McAfee Client Proxy 4.3.x 製品ガイド

Trellix

目次

製品概要

概要

McAfee® Client Proxy ソフトウェアを使用すると、ネットワークの内外から Web にアクセスした時に発生するセキュリティ脅威から、エンドポイントのユーザーを保護できます。

このクライアント ソフトウェアは、Microsoft Windows または macOS を実行しているエンドポイントにインストールされ、フィルタリングのために、Web リクエストをリダイレクトするか、プロキシへの送信を許可します。 サーバー ソフトウェアは、McAfee ePO、McAfee ePO Cloud、MVISION ePO の 3 つの管理プラットフォームのいずれかで実行します。

Web Protection ハイブリッド ソリューション

Client Proxy は、McAfee® Web Protection ハイブリッド ソリューションに必須のコンポーネントです。 このソリューションでは、McAfee® Web Gateway により提供されるネットワークベースのセキュリティ機能と、McAfee® Web Gateway Cloud Service (McAfee® WGCS) により提供されるクラウドベースのセキュリティ機能を統合することができます。

Client Proxy ソフトウェアは、エンドポイントの場所に応じて Web トラフィックを許可またはリダイレクトします。

- ネットワーク内にあるエンドポイントまたは **VPN** 経由で接続されているエンドポイント – トラフィックはフィルタリングのために、ネットワークに設置された Web Gateway アプライアンスへの送信を許可されます。
- ネットワーク外にあるエンドポイント – トラフィックは、フィルタリングのために McAfee WGCS にリダイレクトされます。

Endpoint Security との統合

エンドポイントで McAfee® Endpoint Security と共に Client Proxy を配備する場合、各製品は McAfee® ePolicy Orchestrator® (McAfee® ePO™) 、McAfee ePO Cloud、または MVISION ePO を使用して個別にインストールし管理します。

- Client Proxy 管理者 – 通常どおりにポリシーを設定し、タスクを実行します。
- Endpoint Security 管理者 – Client Proxy がインストールされていて Web トラフィックをアクティブにリダイレクトしている場合に McAfee® Endpoint Security Web 管理が無効になるように設定するオプションがあります。

Windows を実行しているエンドポイントでは、[スタート] メニューから [About McAfee Client Proxy] (McAfee Client Proxy について) ウィンドウを開くと、Client Proxy がエンドポイントにインストールされ実行されていて、トラフィックをアクティブにリダイレクトしているかどうかが確認できます。

主な機能

Client Proxy は、設定したポリシーに基づいて、ユーザーからの Web リクエストを許可またはリダイレクトします。

- トラフィックのリダイレクト – ソフトウェアは、Client Proxy ポリシーの設定に従い、フィルタリングのために Web トラフィックをプロキシ サーバーにリダイレクトします。
- 位置認識 – 位置認識の設定を使用すると、ネットワーク内またはネットワーク外で作業を行うユーザーや、VPN 経由でネットワークに接続するユーザーを、1 つのポリシーで扱うことができます。

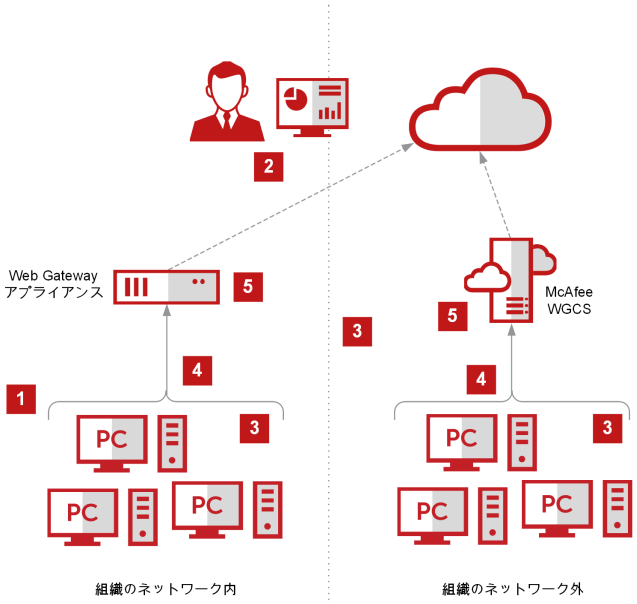
- 集中管理 – McAfee ePO、McAfee ePO Cloud、または MVISION ePO でソフトウェアを管理します。
- ブラウザーに対して独立 – プロキシ サーバーの設定は、エンドポイントで実行しているブラウザーではなく Client Proxy で設定されます。
- 透過的な認証 – Client Proxy は、認証情報の入力を必要とせずにユーザーを認証し、グループ メンバーシップやその他の情報をメタデータに渡して、それを HTTP/HTTPS リクエストに追加します。
- 耐タンパー性 – ユーザーは、一時的な解放コードを管理者に要求して受信しない限り、エンドポイントから Client Proxy ソフトウェアを削除できません。
- **Secure Channel** (セキュア チャネル) – ソフトウェアはすべての HTTP/HTTPS 要求に対して Client Proxy と McAfee WGCS の間のセキュアな通信チャネルを確立します。 これは、クラウド プロキシにのみ適用されます。

機能

Client Proxy ソフトウェアは、Client Proxy ポリシーとエンドポイントの場所に応じて、Web トラフィックをリダイレクト、ブロック、または許可します。

Client Proxy のワークフロー

1. Client Proxy ソフトウェアは、組織内のエンドポイントにインストールされます。
2. McAfee ePO、McAfee ePO Cloud、または MVISION ePO を使用して、管理者は Client Proxy ポリシーを作成し、すべての管理対象エンドポイントにポリシーを割り当てます。
3. 管理対象エンドポイントは、組織のネットワーク内に配置することも、VPN 経由でネットワークに接続することも、ネットワークの外部に配置することもできます。
4. エンドポイントで作業しているユーザーは、Web リソースへのアクセスを要求します。
5. ソフトウェアはユーザーの場所を特定し、Web リクエストを許可またはリダイレクトします。
   - ネットワーク内または VPN 経由で接続されている場合 – Web リクエストは、ネットワークに設置された Web Gateway アプライアンスへの送信を許可されます。Web リクエストはそこでフィルタリングされます。 Client Proxy はパッシブです。
   - ネットワークの外部の場合 – Web リクエストは McAfee WGCS にリダイレクトされ、そこでフィルタリングされます。 Client Proxy はアクティブです。


2
Web Gateway
アプライアンス
5
3
5
McAfee
WGCS
4
1
4
3
3
PC
PC
PC
PC
PC
PC
組織のネットワーク内
組織のネットワーク外

Client Proxy ポリシーの管理

Client Proxy メタデータ

Client Proxy ソフトウェアは、HTTP/HTTPS トラフィックをリダイレクトする際に、メタデータをリクエストに追加します。

Web Gateway や McAfee WGCS などの他の製品は、Web 保護ポリシーを適用する時にこのメタデータ (グループ メンバーシップなど) を使用します。

- 認証トークン – Web リクエストを作成したユーザーに関する識別情報を含むトークン
- 認証バージョン – Client Proxy が共有しているメタデータのバージョン
- クライアント IP アドレス – トラフィックが発信されたエンドポイントの IP アドレス
- 元の宛先 IP アドレス – トラフィックの送信先サーバーの保存された IP アドレス
- 顧客 ID – 顧客の組織を一意に識別します
- ユーザー ID – Web リクエストを作成したユーザーを一意に識別します
- ユーザー グループ – ユーザーがメンバーになっているグループの名前
- テナント ID – クラスター内のノードで共有される ID (McAfee ePO Cloud または MVISION ePO)
- プロセス名 – トラフィックを生成するプロセスの名前
- プロセスの実行パス – トラフィックを生成するプロセスのパス
- システム情報 – ホスト オペレーティング システム名 (Windows、Mac)、ローカル時間 (1/1/1970 からの秒数)、MAC アドレス、プロセスの稼働時間、システム名、mcp ポリシー名などのシステム情報

