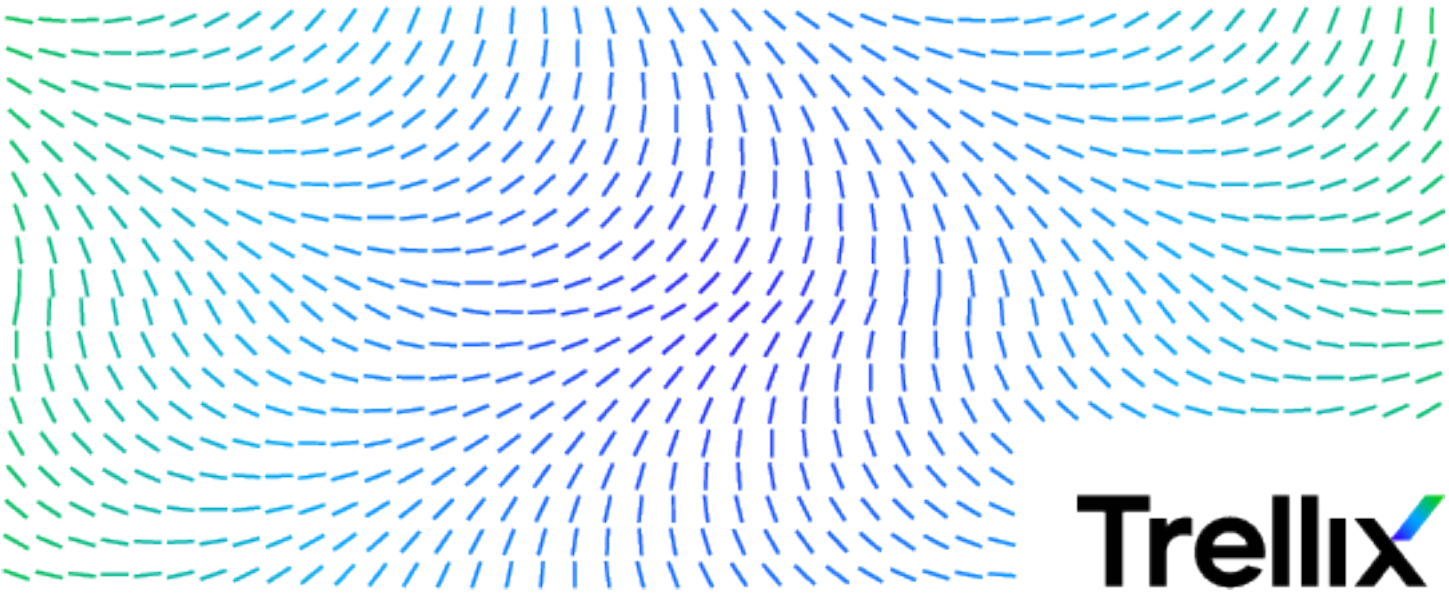
McAfee Client Proxy 4.1.x Product Guide



COPYRIGHT

Copyright © 2022 Musarubra US LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE ENTERPRISE (MUSARUBRA US LLC) OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1 **Product overview** 5

Overview . . . 5
Key features . . . 6
How it works . . . 6

2 **Managing Client Proxy policies** 9

Client Proxy metadata . . . 9
Permission Sets (McAfee ePO) . . . 10
User permissions . . . 10
Configure a permission set . . . 10
Permissions required to administer Client Proxy . . . 11
Policy review and approval . . . 12
How the shared password is used . . . 12
Considerations when changing the shared password (McAfee ePO Cloud) . . . 13
Import your customer ID and shared password (MVISION ePO) . . . 13
Create a Common Catalog instance (McAfee ePO or McAfee ePO Cloud) . . . 14
Configure a policy . . . 15
Create a Client Proxy policy . . . 15
How Client Proxy manages the proxy server list . . . 16
Configure the proxy server list . . . 16
Configure the alternate proxy server list . . . 18
Configure the client settings . . . 19
Configure the bypass list (McAfee ePO or McAfee ePO Cloud) . . . 21
Configure the alternate redirection list (McAfee ePO or McAfee ePO Cloud) . . . 22
Configure the bypass list (MVISION ePO) . . . 23
Configure the alternate redirection list (MVISION ePO) . . . 23
Import or export the bypass list (MVISION ePO) . . . 24
Import or export the alternate redirection list (MVISION ePO) . . . 25
Configure the block list . . . 26
Assign a policy to the endpoints . . . 27
Export a policy to an .xml or .opg file . . . 27
Suspend policy enforcement on a Windows-based or macOS computer . . . 28

3 **Queries and reports** 29

Create and run a database query (McAfee ePO) . . . 29
Create a Client Proxy report (McAfee ePO or MVISION ePO) . . . 30

1 Product overview

Contents

- *Overview*
- *Key features*
- *How it works*

Overview

McAfee® Client Proxy software helps protect your endpoint users from security threats that arise when they access the web from inside or outside your network.

The client software, which is installed on endpoints running Microsoft Windows or macOS, redirects web requests or allows them to continue to a proxy for filtering. The server software runs on one of three management platforms: McAfee ePO, McAfee ePO Cloud, or MVISION ePO.

Web Protection hybrid solution

Client Proxy is an essential component of the McAfee® Web Protection hybrid solution. This solution allows you to integrate the network-based and cloud-based security functions provided by McAfee® Web Gateway and McAfee® Web Gateway Cloud Service (McAfee® WGCS), respectively.

The Client Proxy software allows or redirects web traffic depending on the location of the endpoint:

- **Endpoints located inside the network or connected by VPN** — Traffic is allowed to continue to a Web Gateway appliance installed on the network for filtering.
- **Endpoints located outside the network** — Traffic is redirected to McAfee WGCS for filtering.

Integration with Endpoint Security

When deploying Client Proxy with McAfee® Endpoint Security on the endpoints, you install and manage each product separately using McAfee® ePolicy Orchestrator® (McAfee® ePO™) , McAfee ePO Cloud, or MVISION ePO.

- Client Proxy administrators — Configure policies and run tasks as usual.
- Endpoint Security administrators — Have the option of configuring McAfee® Endpoint Security Web Control so that it is disabled while Client Proxy is installed and actively redirecting web traffic.

On endpoints running Windows, you can view whether Client Proxy is installed and running on the endpoint and actively redirecting traffic by opening the **About McAfee Client Proxy** window from the **Start** menu.

Key features

Client Proxy allows or redirects web requests from users based on policies that you configure.

