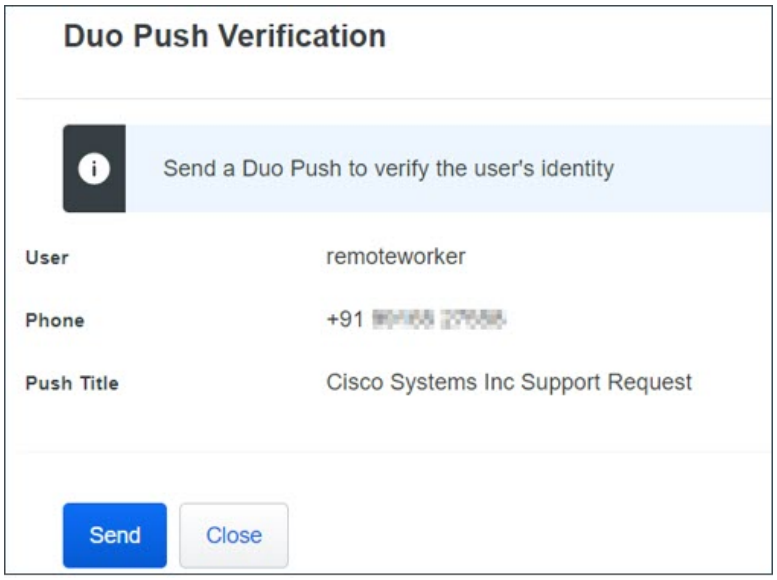
ステップ 2 [ユーザ（Users）] をクリックし、必要なリモートワーカーを検索します。



ステップ 3 ユーザー名のリンクをクリックして、ユーザーの詳細ページを開きます。

ステップ 4 ユーザーが Duo Mobile が有効になっているスマートフォンを接続している場合は、[Duo Push の送信（Send Duo Push）] リンクが表示されます。リンクが表示されない場合は、リモートワーカーが Duo Push 用に電話をアクティブ化できるように支援が必要になることがあります。

ステップ 5 [Duo Pushの送信（Send Duo Push）] リンクをクリックします。



ステップ 6 リモートワーカーがDuoモバイルアプリケーションを使用してデバイスにアクセスできることを確認し、[送信（Send）] をクリックします。

正しく設定されている場合、リモートワーカーはスマートフォンで通知を受信します。

ステップ 7 リモートワーカーがリクエストを確認すると、確認メッセージが表示されます。

認証サーバーと脅威防御の接続の決定

始める前に

これは、脅威防御がプライマリ認証サーバーに到達できない場合に発生する可能性があります。

トラブルシューティングを行うために、認証サーバーと Duo Admin Panel で一時的なユーザーアカウントを作成します。

手順

ステップ 1 脅威防御 CLI にログインします。

ステップ 2 **system support diagnostic-cli** を実行します。

ステップ 3 **show run aaa-server** を実行します。

```
> firepower# show run aaa-server
aaa-server Duo_RADIUS protocol radius
aaa-server Duo_RADIUS (management) host 10.10.0.34
 timeout 60
key *****
authentication-port 1812
accounting-port 1813
aaa-server Radius_ISE_Server protocol radius
aaa-server Radius_ISE_Server (management) host 10.10.0.28
key *****
authentication-port 1812
accounting-port 1813
```

ステップ 4 RADIUS サーバーオブジェクト名をコピーします。この例では、「Duo_RADIUS」は、Duo Authentication Proxy がインストールされているホスト情報を含む RADIUS サーバーオブジェクトの名前です。

ステップ 5 **test aaa authentication <radius server object name> host <host_ip_address>** を実行します。

radius_server_object_name	RADIUS サーバーオブジェクトの名前。
host_ip_address	Duo Authentication Proxy がインストールされているホストの IP アドレス。

ステップ 6 一時ユーザーアカウントのユーザー名とパスワードを入力します。

ステップ 7 通知を受け取ります。

ステップ 8 デバイスがサーバーに到達できる場合は、次のメッセージが表示されます。

INFO: Authentication Successful

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。