権限セット (McAfee ePO)

ユーザー権限

ユーザー権限を管理するには、McAfee ePO インターフェースで権限セットを設定します。役割ごとに 1 つの権限セットを設定します。

UI には、事前に定義された編集可能な役割と権限セットが用意されています。 役割を追加し、それに権限セットを設定することもできます。

管理者ユーザー

事前に定義された役割の 1 つである [MCP Catalog Admin] (MCP カタログ管理者) には、Client Proxy ポリシーの作成、削除、管理に必要なすべての権限が割り当てられています。 次の操作を行うための Client Proxy 管理者権限を割り当てるには、完全な権限セットが必要です。

- ポリシーを作成、削除、および管理する
- ポリシーをエンドポイントにプッシュする
- クエリーを表示する
- Client Proxy 拡張ファイル ソフトウェアを管理する

- マスター リポジトリの機能を実行する
- Help Desk の機能を実行する

McAfee ePO 管理者のみが、次の権限を含む、拡張ファイル ソフトウェアの管理権限を持っています。

- McAfee ePO サーバーに拡張ファイルをインストールする
- McAfee ePO サーバーから拡張ファイルを削除する
- McAfee ePO サーバーにインストールされた拡張ファイルを更新する

権限セットを設定する

既存の役割の権限セットを更新したり、新しい役割に権限セットを設定したりできます。

始める前に

管理者として McAfee ePO サーバーにログオンする必要があります。

タスク

1. McAfee ePO メニューで、[ユーザー管理] → [権限セット] の順に選択します。
2. [権限セット] で役割を選択します。
3. 設定ペインで、[編集] をクリックしていずれかの権限セットを開きます。
4. 権限セットの設定を更新して、[保存] をクリックします。

Client Proxy の管理に必要な権限

Client Proxy を管理するには、特定の権限が必要です。

Client Proxy 管理者の権限

権限	設定	権限を必要とする操作...
[エージェント ハンドラー]	[エージェント ハンドラーを表示] を選択します	· ポリシーをエンドポイントにプッシュする · クエリーを表示する
[クライアント イベント]	[クライアント イベントを表示] を選択します	· ポリシーをエンドポイントにプッシュする · クエリーを表示する

権限	設定	権限を必要とする操作...
[Common Catalog]	[カタログ権限テンプレート] を選択後、次のすべての Common Catalog アクションを選択します。 ・ **[カタログの作成、名前の変更、複製]** ・ **[カタログの削除]** ・ **[他のカタログからのカタログ項目のインポート]** ・ **[ファイルからのカタログ項目のインポート]** ・ **[ファイルへのカタログ項目のエクスポート]**	ポリシーを作成、削除、および管理する
[Help Desk アクション]	次のすべての Client Proxy アクションを選択します。 ・ **[クライアント アンインストール キーを生成する]** ・ **[バイパス クライアント キーを生成する]** ・ **[上のキーにマスター応答キーを生成する]**	Help Desk の機能を実行する **Note:** McAfee ePO 管理者にはデフォルトですべての Help Desk 権限が割り当てられています。 この権限を他の管理者に割り当てるには、まず Help Desk 拡張ファイルをインストールする必要があります。
[McAfee Agent]	・ **[McAfee Agent: ポリシー]** – **[設定を表示して変更]** を選択します ・ **[McAfee Agent: タスク]** – **[設定を表示して変更]** を選択します	・ ポリシーをエンドポイントにプッシュする ・ クエリーを表示する
[MCP ポリシー]	[ポリシーとタスクの設定を表示して変更] を選択します	ポリシーを作成、削除、および管理する
[クエリーとレポート]	[公開グループの編集、プライベート クエリーとレポートの作成と編集、プライベート クエリーとレポートの公開] を選択します	・ ポリシーをエンドポイントにプッシュする ・ クエリーを表示する
[ソフトウェア]	[マスター リポジトリ] – [パッケージの追加、削除、または変更; プル タスクの実行] を選択します [分散リポジトリ] – [リポジトリの追加、削除、または変更; 複製タスクの実行] を選択します	次のマスター リポジトリの機能を実行する ・ ソフトウェア パッケージを追加する ・ ソフトウェア パッケージを削除する

権限	設定	権限を必要とする操作...
		・ チェックインされたパッケージを更新する
[システム]	[システム ツリー] – [[システム ツリー] タブの表示] を選択します [アクション] – 次を選択します。 ・ **[エージェント ウェークアップ、エージェント アクティビティ ログの表示]** ・ **[システム ツリー グループとシステムを編集]** ・ **[エージェントの配備]** [タグの使用] – [タグの適用、除外、消去] を選択します [タグ カタログ] – [タグ、タグ グループ、タグ条件の作成および編集] を選択します	・ ポリシーをエンドポイントにプッシュする ・ クエリーを表示する
[システム ツリーへのアクセス]	[ユーザーの組織] を選択します	・ ポリシーをエンドポイントにプッシュする ・ クエリーを表示する

ポリシーの確認と承認

McAfee ePO インターフェースで Client Proxy ポリシーの確認と承認を設定できます。

設定作業では、権限セットの作成とユーザーへの割り当て、および [サーバー設定] ページでの承認の設定を行います。

1. ポリシー管理の権限セットを作成します。
   - ポリシー ユーザーの権限セット – ポリシー ユーザーは、ポリシーを作成、編集する権限を持っています。変更したら、確認のために送信する必要があります。
   - ポリシー管理者の権限セット – ポリシー管理者は、新しいポリシーまたは変更されたポリシーを承認して保存するか、変更を拒否する権限を持っています。
2. ポリシー管理ユーザーを作成します。
   - ポリシー ユーザー – このユーザーを作成したら、ポリシー ユーザーの権限セットを割り当てます。
   - ポリシー管理者 – このユーザーを作成したら、ポリシー管理者の権限セットを割り当てます。
3. **[サーバー設定]** ページの **[承認]** ペインで、ポリシー変更の承認に関する設定を行います。
   - ポリシー ユーザー – 確認のためにユーザーにポリシー変更の送信を要求する場合には、**[ユーザーはポリシーの変更に対して承認を得る必要があります]** を選択します。

- ポリシー管理者 – ポリシー管理者にも確認のためにポリシー変更の送信を要求する場合には、[管理者/承認者はポリシーの変更に対して承認を得る必要があります] を選択します。

詳細については、『McAfee ePolicy Orchestrator 製品ガイド』を参照してください。

共有パスワードの使用方法

共有パスワードは、Client Proxy と、Web Gateway または McAfee WGCS 間の通信を保護するパスワードです。 共有パスワードは共有秘密鍵と呼ばれることもあります。

Client Proxy がオンプレミス、クラウドのみ、またはハイブリッドのいずれの配備で設定されていても、1 つの共有パスワードにより、製品およびポリシー間の通信が保護されます。 設定の詳細は、管理プラットフォームによって異なります。

McAfee ePO の管理対象の場合

1. 顧客 ID と共有パスワードを Web Gateway サーバーから .xml ファイルにダウンロードします。
2. McAfee ePO インターフェースで、Client Proxy ポリシーの設定時に、[クライアントの設定] ページで .xml ファイルから認証情報をインポートします。

McAfee ePO Cloud の管理対象の場合

1. McAfee ePO Cloud インターフェースで、Client Proxy ポリシーの設定時に、[クライアントの設定] ページで共有パスワードを設定します。
2. 認証情報を手動で共有するには、顧客 ID と共有パスワードを .xml ファイルにエクスポートします。

MVISION ePO の管理対象の場合

1. 顧客 ID と共有パスワードを Web Gateway サーバーから .xml ファイルにダウンロードします。
2. MVISION ePO インターフェースの [MCP 管理] ページで、.xml ファイルの認証情報をインポートします。