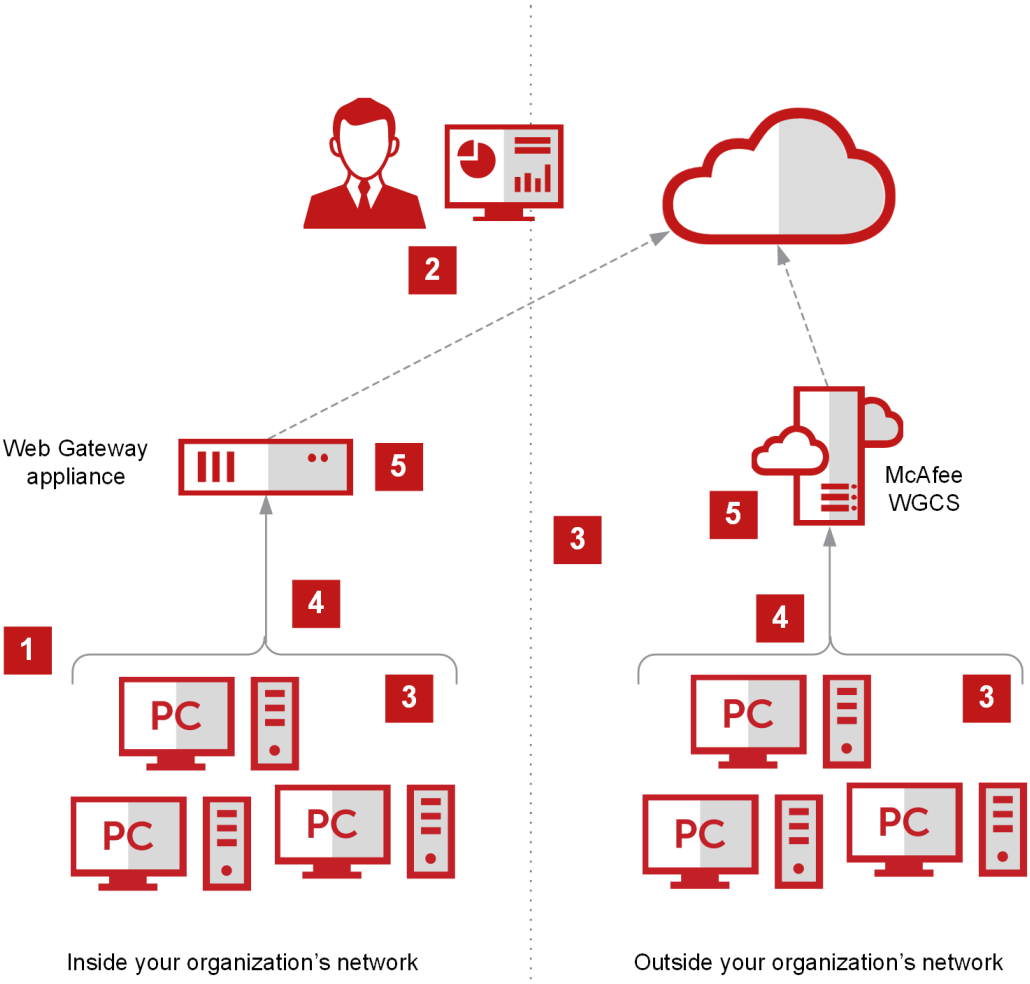
- **Traffic redirection** — The software redirects web traffic to proxy servers for filtering according to the settings in the Client Proxy policy.
- **Location awareness** — Location-awareness settings allow one policy to cover users working inside the network, outside the network, or connected to the network by VPN.
- **Centralized management** — The software is managed with McAfee ePO, McAfee ePO Cloud, or MVISION ePO.
- **Browser independence** — Proxy server settings are configured in Client Proxy instead of in the browsers running on the endpoints.
- **Transparent authentication** — Client Proxy authenticates users without prompting for credentials and passes group membership and other information in metadata that it adds to HTTP/HTTPS requests.
- **Tamper resistance** — Users are not allowed to remove Client Proxy software from the endpoint without requesting and receiving a temporary release code from an administrator.
- **Secure Channel** — The software establishes a secure communication channel between Client Proxy and McAfee WGCS for all HTTP/HTTPS requests. This is applicable only for cloud proxies.

How it works

The Client Proxy software redirects, blocks, or allows web traffic according to the Client Proxy policy and the location of the endpoints.

Client Proxy workflow

1. The Client Proxy software is installed on the endpoints in your organization.
2. Using McAfee ePO, McAfee ePO Cloud, or MVISION ePO, the administrator creates a Client Proxy policy and assigns the policy to all managed endpoints.
3. Managed endpoints can be located inside your organization's network, connected to the network by VPN, or located outside the network.
4. Users working on the endpoints request access to web resources.
5. The software determines the user's location, then allows or redirects the web request:
   - Inside the network or connected by VPN — Allows the web request to continue to a Web Gateway appliance installed on the network, where it is filtered. Client Proxy is *passive*.
   - Outside the network — Redirects the web request to McAfee WGCS for filtering. Client Proxy is *active*.


Web Gateway appliance
McAfee WGCS
PC
PC
PC
PC
PC
PC
1
2
3
4
5
3
4
5
Inside your organization's network
Outside your organization's network

2 Managing Client Proxy policies

Contents

- *Client Proxy metadata*
- *Permission Sets (McAfee ePO)*
- *How the shared password is used*
- *Considerations when changing the shared password (McAfee ePO Cloud)*
- *Import your customer ID and shared password (MVISION ePO)*
- *Create a Common Catalog instance (McAfee ePO or McAfee ePO Cloud)*
- *Configure a policy*
- *Assign a policy to the endpoints*
- *Export a policy to an .xml or .opg file*
- *Suspend policy enforcement on a Windows-based or macOS computer*

Client Proxy metadata

When the Client Proxy software redirects HTTP/HTTPS traffic, it adds metadata to the requests.

Other products, such as Web Gateway and McAfee WGCS, use the metadata (for example, group membership) when applying web protection policies.

- Authentication tokens — Tokens containing identity information about the user making the web request
- Authentication version — Version of the metadata that Client Proxy is sharing
- Client IP address — IP address of the endpoint where the traffic originated
- Original destination IP address — Saved IP address of the server where the traffic is destined
- Customer ID — Uniquely identifies the customer's organization
- User ID — Uniquely identifies the user making the web request
- User groups — Names of any groups where the user is a member
- Tenant ID — ID shared by the nodes in a cluster (McAfee ePO Cloud or MVISION ePO)
- Process name — Name of the process that generates traffic
- Process Executable Path — Path of the process that generates traffic
- System Information — System information such as host operating system name (Windows, Mac), local time (seconds since 1/1/1970), Mac address, process uptime, system name, and mcp policy name

Permission Sets (McAfee ePO)

Contents

- *User permissions*
- *Configure a permission set*
- *Permissions required to administer Client Proxy*
- *Policy review and approval*

User permissions

You manage user permissions by configuring *permissions sets* in the McAfee ePO interface, one permission set for each role.

