

# クライアントとの接続

REST API クライアントを使用して REST API にアクセスできます。通常、REST API クライアントはブラウザのプラグインとして使用できますが、任意の REST API クライアントを使用できます。



- (注) REST API に初めて接続すると、証明書の警告が表示されます。REST API を使用するためには 証明書を受け入れる必要があります。
  - REST API クライアントからの認証 (1ページ)

# REST API クライアントからの認証

APIとのインターフェイスとユーザーインターフェイスには、異なるアカウントを使用することをお勧めします。資格情報は、両方のインターフェイスで同時には使用できません。同時使用すると警告なしにログアウトされます。

REST API に初めて接続する際は、無効な証明書により接続が安全ではないというエラーが表示される場合があります。証明書を使用して接続を許可するように、ブラウザに例外を追加します

トークンベース認証では、ユーザ名とパスワードを指定することによってトークンを取得します。要求ごとにユーザ名とパスワードを必要とせずに、限られた期間だけHTTPサービスにアクセスするには、このトークンを使用します。つまり、要求ごとにユーザ名とパスワードで認証しなくても済むように、ユーザ資格情報を一意に生成されたアクセストークンで置き換えます。これを使用すると最長30分間リソースにアクセスでき、3回まで更新できます。

次の図に、トークンベースの認証の概念を示します。

## **Token-Based Authentication REST Client REST API** HTTP GET Request Get Access Token (Username, Password) Authenticate User HTTP error Code 401 (unauthorized User) Generate Access and Refresh tokens HTTP 200 OK Access and Refresh tokens All HTTP actions Request for access to the Resource (Access token) Validate Access token HTTP error Code 401 (unauthorized User) Appropriate HTTP response Give access to Resource In case the access token expires HTTP POST Generate new Access token (Access and Refresh token) Validate Access and Refresh tokens HTTP error Code 401 (unauthorized User) Generate new Access and Refresh tokens HTTP 200 OK Return Access and Refresh token **REST Client REST API**

# 認証トークンの要求

トークン生成ユーティリティは、REST API クライアントで使用できる認証トークンを提供します。

#### 始める前に

設定済みの Management Center と、REST API を使用するための資格情報を持つアカウントが必要です。基本認証を実行できる REST API クライアントも必要です。

- ステップ1 REST API クライアントを開きます。
- ステップ2 https://<management\_center\_IP\_or\_name>/api/fmc\_platform/v1/auth/generatetokenのURLにPOST コマンドを行うようクライアントを設定します。
- ステップ3 ユーザー名とパスワードを基本認証ヘッダーとして含めます。POST本文は空白にする必要があります。

#### 次のタスク

APIへの要求に、ヘッダー X-auth-access-token:<authentication token value>を追加します。

REST API クライアントからの認証 (1 ページ) に記載されているように、要求にヘッダー X-auth-access-token:<authentication token value> および X-auth-refresh-token:<refresh token value> を追加して、トークンを更新します。

サーバーへのすべての REST 要求に認証トークンからの Domain UUID を使用します。

## 認証トークンの更新

Management Center REST API 認証トークンは 30 分間有効で、3 回まで更新することができます。

#### 始める前に

Management Center REST API から有効な認証と更新のトークンを取得します。これらのトークンの更新が3回未満であることを確認します。

- ステップ1 REST API クライアントを開きます。
- ステップ2 X-auth-access-token:<authentication token value> および X-auth-refresh-token:<refresh token value> ヘッダーを使用して、https://<management\_center\_IP\_or\_name>/api/fmc\_platform/v1/auth/refreshtoken の URL に POST コマンドを行うようクライアントを設定します。

#### 次のタスク

API への要求に、ヘッダー X-auth-access-token:<new authentication token value> を追加します。

要求に、ヘッダー x-auth-refresh-token:<new refresh token value> を追加して、トークンを 更新します。 認証トークンの更新

### 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。