ハイブリッド配備の場合

1. McAfee ePO Cloud インターフェースで、共有パスワードを設定し、認証情報を .xml ファイルにエクスポートします。
2. McAfee ePO インターフェースで、.xml ファイルから認証情報をインポートします。

共有パスワードを変更する場合の注意事項 (McAfee ePO Cloud)

McAfee ePO Cloud インターフェースで共有パスワードを変更する場合には、システムでの更新時間に余裕を持たせてください。

共有パスワードの更新には、次のようなシステム アクションと時間が必要です。

1. McAfee ePO Cloud は、更新された Client Proxy ポリシーを組織内のエンドポイントに配備します。 このアクションの所要時間は、McAfee Agent ポリシーの [ポリシーの施行間隔] 設定に指定された値により変わります。
2. エンドポイントの Client Proxy ソフトウェアは、新しいパスワードを McAfee WGCS と共有します。 このアクションには最大で 20 分かかります。

Caution

共有パスワードは McAfee WGCS で同期する必要があります。同期しない場合、認証が失敗します。

顧客 ID と共有パスワードをインポートする (MVISION ePO)

Client Proxy ポリシーを MVISION ePO で作成する場合、または Client Proxy ポリシーをオンプレミスから MVISION ePO に移行する場合、顧客 ID と共有パスワードを Web Gateway サーバーから .xml ファイルにダウンロードし、そのファイルを [MCP 管理] ページでインポートします。

Note

オンプレミスから MVISION ePO への Client Proxy ポリシーの移行は、Client Proxy オンプレミス 3.0.0 以降でサポートされています。 McAfee ePO オンプレミスから MVISION ePO への移行方法については、McAfee 製品マニュアル ポータル *(docs.mcafee.com)* の *MVISION ePO* への移行クイック スタート ガイド を参照してください。

タスク

1. MVISION ePO メニューで、[設定] → [MCP 管理] の順に選択します。
2. [顧客 ID] の隣にある [ファイルの選択] をクリックします。 .xml ファイルが含まれるフォルダーに移動して選択し、[開く] をクリックします。

タスクの結果

顧客 ID と共有パスワードが Client Proxy にインポートされます。 既存のポリシーと新しいポリシーすべてが、インポートされた顧客 ID と共有パスワードで更新されます。

Common Catalog インスタンスを作成する (McAfee ePO または McAfee ePO Cloud)

Common Catalog に Client Proxy インスタンスを作成できます。これは、ポリシーにバイパス リストを設定する場合に選択します。

始める前に

管理者として McAfee ePO または McAfee ePO Cloud サーバーにログオンする必要があります。

Client Proxy カタログ インスタンスはグローバルに使用できます。 各インスタンスは複数のポリシーに関連付けることができます。

Client Proxy カタログは、次のカテゴリまたは種類でグループ化された項目のリストで構成されています。

- ドメイン名
- ネットワーク アドレス
- ネットワーク ポート
- プロセス名

[Common Catalog] ページで、カタログ インスタンスを作成して設定できます。 各カテゴリの項目のリストを表示したり、リストで項目を追加、編集、削除したりできます。 カタログ インスタンスに必要な数だけリストを追加します。

タスク

1. McAfee ePO または McAfee ePO Cloud メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [カタログ リスト] ページの [アクション] ドロップダウン リストで、[新しいカタログ] を選択します。
3. 新しいカタログの名前と説明 (オプション) を指定して、[OK] をクリックします。
4. [Common Catalog] ペインの [ソース/宛先] で、次のカテゴリから選択します。

   - **[ドメイン名]** – このリストのドメインに送信された Web トラフィックが、プロキシ サーバーをバイパスします。 例: google.com
   - **[ネットワーク アドレス (IP)]** – このリストの IP アドレスに送信された Web トラフィックが、プロキシ サーバーをバイパスします。 アドレスは、個別に設定することも、範囲で設定することも、サブネットを使用することもできます。
     以下に例を示します。

     - 192.168.1.1
     - 172.31.255.10-172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17

   - **[ネットワーク ポート]** – このリストのポートに送信された Web トラフィックが、プロキシ サーバーをバイパスします。
     例: 40, 80, 400-500
   - **[プロセス名のリスト]** – このリストのプロセスから送信された Web トラフィックが、プロキシ サーバーをバイパスします。 エンドポイントではプロセスが実行されます。 Windows のプロセス名は .exe で終わる必要があります。 macOS のプロセス名には、ファイル名の拡張子は必要ありません。 McAfee のプロセスや信頼される他のプロセスをこのリストに追加します。

5. [アクション] ドロップダウン リストで、[新規] を選択します。
6. リストに一意の名前を指定するか、デフォルト名を使用します。
7. [追加] をクリックしてリストに項目を追加し、[保存] をクリックします。
   リストが Common Catalog に追加されます。

タスクの結果

Common Catalog インスタンスが設定され、保存されます。

ポリシーを設定する

Client Proxy ポリシーを作成する

Client Proxy ポリシーは、プロキシ サーバー リスト、リダイレクト設定、バイパス リスト、ブロック リストから構成され、これらにより、Client Proxy が Web リクエストをリダイレクトするかどうかとリダイレクト先が決定されます。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

既存のポリシーをテンプレートとして使用して新しいポリシーを作成できます。 テンプレートとして、デフォルト ポリシーは読み取り専用で、名前の変更、削除、エクスポート、インポート、またはエンドポイントへの割り当てはできません。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [新規ポリシー] をクリックします。
4. [既存のポリシーからポリシーを作成] ドロップダウン リストで、新規ポリシーのテンプレートとして使用する既存のポリシーを選択します。
5. 新しいポリシーの名前を指定した後、[OK] をクリックして保存します。

   Note

   Big Sur 11.2 以降で最初のポリシーを設定する際、McAfeeSystemExtensions ネットワーク アダプターを許可するようアラートで指示されます。 [許可] をクリックして McAfeeSystemExtensions を読み込みます。 許可を選択するまで、Client Proxy はトラフィックをリダイレクトしません。 同意確認のウィンドウをもう一度表示するには、Client Proxy を手動で再起動する必要があります。 詳細については、McAfee Knowledge Base の記事 KB94092 を参照してください。

タスクの結果

新しいポリシーを今すぐ設定するか、設定をキャンセルして、後ほど [ポリシー カタログ] からポリシーを選択して編集できます。

Client Proxy でのプロキシ サーバー リストの管理方法

Client Proxy ソフトウェアは、順序付けされたプロキシ サーバーのリストを管理します。

応答時間が最も速いプロキシ サーバーがリストの先頭に配置されます。 ソフトウェアは、リストを随時更新します。

たとえば、ユーザーがコンピューターを起動した時や、Client Proxy ポリシーが変更された時にリストが更新されます。 VPN 接続が切断されたり、プロキシ サーバーが応答に失敗したりした場合にも更新されます。 ソフトウェアは、これらのタイミングですべてのプロキシ サーバーとの接続をテストし、応答時間に基づいてリストの順序を変更します。

リストの先頭にあるプロキシ サーバーへのリダイレクトが失敗すると、ソフトウェアはリストの 2 番目のプロキシ サーバーにリダイレクトを試みます。 同時に、プロキシ サーバーとの接続を再度テストし、リストを更新します。

Client Proxy ソフトウェアが次のプロキシ サーバーをリストから選択する方法を設定する際には、次のオプションが使用できます。

.

[下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] – ソフトウェアは、設定したリストから次のプロキシ サーバーを選択します。

.

