Tanium™ Endpoint Identity ユーザガイド

バージョン 1.1.3

2021年12月29日

この文書の内容は予告なく変更されることがあります。また、本書に記載の内容は「現状のまま」提供されており、正確性には万全を期しておりますが、Taniumの顧客販売契約に規定されている保証を除き、明示または暗黙を問わずいかなる保証もしません。別段の規定がない限り、Taniumはいかなる責任も負いません。TaniumおよびそのサプライヤIは、Tanium Inc.がかかる損害の可能性を事前に通知されていたとしても、本書の使用または使用できないことから生じる、利益損失やデータ損失をはじめとする間接的損害や特別損害、結果的損害、および付随的損害に対して一切の責任を負いません。

本書で使用されているIPアドレスは、実際のアドレスであることを意図していません。本書に記載されている例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、例示の目的にのみ使用されています。例示コンテンツに実際のIPアドレスが使用されていたとしても、特別な意図はなく、偶然です。

最新のTanium製品のマニュアルについては、https://docs.tanium.com を参照してください。

この文書には、第三者が提供するコンテンツや製品(ハードウェアおよびソフトウェアを含む)、サービス(「第三者のアイテム」)に対するアクセス手段や、第三者のそうした情報そのものが含まれていることがあります。Tanium Inc.およびその関連会社は、(i)それらの第三者のアイテムに対して責任を負うものではなく、第三者のアイテムに関するすべての保証および責任を明示的に放棄し、(ii)お客様とTaniumとの間の有効な契約に明記されているのでない限り、かかる第三者のアイテムへのアクセスや、利用に起因する損失、費用または損害について責任を負いません。

また、この文書は、特定の第三者のアイテムの使用やTanium製品との組み合わせを求めるものでも、想定するものでもありません。そのような組み合わせによって生じた知的財産権の侵害について、Taniumおよびその関連会社は一切責任を負いません。第三者のアイテムとTanium製品の組み合わせが適切であるかどうか、また第三者の知的財産権を侵害しないかどうかの判定の責任はTaniumではなくお客様にあります。

Taniumは、Tanium Softwareの操作をより直感的にして、成功までの時間を短縮できるよう最高のアクセシビリティ基準の達成に全力で取り組んでいます。高いアクセシビリティ基準を確保するため、Taniumは米国連邦規則、特に1998年のリハビリテーション法の第508項に準拠しています。当社は、長年にわたって製品開発の過程でサードパーティのアクセシビリティ評価を実施してきました。最近では2019年9月、すべての主要製品モジュールについてWCAG 2.1/VPAT 2.3規格に対する包括的な監査を終了しました。Taniumは、見込み客を含むあらゆるお客様が大規模なソリューション計画立案プロセスの一環としてモジュール単位でVPATレポートを入手できるようにしています。

新製品や新機能を続々と提供する中、Taniumはテストを実施することでアクセシビリティ指針の徹底を図ります。Taniumは、問題の重要度と変更の範囲を踏まえ、実現可能な範囲でこの徹底に最大限の努力をすることをお約束します。これらの目標は、当社の既存のリソースとともに納品が計画されている機能およびリリースにも組み込まれます。

Taniumは、お客様がご使用のTaniumモジュールと有用な技術要件に基づいてソリューションを使いやすくすることに関するお客様のご意見・ご要望をお待ちしています。Taniumのカスタマーコミュニティにとってアクセシビリティ要件は重要であり、当社は全体的な製品のロードマップの中でそうした要件に対する遵守を優先させることをお約束します。Taniumは当社の進捗とマイルストーンの透明性を維持し、この作業に関するさらなる質問や話し合いを歓迎します。詳細は、営業担当者にお問い合わせいただくか、Taniumサポート(support@tanium.com)またはaccessibility@tanium.comに電子メールでお問い合わせください。