The UI comes with predefined roles and permission sets that you can edit. You can also add a role and configure a set of permissions for it.

Administrative users

One predefined role, the **MCP Catalog Admin**, has all permissions required to create, delete, and manage Client Proxy policies. A full permission set is required to give Client Proxy administrators permission to:

- Create, delete, and manage policies
- Push policies to endpoints
- View queries
- Manage Client Proxy extension software
- Perform Master Repository functions
- Perform Help Desk functions

Only McAfee ePO administrators have permissions to manage extension software, including permission to:

- Install extensions on a McAfee ePO server
- Remove extensions from a McAfee ePO server
- Update extensions installed on a McAfee ePO server

Configure a permission set

You can update the permission sets for an existing role or configure them for a new role.

Before you begin

You must be logged on to the McAfee ePO server as an administrator.

Task

1. From the McAfee ePO menu, select **User Management** | **Permission Sets**.
2. Under **Permission Sets**, select a role.
3. In the configuration pane, click **Edit** to open any permission set.
4. Update the settings in the permission set, then click **Save**.

Permissions required to administer Client Proxy

Specific permissions are required to administer Client Proxy.

Table 2-1 Client Proxy administrator permissions

Permissions	Settings	Required to...
Agent Handler	Select **View Agent Handlers**	• Push policies to endpoints • View queries
Client Events	Select **View Client Events**	• Push policies to endpoints • View queries
Common Catalog	Select a **Catalog Permission Template**, then select all Common Catalog actions: • **Create, rename and duplicate catalogs** • **Delete catalogs** • **Import catalog items from other catalogs** • **Import catalog items from files** • **Export catalog items to files**	Create, delete, and manage policies
Help Desk Actions	Select all Client Proxy actions: • **Generate client uninstall key** • **Generate bypass client key** • **Generate master response key for the keys above**	Perform Help Desk functions McAfee ePO administrators have all Help Desk permissions by default. Before you can give these permissions to other administrators, you must first install the Help Desk extension.
McAfee Agent	• **McAfee Agent : Policy** — Select **View and change settings** • **McAfee Agent : Tasks** — Select **View and change settings**	• Push policies to endpoints • View queries
MCP Policy	Select **View and change policy and task settings**	Create, delete, and manage policies
Queries and Reports	Select **Edit public groups; create and edit private queries/reports; make private queries/reports public**	• Push policies to endpoints • View queries
Software	**Master Repository** — Select **Add, remove, and change packages; perform pull tasks** **Distributed Repositories** — Select **Add, remove, and change repositories; perform replication tasks**	Perform Master Repository functions: • Add software packages • Remove software packages • Refresh checked-in packages

Table 2-1 Client Proxy administrator permissions *(continued)*

Permissions	Settings	Required to...
Systems	**System Tree** — Select **View "System Tree" tab** **Actions** — Select: • **Wake up agents; view Agent Activity Log** • **Edit System Tree groups and systems** • **Deploy agents** **Tag use** — Select **Apply, exclude, and clear tags** **Tag catalog** — Select **Create and edit tags, tag groups and tag criteria**	• Push policies to endpoints • View queries
System Tree access	Select **My Organization**	• Push policies to endpoints • View queries

Policy review and approval

You can set up the review and approval of Client Proxy policies in the McAfee ePO interface.

Setup tasks include creating permission sets, assigning them to users, and configuring the approval settings on the **Server Settings** page.

1 Create policy management permission sets:
   - Policy User permission set — Policy users have permission to create or edit policies and must submit the changes for review.
   - Policy Administrator permission set — Policy administrators have permission to approve and save new or changed policies or reject the changes.

2 Create policy management users:
   - Policy User — Create this user and assign the Policy User permission set.
   - Policy Administrator — Create this user and assign the Policy Administrator permission set.

3 Configure approval settings for policy changes on the **Approvals** pane of the **Server Settings** page.
   - Policy User — To require policy users to submit policy changes for review, select **Users need approval for policy changes**.
   - Policy Administrator — To require policy administrators to also submit policy changes for review, select **Administrators and Approvers need approval for policy changes**.

For more information, see the *McAfee ePolicy Orchestrator Product Guide*.

How the shared password is used

The *shared password* is the password that secures communication between Client Proxy and Web Gateway or McAfee WGCS. The shared password is sometimes called the *shared secret*.

Whether you are setting up Client Proxy in an on-premises, cloud-only, or hybrid deployment, one shared password secures communication across products and policies. Configuration details depend on the management platform.

Managed with McAfee ePO

1 Download your customer ID and the shared password from a Web Gateway server to an .xml file.

2 In the McAfee ePO interface, import your credentials from the .xml file on the **Client Configuration** page while configuring a Client Proxy policy.

Managed with McAfee ePO Cloud

1 In the McAfee ePO Cloud interface, configure the shared password on the **Client Configuration** page while configuring a Client Proxy policy.

2 To share your credentials manually, export your customer ID and the shared password to an .xml file.

Managed with MVISION ePO

1 Download your customer ID and the shared password from a Web Gateway server to an .xml file.

2 In the MVISION ePO interface, import your credentials from the .xml file on the **MCP Administration** page.

Hybrid deployment

1 In the McAfee ePO Cloud interface, configure the shared password and export your credentials to an .xml file.

2 In the McAfee ePO interface, import your credentials from the .xml file.

Considerations when changing the shared password (McAfee ePO Cloud)

When changing the shared password in the McAfee ePO Cloud interface, allow enough time for it to be updated in the system.

Updating the shared password involves these system actions and time estimates:

1 McAfee ePO Cloud deploys the updated Client Proxy policy to the endpoints in your organization. The time this action takes depends on the value configured for the **Policy enforcement interval** setting in your McAfee Agent policy.

2 The Client Proxy software on the endpoints shares the new password with McAfee WGCS. This action can take up to 20 minutes.

The shared password must be synchronized in McAfee WGCS, or authentication fails.

Import your customer ID and shared password (MVISION ePO)

When creating Client Proxy policies on MVISION ePO or migrating Client Proxy policies from on-premises to MVISION ePO, download the customer ID and shared password from a Web Gateway server to an .xml file and import the file on the **MCP Administration** page.