[最も応答時間の短いプロキシ サーバーに接続する] – ソフトウェアは、自身が管理するリストから、次のプロキシ サーバーを選択します。このリストは応答時間に基づいています。

自動プロキシ切り替え

このオプションを有効にすると、ソフトウェアは指定した間隔でプロキシ サーバー リストを確認します。 より優先度の高いプロキシ サーバーが使用可能な場合には、ソフトウェアが自動的にそのサーバーに切り替えます。

自動プロキシ切り替えオプションは、[下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] が選択されている場合のみ有効です。

プロキシ サーバー リストを設定する

Web トラフィックをプロキシ サーバーにリダイレクトするには、プロキシ サーバー リストとルールを設定します。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

プロキシ サーバー リストを設定する際には、Client Proxy、McAfee ePO、または McAfee ePO Cloud に MVISION ePO が配備されているかどうかを考慮します。

- オンプレミス – ネットワークに設置されている 1 つ以上の Web Gateway アプライアンスをプロキシ サーバーとして設定します。
- クラウド内 – McAfee WGCS をプロキシ サーバーとして設定します。ホスト名には c<顧客 ID>.saasprotection.com の形式を使用します。

例: c12345678.saasprotection.com

Note

ポリシーを保存する前に、1 つ以上のプロキシ サーバーの IP アドレスまたはホスト名、およびポート番号を入力する必要があります。

Note

プロキシ サーバー リストに少なくとも 1 つのクラウド プロキシが設定されている状態で [Secure Channel] (セキュア チャネル) 設定を有効にすると、Client Proxy はオンプレミス プロキシ サーバーを無視し、リスト内のクラウド プロキシ サーバーのみを考慮します。 クラウド プロキシ サーバーとポートの可用性に応じて、Client Proxy はリダイレクト、ブロック、またはフォールバック (セキュア チャネルなしで接続を許可) オプションを適用します。 c*******.wgcs.mcafee-cloud.com や c*******.saasprotection.com などのドメインを持つプロキシは、クラウド プロキシと見なされます。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy 設定] メニューで、[プロキシ サーバー] を選択します。
6. ソフトウェアがリストからプロキシ サーバーを選択する方法を指定するには、次のいずれかのオプションを選択します。

   ·

   [下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] – ソフトウェアは、設定したリストから次のプロキシ サーバーを選択します。

   ·

   [最も応答時間の短いプロキシ サーバーに接続する] – ソフトウェアは、自身が管理するリストから、次のプロキシ サーバーを選択します。このリストは応答時間に基づいています。

7. プロキシ サーバーを [プロキシ サーバー リスト] に追加するには、次の設定を行い、[追加] をクリックします。
   - **[プロキシ サーバーのアドレス]** – プロキシ サーバーの IP アドレスまたはホスト名を指定します。
   - **[プロキシ ポート]** – プロキシ サーバーのポート番号を指定します。
   - **[HTTP/HTTPS]** – このチェックボックスをオンにすると、ポート 80 と 443 に送信されたトラフィックがプロキシ サーバーにリダイレクトされます。
   - **[非 HTTP/HTTPS にリダイレクトされたポート]** – HTTP/HTTPS 以外でトラフィックをリダイレクトするプロトコルのポート番号を指定します。 プロキシ サーバーがそのプロトコルに対応していることを確認してください。 このフィールドには、最大で 1024 文字まで入力できます。
8. [Enable Auto proxy switch over] (自動プロキシ切り替えを有効にする) を選択した後、[ポーリング間隔] に 10 ～ 3600 秒の範囲で値を指定します。 推奨値は 60 秒です。

   自動プロキシ切り替えオプションは、[下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] が選択されている場合のみ有効です。

   Note

   [Secure Channel] (セキュア チャネル) 機能を使用する場合、[自動プロキシ切り替えを有効にします] 設定はプロキシ サーバー リストには適用されません。

9. [HTTP/HTTPS トラフィックとしてリダイレクトするように設定する追加のポートを指定します] フィールドで、HTTP/HTTPS トラフィックと同様にリダイレクトするトラフィックの他のポート番号を指定します。 たとえば、アプリケーションに送信されるトラフィックをリダイレクトできます。 このフィールドには、最大で 1024 文字まで入力できます。
10. 必要に応じて、[接続可能なプロキシ サーバーがない場合は設定したポートのトラフィックをブロックする] を選択します。
    設定したどのプロキシ サーバーにも接続できない場合、設定済みのポートと、デフォルトのポート 80 および 443 へのすべてのトラフィックがブロックされます。

11. [MCP が準備完了になるまで設定したポートのトラフィックをブロックする] を選択し、Client Proxy が起動中の間、エンドポイントを保護します。
    ユーザーがインターネットにアクセスしてから、Client Proxy がバイパス モードを終了してトラフィックのリダイレクトを開始するまで、設定したポートと、デフォルトのポート 80 および 443 へのすべてのトラフィックがブロックされます。
12. [設定したポートで IPv6 トラフィックをブロックする] を選択し、IPv4 にフォールバックするよう Web ブラウザーに要求します。
13. [プライマリ プロキシとの相互認証に失敗した場合にトラフィックをブロックする] を選択し、Client Proxy がプロキシ サーバーを認証できるときにそれのみが Web リクエストをリダイレクトするようにします。
14. [ローカル アドレスのプロキシ サーバーはバイパスする] の選択を解除し、組織のネットワーク内のローカル アドレスに送信されるトラフィックを含むすべてのトラフィックを、プロキシ サーバーにリダイレクトします。 IP アドレス、IP アドレス範囲、サブネット、または CIDR を設定できます。 たとえば、192.168.1.1、172.31.255.10-172.31.255.20、10.50.0.0/255.255.128.0、または 10.50.0.0/17 と設定します。
15. [IPv4 と IPv6 のポート 80/443 で UDP トラフィックをブロックする] を選択し、このトラフィックをブロックします。
16. [保存] をクリックします。

タスクの結果

プロキシ サーバー リストがポリシーと共に保存されます。

代替プロキシ サーバー リストを設定する

代替プロキシ サーバーを設定して、選択した Web トラフィックを複数のプロキシ サーバーに分割できます。 代替プロキシ サーバーがダウンしており、プライマリのプロキシ サーバーが使用できる場合、Client Proxy はトラフィックをプライマリにリダイレクトします。 プライマリのプロキシ サーバーがダウンしている場合、Client Proxy は、代替リダイレクトに設定しているトラフィックを代替プロキシ サーバーにリダイレクトします。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

プロキシ サーバー リストを設定する際には、Client Proxy、McAfee ePO、または McAfee ePO Cloud に MVISION ePO が配備されているかどうかを考慮します。

- オンプレミス – ネットワークに設置されている 1 つ以上の Web Gateway アプライアンスをプロキシ サーバーとして設定します。
- クラウド内 – McAfee WGCS をプロキシ サーバーとして設定します。ホスト名には c<顧客 ID>.saasprotection.com の形式を使用します。

例: c12345678.saasprotection.com

Note

ポリシーを保存する前に、1 つ以上のプロキシ サーバーの IP アドレスまたはホスト名、およびポート番号を入力する必要があります。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy 設定] メニューで、[プロキシ サーバー] を選択します。
6. [代替プロキシ サーバー リスト] タブをクリックします。
7. ソフトウェアがリストからプロキシ サーバーを選択する方法を指定するには、次のいずれかのオプションを選択します。

   ・

   [下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] – ソフトウェアは、設定したリストから次のプロキシ サーバーを選択します。

   ・

   [最も応答時間の短いプロキシ サーバーに接続する] – ソフトウェアは、自身が管理するリストから、次のプロキシ サーバーを選択します。このリストは応答時間に基づいています。

8. プロキシ サーバーを [プロキシ サーバー リスト] に追加するには、次の設定を行い、[追加] をクリックします。
   - **[プロキシ サーバーのアドレス]** – プロキシ サーバーの IP アドレスまたはホスト名を指定します。
   - **[プロキシ ポート]** – プロキシ サーバーのポート番号を指定します。
   - **[HTTP/HTTPS]** – このチェックボックスをオンにすると、ポート 80 と 443 に送信されたトラフィックがプロキシ サーバーにリダイレクトされます。
   - **[非 HTTP/HTTPS にリダイレクトされたポート]** – HTTP/HTTPS 以外でトラフィックをリダイレクトするプロトコルのポート番号を指定します。 プロキシ サーバーがそのプロトコルに対応していることを確認してください。 このフィールドには、最大で 1024 文字まで入力できます。
9. [代替プロキシで自動プロキシ切り替えを有効にします] を選択した後、[ポーリング間隔 (秒)] に 10 ～ 3600 秒の範囲で値を指定します。 推奨値は 60 秒です。