Taniumは米国およびその他の国におけるTanium,Inc.の商標です。記載されているその他の社名、製品名、サービス名は各社の商標または登録商標です。

目次

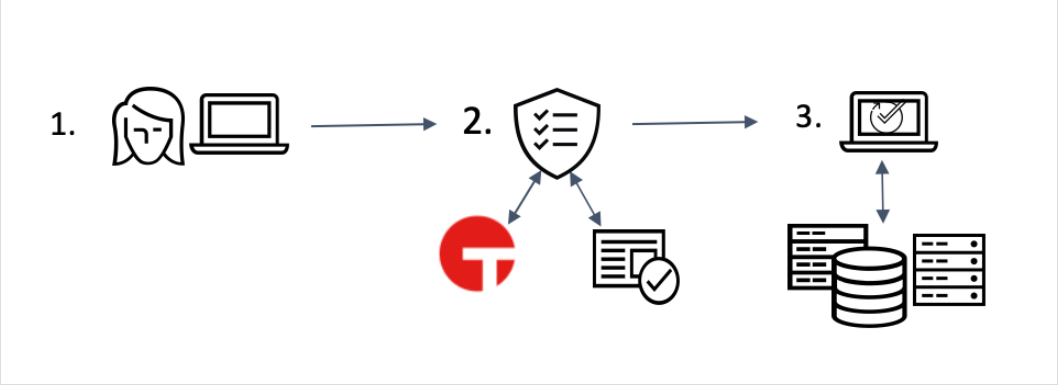
Endpoint Identityの概要

Endpoint Identityを使用すると、クラウドアクセスセキュリティブローカや、CloudflareやGoogle BeyondCorpなどのゼロトラストネットワークアクセスプロバイダとTaniumを統合して、クラウドアプリケーションやゼロトラストネットワークに接続するデバイスが管理され、安全を確保できます。

統合シナリオの概要

TaniumエンドポイントでEndpoint Identityを設定されていると、IDプロバイダはエンドポイントにクエリを発行して情報を得ることができます。この情報は、認証プロバイダや承認プロバイダがエンドポイントとユーザに特権アプリケーションへのアクセスを許可するかどうかを決定するのに役立ちます。

次の図は、この仕組みを表しています。



1. 従業員がアプリケーションへのアクセス権を申請します。たとえば、従業員が、会社支給の新しいコンピュータ、あるいは会社支給の古いコンピュータ、自宅のコンピュータからアクセス権を申請するとします。
2. 認証または承認プロバイダは申請を受け取って、以下のことを行います。
    1. Endpoint Identityを使用したエンドポイントのセキュリティの確認。Endpoint Identityから認証または承認プロバイダに情報が返されます。エンドポイントにTanium Clientがインストールされている場合、この情報にはオペレーティングシステムの更新が最後に適用された日時、脆弱性スコアが含まれます。
    2. ユーザIDの確認。
3. 検証結果と会社のポリシーに基づいて、認証または承認プロバイダは、アプリケーションへのアクセス権を従業員に付与するか却下します。
   たとえば、従業員はTaniumが管理する最新のコンピュータから重要なアプリケーションにアクセスできるかもしれませんが、Taniumの管理対象外のコンピュータからは同じアプリケーションにアクセスできません。同じ従業員が、Taniumの管理対象外のコンピュータから重要でないアプリケーションにはアクセスできます。

設定の概要

TaniumエンドポイントがEndpoint Identityのデータを提供するように設定するには、設定とパッケージをエンドポイントに展開します。詳細は、エンドポイントでEndpoint Identityを設定する(10ページ)を参照してください。

IDプロバイダの統合

エンドポイントが設定されると、Endpoint IdentityのAPIは、Taniumが管理するエンドポイントに関するプラットフォームやPatchのステータス、Complyの脆弱性情報を認証または承認プロバイダに返します。Taniumは、APIリクエストを受信するたびに値を計算します。認証または承認プロバイダは、このエンドポイント情報を利用して、クラウドアプリケーションやゼロトラストネットワークに対するアクセス権を管理することができます。

他のTanium製品との統合

Comply

Tanium™ Complyによって脆弱性スキャンが実行されている場合は、エンドポイントごとにスキャンの最新の結果が返されます。詳細は、「Tanium Complyユーザガイド」を参照してください。

Patch

Tanium™ Patchによってパッチ配信が自動化されている場合は、エンドポイントごとにスキャンの最新の結果が返されます。詳細は、「Tanium Patchユーザガイド」を参照してください。