The migration of Client Proxy policies from on-premises to MVISION ePO is supported from Client Proxy on-premises 3.0.0 and later. For information about how to migrate McAfee ePO on-premises to MVISION ePO, see *Migration to MVISION ePO Quick Start Guide* on the McAfee product documentation portal *(docs.mcafee.com)*.

Task

1 From the MVISION ePO menu, select **Configuration** | **MCP Administration**.

2 Next to **Customer Identifier**, click **Choose File**. Navigate to the folder containing the .xml file, select it, and click **Open**.

The customer ID and shared password are imported to Client Proxy. All existing and new policies are updated with the imported customer ID and shared password.

Create a Common Catalog instance (McAfee ePO or McAfee ePO Cloud)

You can create a Common Catalog instance for Client Proxy, then select it when configuring the bypass list in a policy.

Before you begin
You must be logged on to the McAfee ePO or McAfee ePO Cloud server as an administrator.

Client Proxy catalog instances are globally available. You can associate each instance with more than one policy.

A Client Proxy catalog consists of lists of items that are grouped by these categories or types:

- Domain names
- Network addresses
- Network ports
- Process names

On the Common Catalog page, you can create and configure a catalog instance. You can view the lists of items in each category and add, edit, or remove items from the lists. Add as many lists to the catalog instance as you need.

Task

1. From the McAfee ePO or McAfee ePO Cloud menu, select **Policy** | **Policy Catalog**.
2. From the **Actions** drop-down list on the **Catalog List** page, select **New Catalog**.
3. Specify a name for the new catalog and an optional description, then click **OK**.
4. Under **Source / Destination** in the **Common Catalog** pane, select a category:
   - **Domain name** — Web traffic sent to the domains in this list bypasses the proxy server. Example: google.com
   - **Network Address (IP)** — Web traffic sent to the IP addresses in this list bypasses the proxy server. Addresses can be configured individually, as a range, or using a subnet.
     Examples include:
     - 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
   - **Network Port** — Web traffic sent to the ports in this list bypasses the proxy server. Examples: 40, 80, 400–500
   - **Process Name List** — Web traffic coming from the processes in this list bypasses the proxy server. A process runs on the endpoints. Windows process names must end with .exe. macOS process names don't require a file name extension. Add McAfee and other trusted processes to this list.
5. From the **Actions** drop-down list, select **New**.
6. Specify a unique name for the list or use the default name.
7. Click **Add** to add items to the list, then click **Save**.

   The list is added to the Common Catalog.

The Common Catalog instance is configured and saved.

Configure a policy

Contents

- *Create a Client Proxy policy*
- *How Client Proxy manages the proxy server list*
- *Configure the proxy server list*
- *Configure the alternate proxy server list*
- *Configure the client settings*
- *Configure the bypass list (McAfee ePO or McAfee ePO Cloud)*
- *Configure the alternate redirection list (McAfee ePO or McAfee ePO Cloud)*
- *Configure the bypass list (MVISION ePO)*
- *Configure the alternate redirection list (MVISION ePO)*
- *Import or export the bypass list (MVISION ePO)*
- *Import or export the alternate redirection list (MVISION ePO)*
- *Configure the block list*

Create a Client Proxy policy

A Client Proxy policy consists of a proxy server list, redirection settings, a bypass list, and a block list that together determine whether and where Client Proxy redirects web requests.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

You can create a new policy by using an existing policy as a template. As a template, the default policy is read-only and cannot be renamed, deleted, exported, imported, or assigned to the endpoints.

Task

1. From the main menu, select **Policy** | **Policy Catalog**.
2. From the **Products** list, select the current version of Client Proxy.
3. Click **New Policy**.
4. From the **Create a policy based on this existing policy** drop-down list, select an existing policy to use as a template for the new policy.
5. Specify a name for the new policy, then click **OK** to save it.

While configuring the first policy on Mac system with Big Sur 11.2 and later, an alert is prompted to allow McAfeeSystemExtensions Network adaptor. Click **Allow** to load McAfeeSystemExtensions. Client Proxy will not redirect traffic until you choose allow. You need to restart Client Proxy manually to view the consent pane again. For more information, see McAfee Knowledge Base article KB94092.

You can configure the new policy now or cancel the configuration and select and edit the policy from the **Policy Catalog** later.

How Client Proxy manages the proxy server list

The Client Proxy software maintains an ordered list of proxy servers.

The proxy server with the fastest response time is placed at the top of the list. The software updates the list from time to time.

For example, the list is updated when the user starts the computer or the Client Proxy policy changes. It is also updated if the VPN connection breaks or a proxy server fails to respond. At these times, the software tests the connections to all proxy servers and reorders the list based on response times.

If redirection to the proxy server at the top of the list fails, the software tries redirecting to the second proxy server in the list. At the same time, the software tests the proxy server connections again and updates the list.

When configuring how the Client Proxy software selects the next proxy server from the list, you have these options:

- **connect to the first accessible Proxy Server based on their order in the list below** — The software selects the next proxy server from the list that you configure.
- **connect to the Proxy Server that has the fastest response time** — The software selects the next proxy server from the list that it maintains, which is based on response time.

Auto-proxy switchover

When this option is enabled, the software checks the proxy server list at the interval you specify. If a higher priority proxy server is available, the software automatically switches to it.

The auto-proxy switchover option is available only when **connect to the first accessible Proxy Server based on their order in the list below** is selected.

Configure the proxy server list

To redirect web traffic to a proxy server, configure the proxy server list and rules.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

When configuring the proxy server list, consider whether Client Proxy is deployed with McAfee ePO, McAfee ePO Cloud, or MVISION ePO.

- **On-premises** — Configure at least one of the Web Gateway appliances installed on your network as the proxy server.
- **In the cloud** — Configure McAfee WGCS as the proxy server, using this format for the host name: c<customer_id>.saasprotection.com.

  Example: c12345678.saasprotection.com

Before you can save the policy, you must provide the IP address or host name of at least one proxy server and a port number.

When you enable the **Secure Channel** setting with at least one cloud proxy configured in the proxy server list, Client Proxy ignores on-premise proxy servers and considers only cloud proxy servers in the list. Depending on the availability of cloud proxy server and port, Client Proxy applies redirect, block, or fallback (Allow Connection without Secure Channel) option. Proxies with domains like c*******.wgcs.mcafee-cloud.com and c*******.saasprotection.com are considered as cloud proxies.