   自動プロキシ切り替えオプションは、[下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] が選択されている場合のみ有効です。

10. [保存] をクリックします。

タスクの結果

代替プロキシ サーバー リストがポリシーと共に保存されます。

クライアントを設定する

エンドポイントの場所と、Web トラフィックをいつリダイレクトするかを決定するために Client Proxy が使用する設定を行います。クライアント ソフトウェアは、TCP 3 ウェイ ハンドシェイクを使って接続をテストし、その後、接続を閉じます。エンドポイントは、ネットワークの内側または外側に配置でき、また VPN 経由でネットワークに接続することもできます。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

Note

ポリシーを保存する前に、顧客 ID と共有パスワードの値を入力する必要があります。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy 設定] リストで [クライアントの設定] を選択します。
6. お使いの管理プラットフォームに応じて、次のいずれかの設定を行います。

   - McAfee ePO – **[顧客 ID]** セクションで **[参照]** をクリックし、Web Gateway または McAfee WGCS 管理者により提供された顧客 ID の .xml ファイルを探して開きます。このファイルの値が、**[固有の顧客 ID]** フィールドと **[共有パスワード]** フィールドに自動的に入力されます。
   - McAfee ePO Cloud – **[共有パスワードを設定]** セクションで、Client Proxy が McAfee WGCS と共有するパスワードを入力し、確認用に再度入力します。パスワードをリセットまたはエクスポートするオプションもあります。
   - MVISION ePO – Client Proxy ポリシーを MVISION ePO で作成する前に、またはポリシーを MVISION ePO に移行する前に、**[MCP 管理]** ページで顧客 ID と共有パスワードをインポートします。正常にインポートできると、Client Proxy の既存のポリシーと新しいポリシーすべてが、インポートされた顧客 ID と共有パスワードで更新されます。

   Note

   オンプレミスから MVISION ePO への Client Proxy ポリシーの移行は、Client Proxy オンプレミス 3.0.0 以降でサポートされています。McAfee ePO オンプレミスから MVISION ePO への移行方法については、McAfee 製品マニュアル ポータル *(docs.mcafee.com)* の *MVISION ePO* への移行クイック スタート ガイド を参照してください。

7. [クラウド プロキシ用のセキュア チャネル] 設定を選択します。

   Note

   このオプションは McAfee WGCS にのみ適用されます。

   - **[セキュア チャネルを有効にする]** – Client Proxy と McAfee WGCS の間のセキュア接続を確立するには、このチェックボックスを選択します。このチェックボックスを選択すると、ソフトウェアはデバイス証明書ストアに照合してクラウド プロキシ証明書を検証し、セキュア接続を確立します。

Note

[Secure Channel] (セキュア チャネル) を有効にすると、Client Proxy は 8081 ポートを使用してクラウド プロキシ接続を確認します。ただし、クラウド プロキシ サーバーを追加する場合は、引き続き 8080 ポートとプロキシ サーバーのホスト名を設定できます。Client Proxy は、クラウド プロキシ サーバーとの安全な接続を確立するために Transport Layer Security (TLS) 1.2 以降を使用します。安全なチャネルを経由して転送されるトラフィックはすべてプライベートのままです。

- **[検証が失敗した場合はブロック]** – このチェックボックスを選択すると、証明書の検証が失敗したときにクラウド プロキシ サーバーへのトラフィックがブロックされます。

Note

プロキシ サーバーの証明書の検証が失敗すると、そのプロキシ (プライマリまたは代替) サーバーへのトラフィックがブロックされます。

- ポート 8081 (セキュア チャネル ポート) で接続の問題が発生した場合は、接続を許可するかブロックするかを決定できます。以下のいずれかを実行します。
  - **[接続をブロック]** – 接続をブロックするにはこれを選択します。

    Note

    プロキシ サーバーの証明書の検証が失敗すると、そのプロキシ (プライマリまたは代替) サーバーへのトラフィックがブロックされます。

  - **[セキュア チャネルなしで接続を許可]** – Client Proxy と McAfee WGCS の間で安全な接続を確立せずに、設定されたプロキシ ポート (8080) 経由の接続を許可するには、これを選択します。

    Note

    このオプションを選択すると、設定済みのすべての (オンプレミスとクラウドの両方の) プロキシ サーバーがトラフィックのフィルタリングの対象と見なされます。プロキシ サーバーが選択される順序は、プロキシ サーバー リストの設定時に選択したオプションによって異なります ([下記のリスト順に、最初にアクセス可能なプロキシ サーバーに接続する] または [最も応答時間の短いプロキシ サーバーに接続する])。

8. [トラフィック リダイレクト] の設定を選択します。
   - **[コンピューターが会社のネットワークに接続されておらず、VPN を介して操作をしていない場合にネットワーク トラフィックをリダイレクトする]** – ユーザーが組織のネットワーク外で作業しており、VPN を介して接続されていない場合に、Web リクエストをプロキシ サーバーにリダイレクトします。
   - **[常にネットワーク トラフィックをプロキシ サーバーにリダイレクトする]** – ネットワーク内およびネットワーク外で作業するユーザーや、VPN を介してネットワークに接続して作業するユーザーからのリクエストを含む、すべての Web リクエストをプロキシ サーバーにリダイレクトします。
9. [会社のネットワークの検出] の設定を選択します。
   - **[ePO への接続をテストする]** – クライアント ソフトウェアが McAfee ePO サーバーに接続できた場合は、エンドポイントがネットワーク内にあります。

- **[以下のいずれかの会社のサーバーへの接続をテストする]** – クライアント ソフトウェアが設定したネットワーク サーバーに接続できた場合は、エンドポイントがネットワーク内にあります。

10. [会社の VPN 検出] を設定するには、1 つ以上の VPN サーバーのアドレスとポート番号を指定します。クライアント ソフトウェアが設定した VPN に接続できた場合は、エンドポイントは VPN によりネットワークに接続しています。
11. 正規表現を使用して [Active Directory グループ フィルター] を設定し、プロキシ サーバーに Web リクエストをリダイレクトする前に、クライアント ソフトウェアが Web リクエストに追加するヘッダーのグループを制限します。グループ メンバーシップ情報は 4096 文字以下にする必要があります。
    形式: <ドメイン名>\\<グループ名>
12. (macOS) [ログ ファイル] の設定を選択します。
    - **[Log messages with Error and Critical priority]** (エラーと重大度の優先順位を含むメッセージを記録する)
    - **[Log messages with Error, Critical, Information, and Warning priority]** (エラー、重大度、情報、および警告の優先順位を含むメッセージを記録する)
    - **[すべてのメッセージを記録する (トラブルシューティングとデバッグの目的の場合に推奨)]**
    - **[メッセージを記録しない]**

    Note

    Windows が実行されているエンドポイントの場合、ログ ファイルは C:\Program Data\McAfee\MCP\Logs フォルダーにあります。重大なエラー メッセージが Mcp.log という名前のファイルに保存されます。

13. (Windows) [アクセス保護] を設定します。
    - **[アクセス保護を有効にする]** – 選択すると、ユーザーは、Windows タスク マネージャーを使用してクライアント ソフトウェアを無効にしたり、ファイルを編集または削除したり、レジストリ値を変更したりできなくなります。
    - **[手動で削除するリリース キーを要求する]** – 選択すると、ユーザーは管理者に解放コードを要求し、それを使用してクライアント ソフトウェアをアンインストールできます。選択を解除すると、ユーザーは Windows のアンインストール機能を使用してソフトウェアをアンインストールする必要があります。ベストプラクティスは、解放コードを使用してソフトウェアをアンインストールすることです。
14. [保存] をクリックします。