Endpoint Identityの要件

Endpoint Identityをインストールおよび使用するにあたっては要件を確認してください。

Taniumの依存関係

Endpoint Identity用のライセンスに加えて、ご使用の環境が以下の要件を満たしていることを確認します。

コンポーネント	要件
Tanium™ Core Platform	7.2以降
Taniumの製品	(オプション) • Tanium Comply 2.6以降 • Tanium Patch 3.0以降

エンドポイント

サポートされているオペレーティングシステム

Endpoint Identityでは、エンドポイントの以下のオペレーティングシステムに対応しています。

- Windows
- macOS
- Linux

Tanium Clientのオペレーティングシステムのサポートについては、以下を参照してください。Tanium Client Managementユーザガイド：クライアントのバージョンとホストシステムの要件。

サードパーティのソフトウェア

Endpoint Identityは、以下のサードパーティベンダとの統合をサポートしています。

- Cloudflare
- Google BeyondCorp

次の表は、各ベンダが提供する統合機能をまとめています。

アイデンティティプロバイダ	Platform統合	Patch統合	Comply統合
Cloudflare			
Google BeyondCorp			

ホストとネットワークセキュリティの要件

Endpoint Identityの実行には、特定のポートおよびプロセスが必要です。

ポート

Endpoint Identityの通信には、以下のポートが必要です。

コンポーネント	ポート	方向	目的
エンドポイント	17472	インバウンド/アウトバウンド	クライアント/サーバ通信

セキュリティの除外

未知のホストシステムプロセスを監視およびブロックするために環境でセキュリティソフトウェアが使用されている場合、セキュリティ管理者はTaniumプロセスが問題なく実行できるよう除外を作成する必要があります。

Endpoint Identityのセキュリティ除外

対象デバイス	プロセス
エンドポイント側(Windows)	*<Tanium Client>*\TaniumCX.exe
エンドポイント(macOS, Linux)	*<Tanium Client>*/TaniumCX

Endpoint Identityのインストール

[**Tanium Solutions (Taniumソリューション)**] ページを使用してEndpoint Identityをインストールします。

使用を開始する前に

- リリースノートをお読みください。
- Endpoint Identityの要件 (7ページ)を確認します。

Endpoint Identityをインポートする

1. メインメニューから **[Administration (運用管理)] > [Configuration (設定)] > [Solutions (ソリューション)]** に移動して、**[Content (コンテンツ)]** セクションまでスクロールします。
2. **[Endpoint Identity]** を選択し、**[Import Selected (選択をインポート)]** をクリックしてインポートを実行します。
   詳細については、Tanium Consoleユーザガイド：Taniumの共有サービスとコンテンツを管理します。

エンドポイントでEndpoint Identityを設定する

Taniumエンドポイントでendpoint Identityが設定されていると、IDプロバイダはエンドポイントにクエリを発行して情報を得ることができます。この情報は、IDプロバイダがエンドポイントとユーザに特権アプリケーションへのアクセスを許可するかどうかを決定するのに役立ちます。Endpoint Identityを設定するには、ツールパッケージと設定パッケージをエンドポイントに配布する必要があります。

> 次の手順では、アクションを使用して設定パッケージをエンドポイントに配布することができます。組織規模の展開では、スケジュール済みアクションを使用することで簡単に配布することができます。詳細は、「スケジュール済みアクションとアクション履歴の管理」を参照してください。

ツールのパッケージを配布する

Endpoint Identityツールのパッケージをエンドポイントに配布します。特定のオペレーティングシステムを対象とするQuestionを作成し、エンドポイントにアクションを展開します。アクションの展開についての詳細は、「Tanium Interactユーザガイド：アクションの展開」を参照してください。