Task

1 From the main menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** menu, select **Proxy Servers**.

6 To specify how the software selects a proxy server from the list, select an option:

- **connect to the first accessible Proxy Server based on their order in the list below** — The software selects the next proxy server from the list that you configure.
- **connect to the Proxy Server that has the fastest response time** — The software selects the next proxy server from the list that it maintains, which is based on response time.

7 To add proxy servers to the **Proxy Server List**, configure these settings, then click **Add**.

- **Proxy Server Address** — Specifies the IP address or host name of the proxy server.
- **Proxy Port** — Specifies the port number of the proxy server.
- **HTTP/HTTPS** — Select this checkbox to redirect traffic sent to ports 80 and 443 to a proxy server.
- **Non-HTTP/HTTPS Redirected Ports** — Specifies the port numbers of protocols other than HTTP/HTTPS whose traffic you want redirected. Verify that the proxy server supports these protocols. You can enter up to 1024 characters in this field.

8 Select **Enable Auto proxy switch over**, then specify a value for the **Polling interval** in this range: 10–3600 seconds. The recommended value is 60 seconds.

The auto-proxy switchover option is available only when **connect to the first accessible Proxy Server based on their order in the list below** is selected.

While using the **Secure Channel** feature, the **Enable Auto proxy switch over** setting is not applicable for a proxy server list.

9 In the **Specify additional ports that you would like to redirect as HTTP/HTTPS traffic** field, specify the numbers of other ports whose traffic you want redirected like HTTP/HTTPS traffic. For example, you can redirect traffic sent to an application. You can enter up to 1024 characters in this field.

10 Optionally, select **Block Traffic on configured Ports if none of the Primary Proxy servers is reachable**.

When none of the configured proxy servers can be reached, all traffic to the configured ports and default ports 80 and 443 is blocked.

11 Select **Block Traffic on configured Ports until MCP is Ready** to protect the endpoint while Client Proxy is starting.

All traffic to the configured ports and default ports 80 and 443 is blocked from the time the user has internet access until Client Proxy exits bypass mode and starts redirecting traffic.

12 Select **Block IPv6 Traffic on configured Ports** to require web browsers to fall back to IPv4.

13 Select **Block Traffic when Mutual Authentication with Primary Proxy Failed** to make sure that Client Proxy only redirects web requests when it can authenticate the proxy server.

14 Deselect **Bypass proxy server for local addresses** to redirect all traffic, including traffic sent to local addresses inside your organization's subnet network, to a proxy server. You can configure an IP address, IP address range, subnet, or CIDR. For example, 192.168.1.1, 172.31.255.10-172.31.255.20, 10.50.0.0/255.255.128.0 or 10.50.0.0/17.

15 Select **Block UDP Traffic on Ports 80/443 for IPv4 and IPv6** to block this traffic.

16 Click **Save**.

The proxy servers list is saved with the policy.

Configure the alternate proxy server list

You can configure alternate proxy servers and split the selected web traffic to multiple proxy servers. When an alternate proxy server is down and primary is available, Client Proxy redirects all traffic to the primary proxy server. When a primary proxy server is down, Client Proxy redirects the traffic marked for alternate redirection to the alternate proxy server.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

When configuring the proxy server list, consider whether Client Proxy is deployed with McAfee ePO, McAfee ePO Cloud, or MVISION ePO.

- **On-premises** — Configure at least one of the Web Gateway appliances installed on your network as the proxy server.
- **In the cloud** — Configure McAfee WGCS as the proxy server, using this format for the host name: c<customer_id>.saasprotection.com.

  Example: c12345678.saasprotection.com

Before you can save the policy, you must provide the IP address or host name of at least one proxy server and a port number.

Task

1 From the main menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** menu, select **Proxy Servers**.

6 Click the **Alternate Proxy Server List** tab.

7 To specify how the software selects a proxy server from the list, select an option:

- **connect to the first accessible Proxy Server based on their order in the list below** — The software selects the next proxy server from the list that you configure.
- **connect to the Proxy Server that has the fastest response time** — The software selects the next proxy server from the list that it maintains, which is based on response time.

8 To add proxy servers to the **Proxy Server List**, configure these settings, then click **Add**.

- **Proxy Server Address** — Specifies the IP address or host name of the proxy server.
- **Proxy Port** — Specifies the port number of the proxy server.

- **HTTP/HTTPS** — Select this checkbox to redirect traffic sent to ports 80 and 443 to a proxy server.
- **Non-HTTP/HTTPS Redirected Ports** — Specifies the port numbers of protocols other than HTTP/HTTPS whose traffic you want redirected. Verify that the proxy server supports these protocols. You can enter up to 1024 characters in this field.

9 Select **Enable Auto proxy switch over for Alternate Proxy**, then specify a value for the **Polling interval (in seconds)** in this range: 10–3600 seconds. The recommended value is 60 seconds.

The auto-proxy switchover option is available only when **connect to the first accessible Proxy Server based on their order in the list below** is selected.

10 Click **Save**.

The alternate proxy servers list is saved with the policy.

Configure the client settings

Configure the settings that Client Proxy uses to determine the location of the endpoint and when to redirect web traffic. The client software tests for connectivity by using a TCP three-way handshake to connect, then closing the connection. The endpoint can be located inside the network, outside the network, or connected to the network by VPN.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

Before you can save the policy, you must provide values for the customer ID and shared password.

Task

1 From the main menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** list, select **Client Configuration**.

6 Select an option based on your management platform:

- McAfee ePO — In the **Customer Identifier** section, click **Browse** to locate, then open the customer ID .xml file provided by the Web Gateway or McAfee WGCS administrator. The values in this file automatically populate the **Unique Customer ID** and **Shared Password** fields.
- McAfee ePO Cloud — In the **Configure Shared Password** section, enter and confirm the password that Client Proxy shares with McAfee WGCS. You also have the options of resetting or exporting the password.
- MVISION ePO — Before creating Client Proxy policies on MVISION ePO or migrating policies to MVISION ePO, import your customer ID and shared password on the **MCP Administration** page. After you import them successfully, all existing and new Client Proxy policies are updated with the imported customer ID and shared password.

The migration of Client Proxy policies from on-premises to MVISION ePO is supported from Client Proxy on-premises 3.0.0 and later. For information about how to migrate McAfee ePO on-premises to MVISION ePO, see *Migration to MVISION ePO Quick Start Guide* on the McAfee product documentation portal *(docs.mcafee.com)*.

7 Select a **Secure Channel for Cloud Proxies** setting:

This option is applicable only for McAfee WGCS.