タスクの結果

クライアントの設定が Client Proxy ポリシーと共に保存されます。

バイパス リストを設定する (McAfee ePO または McAfee ePO Cloud)

Client Proxy ポリシーは、バイパス リストの項目に一致する Web トラフィックについて、プロキシ サーバーをバイパスしてインターネットに直接送信されるのを許可します。

始める前に

管理者として McAfee ePO または McAfee ePO Cloud サーバーにログオンする必要があります。

このポリシーに関連付ける Common Catalog インスタンスがない場合には、バイパス リストを設定する前にインスタンスを作成する必要があります。

タスク

1. McAfee ePO または McAfee ePO Cloud メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy の設定] メニューで [バイパス リスト] を選択します。
6. [バイパス リスト] ペインの [Common Catalog] ドロップダウン リストで、Common Catalog インスタンスを選択します。
7. リスト項目をカタログからバイパス リストに追加します。
   a. [アクション] ドロップダウン リストで、[バイパス リスト項目を追加] を選択してから、カテゴリを選択します。
   b. [既存の値から選択] ダイアログ ボックスで、バイパス リストに追加するリスト項目を選択します。
   c. (オプション) 既存のリスト項目を編集するか、新しい項目を追加します。

      Caution

      この手順で行った変更は、Common Catalog のこのインスタンスを共有するすべてのポリシーに適用されます。

   d. [OK] をクリックします。

   ダイアログ ボックスが閉じ、選択したリスト項目がバイパス リストに追加されます。
8. (オプション) バイパス リストの項目を編集または削除します。
9. [保存] をクリックします。

タスクの結果

バイパス リストと Common Catalog インスタンスがポリシーと共に保存されます。

代替リダイレクト リストを設定する (McAfee ePO または McAfee ePO Cloud)

Web トラフィックを代替リダイレクト プロキシ サーバーにリダイレクトするには、代替リダイレクト リストでドメイン名、ネットワーク アドレス、ネットワーク ポート、およびプロセス名を設定します。 代替リダイレクト リストに追加された項目のリストを表示したり、必要に応じてアイテムを追加、編集、または削除したりすることができます。

始める前に

管理者として McAfee ePO または McAfee ePO Cloud サーバーにログオンする必要があります。

このポリシーに関連付ける Common Catalog インスタンスがない場合には、代替リダイレクト リストを設定する前にインスタンスを作成する必要があります。

タスク

1. McAfee ePO または McAfee ePO Cloud メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy 設定] メニューから、[代替リダイレクト リスト] を選択します。
6. [代替リダイレクト リスト] ペインの [Common Catalog] ドロップダウン リストから Common Catalog インスタンスを選択します。
7. カタログから代替リダイレクト リストにリスト項目を追加します。
   a. [アクション] ドロップダウン リストから、[Add Alternate Redirection] (代替リダイレクトを追加する) を選択し、カテゴリを選択します。
   b. [既存の値から選択] ダイアログ ボックスで、代替リダイレクト リストに追加するリスト項目を選択します。
   c. (オプション) 既存のリスト項目を編集するか、新しい項目を追加します。

      Caution

      このステップで行った変更は、Common Catalog のこのインスタンスを共有するすべてのポリシーに適用されます。

   d. [OK] をクリックします。

   ダイアログ ボックスが閉じ、選択したリスト項目が代替リダイレクト リストに追加されます。
8. (オプション) 代替リダイレクト リストで項目を編集または削除できます。
9. [保存] をクリックします。

   代替リダイレクト リストと Common Catalog インスタンスがポリシーと共に保存されます。
10. (オプション) [複製] をクリックして、選択した Client Proxy ポリシーを複製します。

バイパス リストを設定する (MVISION ePO)

バイパス リストでは、ドメイン名、ネットワーク アドレス、ネットワーク ポート、プロセス名を設定できます。 バイパス リストに追加された項目のリストを表示したり、必要に応じてリストに項目を追加、編集、または削除したりできます。

始める前に

管理者として MVISION ePO サーバーにログオンする必要があります。

タスク

1. MVISION ePO メニューで、[ポリシー] → [ポリシー カタログ] → [McAfee Client Proxy] の順に選択します。
2. [MCP ポリシー] をクリックしてポリシー リストを表示します。
3. 設定するポリシーと同じ行の [編集] をクリックします。
4. [Client Proxy 設定] で、[バイパス リスト] をクリックします。
5. [バイパス リスト] ペインで、カテゴリを選択します。

- **[ドメイン名]** – ドメイン名を入力して **[追加]** をクリックします。 このリストのドメインに送信された Web トラフィックが、プロキシ サーバーをバイパスします。 例: google.com
- **[ネットワーク アドレス (IP)]** – ネットワーク IP アドレスを入力して **[追加]** をクリックします。 このリストの IP アドレスに送信された Web トラフィックが、プロキシ サーバーをバイパスします。 アドレスは、個別に設定することも、範囲で設定することも、サブネットまたは CIDR を使用することもできます。
  以下に例を示します。
  - 192.168.1.1
  - 172.31.255.10-172.31.255.20
  - 10.50.0.0/255.255.128.0
  - 10.50.0.0/17
- **[ネットワーク ポート]** – ポート番号とその説明を入力して **[追加]** をクリックします。 このリストのポートに送信された Web トラフィックが、プロキシ サーバーをバイパスします。 例: 40, 80, 400-500
- **[プロセス リスト]** – プロセス名を入力して **[追加]** をクリックします。 このリストのプロセスから送信された Web トラフィックが、プロキシ サーバーをバイパスします。 エンドポイントではプロセスが実行されます。 Windows のプロセス名は .exe で終わる必要があります。 macOS のプロセス名には、ファイル名の拡張子は必要ありません。 McAfee のプロセスや信頼される他のプロセスをこのリストに追加します。

6. [保存] をクリックします。
7. 必要に応じて、[複製] をクリックしてポリシーを複製します。

代替リダイレクト リスト (MVISION ePO) を設定する

Web トラフィックを代替リダイレクト プロキシ サーバーにリダイレクトするには、代替リダイレクト リストでドメイン名、ネットワーク アドレス、ネットワーク ポート、およびプロセス名を設定します。 代替リダイレクト リストに追加された項目のリストを表示したり、必要に応じてアイテムを追加、編集、または削除したりすることができます。

始める前に

管理者として MVISION ePO サーバーにログオンする必要があります。

タスク

1. MVISION ePO メニューで、[ポリシー] → [ポリシー カタログ] → [McAfee Client Proxy] の順に選択します。
2. [MCP ポリシー] をクリックしてポリシー リストを表示します。
3. 設定するポリシーと同じ行の [編集] をクリックします。
4. [Client Proxy 設定] の下で、[代替リダイレクト リスト] をクリックします。
5. [代替リダイレクト リスト] ペインで、カテゴリを選択します。
   - **[ドメイン名]** – ドメイン名を入力して **[追加]** をクリックします。 指定したドメインに送信された Web トラフィックは、代替プロキシ サーバーにリダイレクトされます。 例: google.com

- **[ネットワーク アドレス (IP)]** – ネットワーク IP アドレスを入力して **[追加]** をクリックします。 指定した IP アドレスに送信された Web トラフィックは、代替プロキシ サーバーにリダイレクトされます。 アドレスは、個別に設定することも、範囲で設定することも、サブネットまたは CIDR を使用することもできます。
  以下に例を示します。
  - 192.168.1.1
  - 172.31.255.10-172.31.255.20
  - 10.50.0.0/255.255.128.0
  - 10.50.0.0/17
- **[ネットワーク ポート]** – ポート番号とその説明を入力して **[追加]** をクリックします。 指定したポートに送信された Web トラフィックは、代替プロキシ サーバーにリダイレクトされます。 例: 40, 80, 400-500
- **[プロセス リスト]** – プロセス名を入力して **[追加]** をクリックします。 指定したプロセスからの Web トラフィックは、代替プロキシ サーバーにリダイレクトされます。 プロセスはエンドポイントで実行されます。 Windows のプロセス名は .exe で終わる必要があります。 macOS のプロセス名には、ファイル名の拡張子は必要ありません。 McAfee のプロセスや信頼される他のプロセスをこのリストに追加します。