1. Questionを実行して、オペレーティングシステム別に一連のエンドポイントを対象設定します。
    1. すべてのWindowsエンドポイントのQuestion例：`Get Is Windows from all machines`
    2. すべてのLinuxエンドポイントのQuestion例：`Get Is Linux from all machines`
    3. すべてのMacエンドポイントの例：`Get Is Mac from all machines`
2. 一連の対象エンドポイントにアクションを展開します。**[Deploy Action (アクションを展開)]**をクリックします。オペレーティングシステムに応じたパッケージを展開します。
    1. `Endpoint Identity - Tools [Windows]`
    2. `Endpoint Identity - Tools [Linux]`
    3. `Endpoint Identity - Tools [Mac]`

キーペアの生成

RSAキーペアの生成：

- クライアント/統合パートナー用のRSAキーペア1つ。公開キーは、設定パッケージでクライアントの公開キーとして使用されます。この項目については、サードパーティの統合ベンダに確認してください。ベンダからはファイルが提供されるか、キーペアを生成してエクスポートする方法が提供されます。このファイルは、`client-public.key`という名前である必要があります。
- Tanium Endpoint Identityソリューション用のRSAキーペア1つ。設定パッケージに`server-private.key`ファイルを含めます。`server-public.key`ファイルを統合ベンダに提供します。

OpenSSLを使用してTanium RSAキーペアを生成する

OpenSSLがインストールされている場合は、以下のコマンドを実行することができます。これらのコマンドは、使用しているライブラリでサポートされているキーによって異なる場合があることが注意してください。

```
openssl genpkey -out <<client-private.key>> -algorithm RSA -pkeyopt rsa_keygen_
bits:2048
```

```
openssl rsa -in <<client-private.key>> -outform PEM -pubout -out <<client-
public.key>>
```

```
openssl genpkey -out <<server-private.key>> -algorithm RSA -pkeyopt rsa_keygen_
bits:2048
```

```
openssl rsa -in <<server-private.key>> -outform PEM -pubout -out <<server-
public.key>>
```

サーバのキーペアを確認する

`server-private.key`と`server-public.key`のMD5ハッシュが一致していることを確認します。OpenSSLがインストールされている場合は、次のコマンドを実行できます。

```
openssl rsa -noout -modulus -in <<server-private.key>> | openssl md5
```

```
openssl rsa -noout -modulus -pubin -in <<server-public.key>> | openssl md5
```

設定パッケージを更新する

Endpoint Identity設定パッケージを更新して、ポートとキーペアの設定を含めることができます。

1. メインメニューで **[Administration (運用管理)] > [Content (コンテンツ)] > [Packages (パッケージ)]** をクリックします。
2. フィルタに`Endpoint Identity`と入力して、設定パッケージのリストを表示します。
    1. `Endpoint Identity - Configure Endpoint Identity [Windows]`
    2. `Endpoint Identity - Configure Endpoint Identity [Linux]`
    3. `Endpoint Identity - Configure Endpoint Identity [Mac]`
3. 更新するパッケージを選択し、**[Edit (編集)]** をクリックします。

4. パッケージを編集して、使用するキーとポートを設定します。パッケージの **[Files (ファイル)]** セクションで`config.json`ファイルをダウンロードします。ポートと発信元の許可リストを更新します。

    1. `httpPort`プロパティは、エンドポイントが認証プロバイダまたは承認プロバイダからの呼び出しを待機するポートです。デフォルトでは、この値は`8181`です。
    2. これらのファイルをパッケージにアップロードすると、`serverPrivateKey`と`clientPublicKey`プロパティは無視されます。`config.json`ファイルでこれらのプロパティを定義する場合、値は1行にする必要があり、区切りには`\n`を挿入します。
    3. `originAllowed`プロパティは、リクエストの発行を許可するドメインのコンマ区切りのリストです。このリストは、統合ベンダから入手します。このリストに空白スペースがあってはいけません。先頭にアスタリスク(`*`)を使用すると、すべてのサブドメインが許可されます。アスタリスクを値として単独で使用することはできません。

    更新後、`config.json`が有効であることを確認します。以下は例です。

    ```
    {"httpPort": 8181,
    "serverPrivateKey": "",
    "clientPublicKey": "",
    "originAllowed": "provider.com"
     }
    ```