- **Enable Secure Channel** — Select this checkbox to establish a secure connection between Client Proxy and McAfee WGCS. When you select this checkbox, the software validates the cloud proxy certificate against the device certificate store and establishes a secure connection.

  When you enable **Secure Channel**, Client Proxy uses the 8081 port to check cloud proxy connectivity. However, you can continue to configure the 8080 port and proxy server hostname when adding a cloud proxy server.

- **Block If Validation Failed** — Select this checkbox to block traffic to the cloud proxy server when the certificate validation fails.

  When the certification validation for a proxy server fails, then traffic to that proxy (primary or alternate) server is blocked.

- When you have connectivity issues with port 8081 (Secure Channel port), you can decide whether to allow or block the connection. Select one of the following:
  - **Block Connection** — Select this to block the connection.

    When the certification validation for a proxy server fails, then traffic to that proxy (primary or alternate) server is blocked.

  - **Allow Connection without Secure Channel** — Select this to allow the connection through the configured proxy port (8080) without establishing a secure connection between Client Proxy and McAfee WGCS.

    When you select this option, all the configured (both on-premise and cloud) proxy servers are considered for filtering traffic. The order to select a proxy server depends on the option you have selected (**connect to the first accessible Proxy Server based on their order in the list below** or **connect to the Proxy Server that has the fastest response time**) while configuring the proxy server list.

8 Select a **Traffic Redirection** setting:

- **Redirect network traffic when computer is not connected to corporate network and not working through VPN** — Redirects web requests to a proxy server when users are working outside your organization's network and are not connected by VPN.
- **Always redirect network traffic to proxy servers** — Redirects all web requests to a proxy server, including requests from users working inside the network, outside the network, or working connected to the network by VPN.

9 Select a **Corporate Network Detection** setting:

- **by testing connectivity to ePO** — If the client software can connect to the McAfee ePO server, the endpoint is located inside the network.
- **by testing connectivity to any of the following corporate servers** — If the client software can connect to the configured network servers, the endpoint is located inside the network.

10 To configure **Corporate VPN Detection**, specify the addresses and port numbers of one or more VPN servers. If the client software can connect to a configured VPN, the endpoint is connected to the network by VPN.

11 Using regular expressions, configure the **Active Directory Groups Filter** to limit the groups in the header that the client software adds to web requests before redirecting them to the proxy server. Group membership information must not exceed 4096 characters.

Format: <domain_name>\\<group_name>

12 (macOS) Select a **Log File** setting:

- **Log messages with Error and Critical priority**
- **Log messages with Error, Critical, Information, and Warning priority**
- **Log all messages (recommended for troubleshooting and debugging)**
- **Don't log any messages**

On endpoints running Windows, log files are located in this folder: C:\Program Data\McAfee\MCP\Logs. Critical error messages are saved to a file named Mcp.log.

13 (Windows) Configure the **Access Protection** settings:

- **Enable access protection** — When selected, users cannot disable the client software using Windows Task Manager, edit or delete files, and change registry values.
- **Request release key for manual uninstall** — When selected, users can request a release code from an administrator and use it to uninstall the client software. When deselected, users must use the Windows uninstall feature to uninstall the software. Best practice is to use a release code to uninstall the software.

14 Click **Save**.

The client settings are saved with the Client Proxy policy.

Configure the bypass list (McAfee ePO or McAfee ePO Cloud)

The Client Proxy policy allows web traffic that matches the items on the bypass list to bypass the proxy server and go directly to the Internet.

Before you begin

You must be logged on to the McAfee ePO or McAfee ePO Cloud server as an administrator.

If the Common Catalog instance you want to associate with this policy does not exist, you must create it before configuring the bypass list.

Task

1 From the McAfee ePO or McAfee ePO Cloud menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** menu, select **Bypass List**.

6 From the **Common Catalog** drop-down list in the **Bypass List** pane, select a Common Catalog instance.

7 Add list items from the catalog to the bypass list:

a From the **Actions** drop-down list, select **Add bypass list item**, then select a category.

b In the **Choose from existing values** dialog box, select the list items you want to add to the bypass list.

c (Optional) Edit an existing list item or add a new one.

Changes you make in this step apply to all policies that share this instance of the Common Catalog.

d Click **OK**.

The dialog box closes, and the selected list items are added to the bypass list.

8 (Optional) Edit or remove items in the bypass list.

9 Click **Save**.

The bypass list and Common Catalog instance are saved with the policy.

Configure the alternate redirection list (McAfee ePO or McAfee ePO Cloud)

You can configure domain names, network addresses, network ports, and process names in the alternate redirection list to redirect web traffic to the alternate redirection proxy server. You can view the lists of items added to the alternate redirection list and add, edit, or remove items from the lists as you need.

Before you begin

You must be logged on to the McAfee ePO or McAfee ePO Cloud server as an administrator.

If the Common Catalog instance you want to associate with this policy does not exist, you must create it before configuring the alternate redirection list.

Task

1 From the McAfee ePO or McAfee ePO Cloud menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** menu, select **Alternate Redirection List**.

6 From the **Common Catalog** drop-down list in the **Alternate Redirection List** pane, select a Common Catalog instance.

7 Add list items from the catalog to the alternate redirection list:

a From the **Actions** drop-down list, select **Add Alternate Redirection**, then select a category.

b In the **Choose from existing values** dialog box, select the list items you want to add to the alternate redirection list.

c (Optional) Edit an existing list item or add a new one.

Changes you make in this step apply to all policies that share this instance of the Common Catalog.

d Click **OK**.

The dialog box closes, and the selected list items are added to the alternate redirection list.

8 (Optional) You can edit or remove items in the alternate redirection list.

9 Click **Save**.

The alternate redirection list and Common Catalog instance are saved with the policy.

10 (Optional) Click **Duplicate** to duplicate the selected Client Proxy policy.

Configure the bypass list (MVISION ePO)

You can configure domain names, network addresses, network ports, and process names in the bypass list. You can view the lists of items added to the bypass list and add, edit, or remove items from the lists as you need.

Before you begin

You must be logged on to the MVISION ePO server as an administrator.

Task

1. From the MVISION ePO menu, select **Policy** | **Policy Catalog** | **McAfee Client Proxy**.
2. Click **MCP Policy** to view the policy list.
3. Click **Edit** on the same row as the policy you want to configure.
4. Under **Client Proxy Settings**, click **Bypass List**.
5. In the **Bypass List** pane, select a category:
   - **Domain name** — Enter the domain name and click **Add**. The web traffic sent to the domains in this list bypasses the proxy server. Example: google.com
   - **Network Address (IP)** — Enter the network IP address and click **Add**. The web traffic sent to the IP addresses in this list bypasses the proxy server. Addresses can be configured individually, as a range, using a subnet or CIDR.