6. [保存] をクリックします。
7. 必要に応じて、[複製] をクリックしてポリシーを複製します。

バイパス リストをインポートまたはエクスポートする (MVISION ePO)

インポート オプションとエクスポート オプションを使用して、バイパス リストをコピーできます。 バイパス リストをインポートまたはエクスポートすると、バイパス リスト項目の追加、編集、削除を行うことができます。 既存のバイパス リストをエクスポートして、変更し、その後再びファイルをインポートすることをお勧めします。 バイパス リストをインポートすると、既存のすべてのバイパス項目が上書きされます。 インポート オプションまたはエクスポート オプションでサポートされているのは、.txt ファイル形式のみです。

バイパス リストの項目リストのサンプルを以下に示します。

```
type = DOMAIN google.com
intel.com type = NETWORKADDRESS 192.168.1.1
172.31.255.10 - 172.31.255.20
10.50.0.0/255.255.128.0
10.50.0.0/17 type = NETWORKPORT Port Number Description
80,443 Http/Https 21-47 Port with Range
22
31,78,100-500 type = PROCESSNAME chrome.exe
firefox.exe
xcode
```

Note

ポート番号は説明なしで追加できます。プロセス名は、Windows または macOS プロセスの名前です。

タスク

1. MVISION ePO メニューで、[ポリシー] → [ポリシー カタログ] → [McAfee Client Proxy] の順に選択します。
2. [MCP ポリシー] をクリックしてポリシー リストを表示します。
3. バイパス リストをインポートまたはエクスポートするポリシーと同じ行にある [編集] をクリックします。
4. [Client Proxy 設定] で、[バイパス リスト] をクリックします。
5. [バイパス リスト] ペインで、以下を実行します。
   - バイパス リストをエクスポートするには、**[バイパス リストをエクスポートする]** をクリックします。 ブラウザーによって、バイパス リストが .txt ファイルとしてダウンロードされます。
   - バイパス リストをインポートするには、**[バイパス リストをインポートする]** をクリックします。
     - ダイアログ ボックスで、**[ファイルの選択]** をクリックして、バイパス リスト ファイルを含むフォルダーに移動します。 ファイルを選択して、**[開く]** をクリックします。 バイパス リストをインポートすると、確認メッセージが表示されます。

     Note

     バイパス リストの項目のリストが正しい形式になっていることを確認してください。 インポートに失敗した場合、[バイパス リストをインポートする] ダイアログ ボックスに、エラーが発生した行番号が表示されます。 エラーの修正後、ファイルを再度インポートすることができます。
6. [保存] をクリックします。

代替リダイレクト リストをインポートまたはエクスポートする (MVISION ePO)

インポート オプションとエクスポート オプションを使用して、代替リダイレクト リストをコピーできます。 代替リダイレクト リストをインポートまたはエクスポートした後、代替リダイレクト リストに設定されているドメイン名を追加、編集、削除できます。 既存の代替リダイレクト リストをエクスポートして、変更し、その後再びファイルをインポートすることをお勧めします。 代替リダイレクト リストをインポートすると、既存の代替リダイレクト エントリがすべて上書きされます。 インポート オプションまたはエクスポート オプションでサポートされているのは、.txt ファイル形式のみです。

代替リダイレクト リストの例を次に示します。

```
type = DOMAIN google.com
intel.com
```

タスク

1. MVISION ePO メニューで、[ポリシー] → [ポリシー カタログ] → [McAfee Client Proxy] の順に選択します。
2. [MCP ポリシー] をクリックしてポリシー リストを表示します。
3. 代替リダイレクト リストをインポートまたはエクスポートするポリシーと同じ行にある [編集] をクリックします。

4. [Client Proxy 設定] の下で、[代替リダイレクト リスト] をクリックします。
5. [代替リダイレクト リスト] ペインで、次の操作を行います。
   - 代替リダイレクト リストをエクスポートするには、[代替リダイレクト リストのエクスポート] をクリックします。 ブラウザーによって、代替リダイレクト リストが .txt ファイルとしてダウンロードされます。
   - 代替リダイレクト リストをインポートするには、[代替リダイレクト リストのインポート] をクリックします。
     - ダイアログ ボックスで、[ファイルの選択] をクリックして、代替リダイレクト リスト ファイルを含むフォルダーに移動します。 ファイルを選択して、[開く] をクリックします。 代替リダイレクト リストをインポートすると、確認メッセージが表示されます。

     Note

     代替リダイレクト リストでドメイン名のリストが正しい形式になっていることを確認してください。 インポートに失敗した場合、[代替リダイレクト リストのインポート] エラーが発生した行番号が表示されます。 エラーの修正後、ファイルを再度インポートすることができます。

6. [保存] をクリックします。

ブロック リストを設定する

各 Client Proxy ポリシーは、ブロックされるプロセスのリストに関連付けられています。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

プロセス リストは、エンドポイントで実行されるプロセスのリストです。 Windows のプロセス名は .exe で終わる必要があります。 macOS のプロセス名には、ファイル名の拡張子は必要ありません。

フィルタリングのためにプロキシ サーバーにリダイレクトされるトラフィックの量を削減するには、ネットワークへのアクセスがブロックされるエンドポイント プロセスのリストを設定します。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [Client Proxy の設定] メニューで [ブロック リスト] を選択します。
6. 以下のオプションから 1 つを選択します。
   - [トラフィックが宛先に直接移動することを許可する] – すべてのプロセスがプロキシ サーバーを経由せずにインターネットにアクセスすることを許可します。
   - [すべてのプロセスのトラフィックをブロックする (バイパスにリストされたプロセスを除く)] – バイパス リストにあるプロセス以外のすべてのプロセスについて、インターネットへのアクセスをブロックします。

- **[次のプロセスについてのみトラフィックをブロックする]** – このリストにあるプロセス以外のすべてのプロセスが、プロキシ サーバーを経由せずにインターネットにアクセスすることを許可します。 **[追加]**、**[編集]**、**[削除]** の各機能を使用してリストを設定します。

7. [保存] をクリックします。

タスクの結果

ブロック リストが Client Proxy ポリシーと共に保存されます。

ポリシーをエンドポイントに割り当てる

McAfee ePO、McAfee ePO Cloud、または MVISION ePO を使用して、Client Proxy ポリシーをエンドポイントに割り当てることができます。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. ポリシーを割り当てる組織のレベルを選択します。

   ご使用のプラットフォームによって管理されているすべてのエンドポイントを選択するには、[ユーザーの組織] を選択します。

3. [割り当て済みのポリシー] をクリックします。
4. [製品] ドロップダウン リストで、McAfee Client Proxy の現在のバージョンを選択します。
5. [アクション] 列で、割り当てるポリシーと同じ行にある [割り当てを編集] をクリックします。
6. [継承元] で、[継承を無効にし、以下のポリシーおよび設定を割り当てます] を選択します。
7. [割り当て済みのポリシー] ドロップダウン リストで、ポリシーを選択します。
8. [ポリシー継承をロック] のオプションを選択します。
   - **[ロック解除]** – 1 つ以上のサブグループにさまざまなポリシーを割り当てることができます。
   - **[ロック済み]** – このポリシーはすべてのサブグループに割り当てる必要があります。
9. [保存] をクリックします。

タスクの結果

ポリシーがエンドポイントに割り当てられます。

ポリシーを .xml または .opg ファイルにエクスポートする

Client Proxy ポリシーを McAfee ePO、McAfee ePO Cloud、または MVISION ePO から .xml ファイルまたは .opg ファイルにエクスポートします。