5. 設定した`config.json`ファイルをパッケージにアップロードします。既存の`config.json`ファイルを削除し、**[Add (追加)] > [Local File (ローカルファイル)]** をクリックします。
6. 統合ベンダから提供されたクライアントの公開キーをパッケージに追加します。**[Add (追加)] > [Local File (ローカルファイル)]** をクリックします。このファイルの名前は、`client-public.key`である必要があります。このファイルをアップロードすると、`config.json`ファイルの`clientPublicKey`値より優先されます。
7. Tanium Endpoint Identity用に生成したサーバの秘密キーを追加します。**[Add (追加)] > [Local File (ローカルファイル)]** をクリックします。このファイルの名前は、`server-private.key`である必要があります。このファイルをアップロードすると、`config.json`ファイルの`serverPublicKey`値より優先されます。
8. パッケージを保存し、設定パッケージごとに手順を繰り返します。

設定パッケージを配布する

Endpoint Identity設定パッケージをエンドポイントに配布することができます。特定のオペレーティングシステムを対象とするQuestionを作成し、エンドポイントにアクションを展開します。アクションの展開についての詳細は、「Tanium Interactユーザガイド：アクションの展開」を参照してください。

1. Questionを実行して、オペレーティングシステム別に一連のエンドポイントを対象設定します。
    1. すべてのWindowsエンドポイントのQuestion例：`Get Is Windows from all machines`
    2. すべてのLinuxエンドポイントのQuestion例：`Get Is Linux from all machines`
    3. すべてのMacエンドポイントの例：`Get Is Mac from all machines`

2. 一連の対象エンドポイントにアクションを展開します。**[Deploy Action (アクションを展開)]** をクリックします。オペレーティング システムに応じたパッケージを展開します。

    1. `Endpoint Identity - Configure Endpoint Identity [Windows]`
    2. `Endpoint Identity - Configure Endpoint Identity [Linux]`
    3. `Endpoint Identity - Configure Endpoint Identity [Mac]`

Endpoint Identityツールのインストールを確認する

エンドポイントにインストールされたツールのステータスを確認するには、「`Get Endpoint Identity - Tools Version from all machines`」というQuestionを実行します。

次に取り組むこと

これでサードパーティのIDプロバイダは、Endpoint IdentityのAPIを使用して、Taniumが管理するエンドポイントに関する情報を取得できるようになりました。APIは、次の情報を提供します。

- エンドポイントにTanium Clientがインストールされている場合 - エンドポイントのプラットフォームと、エンドポイントがTanium Serverに最後に接続した日時。
- Tanium PatchのスキャンがWindowsエンドポイントで実行されている場合 - Windowsアップデートがエンドポイントに最後に正常に適用された日時。
- Tanium Complyの脆弱性スキャンがエンドポイントで実行されている場合 - APIは以下を提供します。
    - 重大度が「低」、「中」、「高」の脆弱性の数
    - 脆弱性スコアの最高値と平均値、中央値、最小値
    - 脆弱性の合計数
    - レポートの合計数
      Endpoint Identityは、利用可能なすべてのComplyレポートを利用します。