     Examples include:
     - 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
   - **Network Port** — Enter the port number, its description and click **Add**. The web traffic sent to the ports in this list bypasses the proxy server. Examples: 40, 80, 400–500
   - **Process List** — Enter the process name and click **Add**. The web traffic coming from the processes in this list bypasses the proxy server. A process runs on the endpoints. Windows process names must end with .exe. macOS process names don't require a file name extension. Add McAfee and other trusted processes to this list.
6. Click **Save**.
7. Optionally, click **Duplicate** to duplicate a policy.

Configure the alternate redirection list (MVISION ePO)

You can configure domain names, network addresses, network ports, and process names in the alternate redirection list to redirect web traffic to the alternate redirection proxy server. You can view the lists of items added to the alternate redirection list and add, edit, or remove items from the lists as you need.

Before you begin

You must be logged on to the MVISION ePO server as an administrator.

Task

1. From the MVISION ePO menu, select **Policy** | **Policy Catalog** | **McAfee Client Proxy**.
2. Click **MCP Policy** to view the policy list.

3 Click **Edit** on the same row as the policy you want to configure.

4 Under **Client Proxy Settings**, click **Alternate Redirection List**.

5 In the **Alternate Redirection List** pane, select a category:

- **Domain name** — Enter the domain name and click **Add**. The web traffic sent to the domains is redirected to the alternate proxy server. Example: google.com
- **Network Address (IP)** — Enter the network IP address and click **Add**. The web traffic sent to the IP addresses is redirected to the alternate proxy server. Addresses can be configured individually, as a range, using a subnet or CIDR.

  Examples include:

  - 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
- **Network Port** — Enter the port number, its description and click **Add**. The web traffic sent to the ports is redirected to the alternate proxy server. Examples: 40, 80, 400–500
- **Process List** — Enter the process name and click **Add**. The web traffic coming from the processes is redirected to the alternate proxy server. A process runs on the endpoints. Windows process names must end with .exe. macOS process names don't require a file name extension. Add McAfee and other trusted processes to this list.

6 Click **Save**.

7 Optionally, click **Duplicate** to duplicate a policy.

Import or export the bypass list (MVISION ePO)

You can use the import and export options to copy the bypass lists. After you import or export the bypass list, you can add, edit, and remove the bypass list items. It is a good practice to export the existing bypass list, modify it, and import the file again. Importing a bypass list overwrites all the existing bypass entries. Only .txt file format is supported for import or export options.

The following is a sample list of items in the bypass list:

```
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
```

You can add port numbers without any descriptions, and process name is the name of the Windows or macOS process.

Task

1 From the MVISION ePO menu, select **Policy** | **Policy Catalog** | **McAfee Client Proxy**.

2 Click **MCP Policy** to view the policy list.

3 Click **Edit** on the same row as the policy for which you want to import or export the bypass list.

4 Under **Client Proxy Settings**, click **Bypass List**.

5 In the **Bypass List** pane, do the following:

- To export a bypass list, click **Export Bypass List**. The browser downloads the bypass list as a .txt file.
- To import a bypass list, click **Import Bypass List**.
  - In the dialog box, click **Choose File** to navigate to the folder containing the bypass list file. Select the file, then click **Open**. A confirmation message appears after importing the bypass list.

Make sure that the list of items in the bypass list is in the correct format. If the import fails, the **Import Bypass List** dialog box returns the line number at which the error has occurred. After fixing the errors, you can import the file again.

6 Click **Save**.

Import or export the alternate redirection list (MVISION ePO)

You can use the import and export options to copy the alternate redirection lists. After you import or export the alternate redirection list, you can add, edit, and remove the domain names configured in the alternate redirection list. It is a good practice to export the existing alternate redirection list, modify it, and import the file again. Importing an alternate redirection list overwrites all the existing alternate redirection entries. Only .txt file format is supported for import or export options.

The following is a sample alternate redirection list:

```
type = DOMAIN

google.com
intel.com
```

Task

1 From the MVISION ePO menu, select **Policy** | **Policy Catalog** | **McAfee Client Proxy**.

2 Click **MCP Policy** to view the policy list.

3 Click **Edit** on the same row as the policy for which you want to import or export the alternate redirection list.

4 Under **Client Proxy Settings**, click **Alternate Redirection List**.

5 In the **Alternate Redirection List** pane, do the following:

- To export the alternate redirection list, click **Export Alternate Redirection List**. The browser downloads the alternate redirection list as a .txt file.
- To import the alternate redirection, click **Import Alternate Redirection List**.
  - In the dialog box, click **Choose File** to navigate to the folder containing the alternate redirection list file. Select the file, then click **Open**. A confirmation message appears after importing the alternate redirection list.

Make sure that the list of domain names in the alternate redirection list is in the correct format. If the import fails, the **Import Alternate Redirection List** dialog box returns the line number at which the error has occurred. After fixing the errors, you can import the file again.

6 Click **Save**.

Configure the block list

Each Client Proxy policy is associated with a list of blocked processes.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

A process list is a list of processes that run on the endpoints. Windows process names must end with .exe. macOS process names don't require a file name extension.

To reduce the amount of traffic that is redirected to the proxy server for filtering, configure a list of endpoint processes that are blocked from accessing the network.

Task

1 From the main menu, select **Policy** | **Policy Catalog**.

2 From the **Products** list, select the current version of Client Proxy.

3 Click **MCP Policy** to view the policy list.

4 Click **Edit** on the same row as the policy you want to configure.

5 From the **Client Proxy Settings** menu, select **Block List**.

6 Select an option:

- **Allow traffic to go directly to destination** — All processes are allowed to access the Internet without going through a proxy server.
- **Block traffic for all processes (except bypass listed processes)** — All processes are blocked from accessing the Internet except for processes on the bypass list.
- **Block traffic only for the following processes** — All processes are allowed to access the Internet without going through a proxy server except for the ones on this list. Configure the list using the **Add**, **Edit**, and **Delete** functions.

7 Click **Save**.

The block list is saved with the Client Proxy policy.

Assign a policy to the endpoints

You can assign a Client Proxy policy to your endpoints using McAfee ePO, McAfee ePO Cloud, or MVISION ePO.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

Task

1. From the main menu, select **Policy** | **Policy Catalog**.
2. Select the organizational level where you want the policy assigned.