始める前に

管理者として McAfee ePO、McAfee ePO Cloud、または MVISION ePO サーバーにログオンする必要があります。

McAfee ePO や McAfee ePO Cloud で管理されていないスタンドアロン コンピューターの場合は、ポリシーを .opg ファイルにエクスポートして、コンピューターのローカルに保存する必要があります。

タスク

1. メイン メニューで、[ポリシー] → [ポリシー カタログ] の順に選択します。
2. [製品] リストで、Client Proxy の現在のバージョンを選択します。
3. [MCP ポリシー] をクリックしてポリシー リストを表示します。
4. 設定するポリシーと同じ行の [編集] をクリックします。
5. [アクション] ドロップダウン リストで、[ポリシーをファイルにエクスポート] を選択します。
6. ダウンロードするポリシー ファイルを右クリックして、[保存] → [OK] の順にクリックします。
   - **[McAfee Client Proxy** ポリシー サーバー ファイル**]** – Client Proxy ポリシーを .xml ファイルにエクスポートします。これはトラブルシューティングに使用できます。
   - **[McAfee Client Proxy** ポリシー クライアント ファイル**]** – Client Proxy ポリシーを .opg ファイルにエクスポートします。これはスタンドアロン コンピューターまたはエンドポイント コンピューターに保存できます。
7. .opg ファイルの名前を MCPPolicy.opg に変更して、クライアント コンピューターの次の場所にコピーします。
   - Windows ベースのコンピューター – C:\ProgramData\McAfee\MCP\Policy\Temp
   - macOS のコンピューター – /usr/local/mcafee/mcp/policy

タスクの結果

Client Proxy がスタンドアロン コンピューターまたはエンドポイント コンピューターで実行を開始すると、ポリシーが読み込まれ、トラフィックのリダイレクトが開始されます。

Windows ベースまたは macOS のコンピューターでポリシー強制を中断する

承認されたビジネス上の理由によりユーザーが機密情報にアクセスしたり、転送したりする必要がある場合には、Windows または macOS を実行しているスタンドアロン コンピューターまたはエンドポイント コンピューターで、ポリシー強制を中断できます。

ポリシー強制を中断するには、Help Desk ソフトウェアにより提供されるチャレンジ応答プロトコルに従います。

タスク

1. ユーザー – [解放コードを入力] ダイアログ ボックスを開き、次のようにします。
   - Windows – **[スタート]** メニューで、[McAfee] → [Bypass McAfee Client Proxy (McAfee Client Proxy をバイパス)] の順にクリックします。
   - macOS – ステータス バーの McAfee メニュレットで **[コンソール]** を選択した後、**[Client Proxy]** を選択します。

   Caution

   解放コードを待っている間、ユーザーはダイアログ ボックスを開いたままにしておく必要があります。 ボックスを閉じた場合には、手順をやり直す必要があります。

2. ユーザー – 以下が記載された電子メールを管理者に送ります。
   - ユーザー名と電子メール アドレス
   - **[ポリシー名とポリシー リビジョン]**番号 (**[解放コードを入力]** ダイアログ ボックスからコピー)
   - **[識別]** コード (**[解放コードを入力]** ダイアログ ボックスからコピー)
3. 管理者 – Help Desk ソフトウェアとユーザーから提供された値を使用して解放コードを生成し、ユーザーに送信します。 MVISION ePO の [MCP 管理] ページで、解放コードを生成できます。
4. ユーザー – [解放] フィールドに解放コードを入力し、[OK] (Windows) または [解放] (macOS) をクリックします。

タスクの結果

ポリシー強制が、解放コードの生成時に指定された期間だけ中断されます。

クエリーとレポート

データベース クエリーを作成して実行する (McAfee ePO)

データベース クエリーを作成して実行し、クライアント タスクとポリシーに関する情報を返します。

始める前に

管理者として McAfee ePO サーバーにログオンする必要があります。

Note

McAfee ePO Cloud 管理者はクエリーを実行できますが、作成することはできません。

タスク

1. McAfee ePO メニューで、[レポート] → [クエリーとレポート] の順に選択します。
2. [グループ] メニューで、[McAfee グループ] → [McAfee Client Proxy] の順に選択し、[新しいクエリー] をクリックします。
3. [クエリー ビルダー] で、[機能グループ] リストから [ポリシー管理] を選択します。
4. [結果タイプ] を選択し、[次へ] をクリックします。
   - **[適用済みのクライアント タスク]** – クライアント タスクの名前と、タスクが適用された組織のレベルが返されます。
   - **[適用されたポリシー]** – ポリシーの名前と、ポリシーが適用された組織のレベルが返されます。
   - **[クライアント タスクの割り当てで無効な継承]** – クライアント タスクの名前と、タスクの割り当てが無効になっている組織のレベルが返されます。
   - **[ポリシー割り当てで無効な継承]** – ポリシーの名前と、ポリシーの割り当てが無効になっている組織のレベルが返されます。

   [グラフ] ページが開きます。
5. クエリーの結果をグラフ形式で表示する方法を設定します。
   a. グラフ タイプを選択します。
   b. 必要に応じて、ラベル、単位、ソート順などの値を指定します。
   c. [次へ] をクリックします。

   [列] ページが開きます。
6. クエリーの結果を表形式で表示する方法を設定し、[次へ] をクリックします。
   - **[使用可能な列]** メニューで、列名をクリックして選択します。
   - **[選択された列]** ペインで、列を閉じて削除します。
   - 選択した列の順序を変更するには、列をドラッグ アンド ドロップするか、矢印キーを使用します。

   [フィルター] ページが開きます。
7. クエリーの結果をフィルタリングする方法を設定します。
   a. [使用可能なプロパティ] メニューで、プロパティ名をクリックして選択します。
   b. [比較] ドロップダウン リストで、各プロパティの演算子を選択します。

   c. 各演算子に値を選択します。
8. [実行] をクリックしてクエリーの結果を表示した後、必要に応じて [クエリーの編集] をクリックして変更を行います。
9. [保存] をクリックした後、[クエリーの保存] ページで以下を実行します。
   a. クエリーの名前と説明 (オプション) を指定します。
   b. 既存のグループを選択するか、新しいグループを指定します。
   c. [保存] をクリックします。

タスクの結果

データベース クエリーが保存され、後で使用できるようになります。

Client Proxy レポートを作成する (McAfee ePO または MVISION ePO)

過去 1 か月間に Client Proxy のインストールが成功または失敗したエンドポイントの数を .pdf 形式で出力します。

始める前に

管理者として McAfee ePO サーバーまたは MVISION ePO サーバーにログオンする必要があります。

タスク

1. McAfee ePO または MVISION ePO メニューで、[レポート] → [クエリーとレポート] の順に選択します。
2. [グループ] リストで、[McAfee グループ] → [McAfee Client Proxy] の順に選択します。
3. [レポート] タブをクリックして、[新しいレポート] をクリックします。
4. [ツールボックス] で、1 つ以上のテンプレートを [レポートのレイアウト] 領域にドラッグし、それらを設定して配置します。
   - **[イメージ]**
   - **[ページ区切り]**
   - **[クエリー グラフ]**
   - **[クエリー テーブル]**
   - **[テキスト]**

   Note

   クエリー グラフまたはテーブルを追加する際に、[クエリー] ドロップダウン リストから [MCP: 先月の Endpoint インストールの成功/失敗イベント] を選択します。

5. レポートをカスタマイズするには、次のオプションをクリックします。
   - **[ヘッダーとフッター]**
   - **[ページ設定]**
   - **[ランタイム パラメーター]**
6. [実行] をクリックすると、レポートが .pdf 形式で表示されます。

7. [保存] をクリックした後、[名前、説明、グループ] ダイアログ ボックスで次を実行します。
    a. レポートの名前と説明 (オプション) を指定します。
    b. 既存のグループを選択するか、新しいグループを指定します。
    c. [OK] をクリックします。

タスクの結果

Client Proxy レポートが保存され、再度実行できます。

著作権