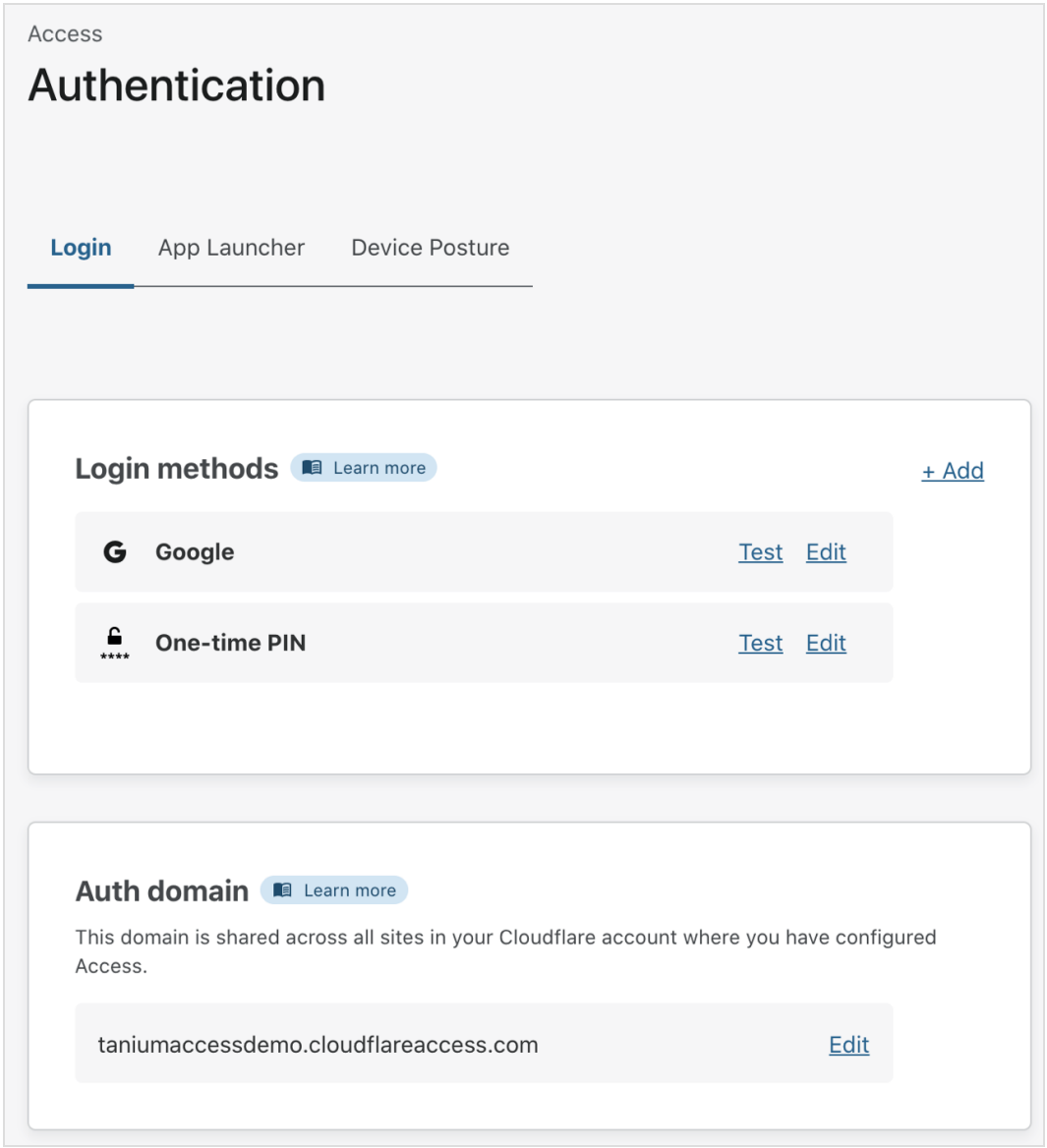
Endpoint Identityのトラブルシューティング

トラブルシューティング用に情報を収集してTaniumに送信するには、関連する情報を収集します。

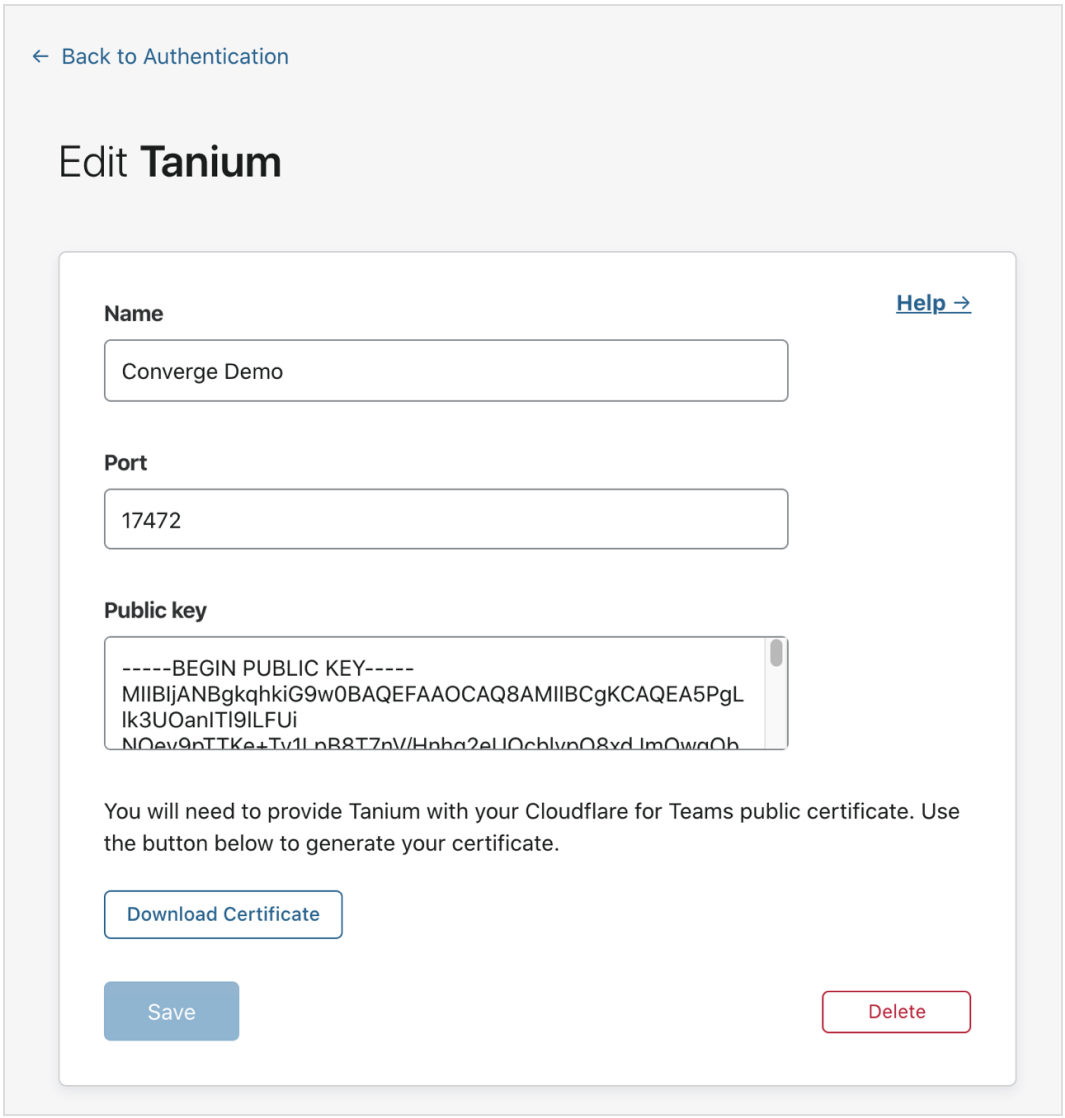
Cloudflare統合時の問題のトラブルシューティング

Cloudflare for Teamsで以下の項目が正しく設定されていることを確認します。

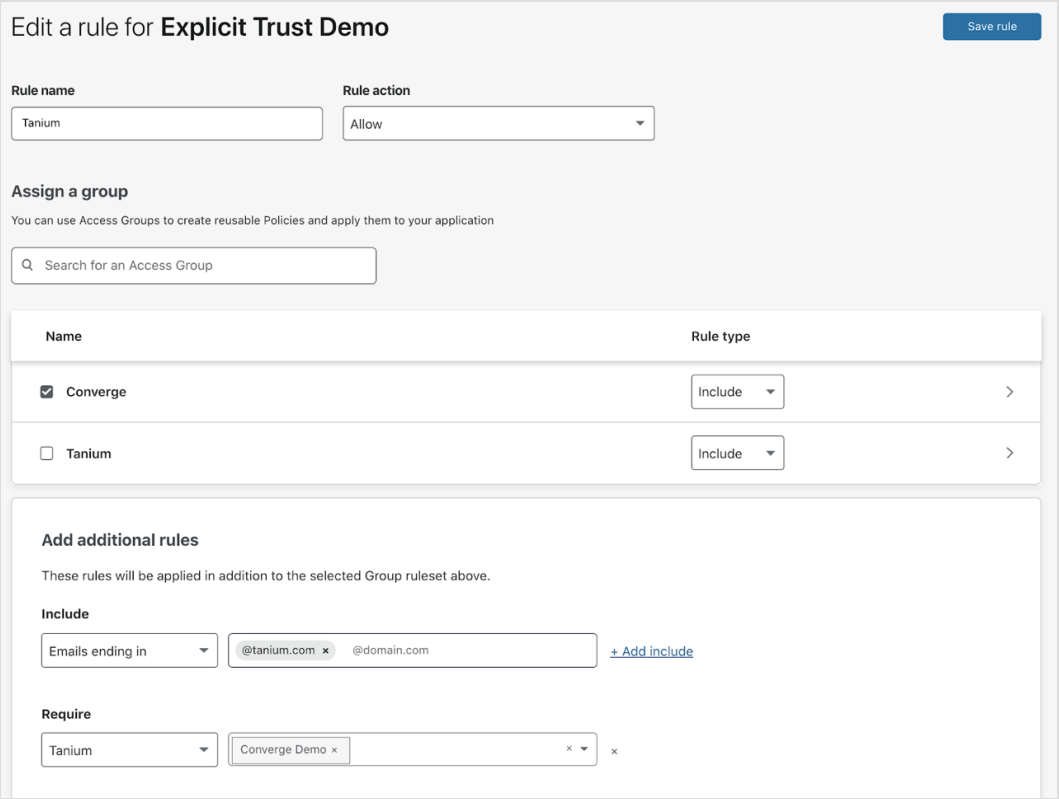
- Authentication domain (認証ドメイン). Cloudflare for Teamsで **[Access] > [Authentication] > [Login]** をクリックします。認証ドメインが`config.json`のドメインと一致していること、または`*.cloudflareaccess.com`を使用していることを確認します。



- Device posture。Cloudflare for Teamsで **[Access] > [Authentication] > [Device Posture]** をクリックします。Taniumエンドポイントno保護プロバイダの **[Edit (編集)]** をクリックします。以下を確認します。
    - **Port**が`config.json`に指定されているポート番号と一致している。