   To select all endpoints managed by your platform, select **My Organization**.
3. Click **Assigned Policies**.
4. From the **Product** drop-down list, select the current version of McAfee Client Proxy.
5. In the **Actions** column, click **Edit Assignment** on the same line as the policy you want to assign.
6. For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
7. From the **Assigned policy** drop-down list, select the policy.
8. Select an option for **Lock policy inheritance**:
   - **Unlocked** — A different policy can be assigned to one or more subgroups.
   - **Locked** — This policy must be assigned to all subgroups.
9. Click **Save**.

The policy is assigned to your endpoints.

Export a policy to an .xml or .opg file

Export a Client Proxy policy from McAfee ePO, McAfee ePO Cloud, or MVISION ePO to an .xml or .opg file.

Before you begin

You must be logged on to the McAfee ePO, McAfee ePO Cloud, or the MVISION ePO server as an administrator.

For standalone computers that are not managed with McAfee ePO or McAfee ePO Cloud, you must export the policy to an .opg file and save the file locally on your computers.

Task

1. From the main menu, select **Policy** | **Policy Catalog**.
2. From the **Products** list, select the current version of Client Proxy.
3. Click **MCP Policy** to view the policy list.
4. Click **Edit** on the same row as the policy you want to configure.
5. From the **Actions** drop-down list, select **Export Policy to File**.

6 Right-click the policy file you want downloaded, then click **Save** | **OK**.
   - **McAfee Client Proxy Policy Server File** — Exports the Client Proxy policy to an .xml file that you can use for troubleshooting.
   - **McAfee Client Proxy Policy Client File** — Exports the Client Proxy policy to an .opg file that you can save on your standalone or endpoint computers.

7 Rename the .opg file to MCPPolicy.opg, then copy it to this location on the client computers:
   - Windows-based computers — C:\ProgramData\McAfee\MCP\Policy\Temp
   - macOS computers — /usr/local/mcafee/mcp/policy

When Client Proxy starts running on the standalone or endpoint computers, it loads the policy and begins redirecting traffic.

Suspend policy enforcement on a Windows-based or macOS computer

If a user needs to access or transfer sensitive information for an approved business reason, you can suspend policy enforcement on a standalone or endpoint computer running Windows or macOS.

To suspend policy enforcement, follow the challenge-response protocol provided by the Help Desk software.

Task

1 **User** — Opens the **Enter Release Code** dialog box:
   - Windows — From the **Start** menu, clicks **McAfee** | **Bypass McAfee Client Proxy**.
   - macOS — From the McAfee menulet on the status bar, selects **Console**, then select **Client Proxy**.

   ⚠ While waiting for the release code, the user must leave the dialog box open. If the box is closed, the procedure must be started over.

2 **User** — Sends you an email that includes:
   - User name and email address
   - **Policy Name and Policy Revision** number (copied from the **Enter Release Code** dialog box)
   - **Identification** code (copied from the **Enter Release Code** dialog box)

3 **Administrator** — Using the Help Desk software and the values provided by the user, generates the release code and sends it to the user. On MVISION ePO, you can generate release code on the **MCP Administration** page.

4 **User** — Enters the release code in the **Release** field, then clicks **OK** (Windows) or **Release** (macOS).

Policy enforcement is suspended for the time period you specified when you generated the release code.

3 Queries and reports

Contents

- *Create and run a database query (McAfee ePO)*
- *Create a Client Proxy report (McAfee ePO or MVISION ePO)*

Create and run a database query (McAfee ePO)

Create and run a database query to return information about client tasks and policies.

Before you begin

You must be logged on to the McAfee ePO server as an administrator.

A McAfee ePO Cloud administrator can run queries, but not create them.

Task

1 From the McAfee ePO menu, select **Reporting** | **Queries & Reports**.

2 From the **Groups** menu, select **McAfee Groups** | **McAfee Client Proxy**, then click **New Query**.

3 In the **Query Builder**: From the **Feature Group** list, select **Policy Management**.

4 Select a **Result Type**, then click **Next**:

- **Applied Client Tasks** — Returns the names of client tasks and the organizational levels where they were applied.
- **Applied Policies** — Returns the names of policies and the organizational levels where they were applied.
- **Client Task Assignment Broken Inheritance** — Returns the names of client tasks and the organizational levels where task assignments were broken.
- **Policy Assignment Broken Inheritance** — Returns the names of policies and the organizational levels where policy assignment was broken.

The **Chart** page opens.

5 Configure how you want the query results displayed in chart format:

a Select a chart type.

b Specify labels, units, sort orders, and other values as needed.

c Click **Next**.

The **Columns** page opens.

6 Configure how you want the query results displayed in table format, then click **Next**:
   - In the **Available Columns** menu, click column names to select them.
   - In the **Selected Columns** pane, close columns to remove them.
   - To reorder selected columns, drag and drop them or use the arrow keys.

   The **Filter** page opens.

7 Configure how you want the query results filtered:
   a In the **Available Properties** menu, click property names to select them.
   b From the **Comparison** drop-down list, select an operator for each property.
   c For each operator, select a value.

8 Click **Run** to see the query results, then click **Edit Query** to make changes as needed.

9 Click **Save**, then on the **Save Query** page:
   a Specify a name and optional description for the query.
   b Select an existing group or specify a new group.
   c Click **Save**.

The database query is saved for later use.

Create a Client Proxy report (McAfee ePO or MVISION ePO)

Output in .pdf format the number of endpoints where Client Proxy installation succeeded or failed in the past month.

Before you begin

You must be logged on to the McAfee ePO or MVISION ePO server as an administrator.

Task

1 From the McAfee ePO or MVISION ePO menu, select **Reporting** | **Queries & Reports**.

2 From the **Groups** list, select **McAfee Groups** | **McAfee Client Proxy**.

3 Click the **Reports** tab, then click **New Report**.

4 From the **Toolbox**, drag one or more templates to the **Report Layout** area, then configure and position them:
   - **Image**
   - **Page Break**
   - **Query Chart**
   - **Query Table**
   - **Text**

When adding a query chart or table, select **MCP: Endpoint Install Success/Failed events in last month** from the **Query** drop-down list.

5 To customize the report, click these options:
   - **Header and Footer**
   - **Page Setup**
   - **Runtime Parameters**

6 Click **Run** to view the report in .pdf format.

7 Click **Save**, then on the **Name, Description and Group** dialog box:
   a Specify a name and optional description for the report.
   b Select an existing group or specify a new group.
   c Click **OK**.

The Client Proxy report is saved and can be run again.