    - **Public key**が`server-public.key`である。
    - **[Download Certificate (証明書のダウンロード)]** をクリックしてダウンロードした証明書が`client-public.key`である。



- Application configuration。Cloudflare for Teamsで **[Access] > [Applications]** の順にクリックします。アプリケーションの **[Edit (編集)]** をクリックします。以下を確認します。
    - **[Rule Action]** は**Allow**に設定します。
    - **Include**ルールには、含めるユーザの種類(メールアドレスがtanium.comで終わるユーザなど)を指定します。
    - **Require**ルールには、**Tanium**とTaniumエンドポイントの保護プロバイダ名を指定します。



エンドポイントからEndpoint Identityのツールを削除する

エンドポイントEndpoint Identityのツールを削除するアクションを展開することができます。

1. Interactで、特定のオペレーティングシステムを対象設定するQuestionを実行します。たとえば、`Get Endpoint Identity - Tools Version from all machines with Is Windows equals True`などです。
2. 一連の対象エンドポイントにアクションを展開します。**[Deploy Action (アクションを展開)]** をクリックします。オペレーティングシステムに応じたパッケージを展開します。
    1. `Endpoint Identity - Remove Tools[Windows]`
    2. `Endpoint Identity - Remove Tools[Linux]`
    3. `Endpoint Identity - Remove Tools[Mac]`

3. (任意) データベースとログを含めてToolsフォルダからEndpoint Identityフォルダを削除するには、**[Remove saved data (保存済みデータの削除)]** を選択します。
4. **[Show Preview to Continue (プレビューを表示して続行)]**をクリックします。
5. ページ下部の結果グリッドに、アクション対象のエンドポイントが表示されます。結果に問題がなければ**[Deploy Action (アクションのデプロイ)]**をクリックします。

> エンドポイント設定を有効にしている場合、ツールがエンドポイントから削除されるには、エンドポイント設定でツールの削除が承認されている必要があります。

Taniumサポートに問い合わせる

Taniumサポートに問い合わせるには、https://support.tanium.comにサインインします。