Deployment Guide

McAfee Web Protection Hybrid

Deploying the hybrid solution

A McAfee® Web Protection license provides all components needed to set up McAfee® Web Gateway and McAfee® Web Gateway Cloud Service (McAfee® WGCS) in a hybrid deployment.

The Web Protection hybrid deployment is also known as the hybrid solution.

What is the hybrid solution?

Organizations that have a Web Gateway appliance installed on the network and are using McAfee WGCS can manage one Web Protection policy for both and apply it across the organization.

The Web Protection policy is configured in the Web Gateway interface and pushed to McAfee WGCS at the synchronization interval you specify. Together, the on-premise and cloud components protect your organization from threats that might arise when users access the web from inside or outside your network.

In addition to Web Gateway and McAfee WGCS, hybrid components include:

- McAfee® Client Proxy
- McAfee® Content Security Reporter
- McAfee® ePolicy Orchestrator® Cloud (McAfee® ePO™ Cloud)
- McAfee® ePolicy Orchestrator® (McAfee® ePO™)

Components of the hybrid solution

The hybrid solution integrates McAfee components installed on your network with McAfee cloud services.

If you require a hardware platform to run Web Gateway, the hardware is a separate purchase.

Components of the hybrid solution include:

- Web Gateway — This hardware-based or virtual appliance is installed locally on your organization's network. The on-premise appliance protects your network from threats that might arise when users access the web from inside the network. The appliance has its own interface, where administrators manage the product.
- McAfee WGCS — This cloud service protects your network from threats that might arise when users access the web from inside or outside the network. The service is managed with McAfee ePO Cloud.
- Client Proxy — This software, when installed on the endpoint, is aware of the user's location and redirects network traffic or lets it pass, accordingly:
  - Inside the network or connected to the network by VPN — Client Proxy lets network traffic pass to Web Gateway for filtering.
  - Outside the network — Client Proxy redirects network traffic to McAfee WGCS for filtering.

  Client Proxy can be managed with McAfee ePO, McAfee ePO Cloud, or both depending on the setup.
- Content Security Reporter — This extension, which is managed with McAfee ePO, allows you to view web traffic and usage trends consolidated from Web Gateway and McAfee WGCS logs.
- McAfee ePO — This management platform, which is installed on your network, allows you to manage Client Proxy and Content Security Reporter.
- McAfee ePO Cloud — This cloud-based management platform allows you to manage McAfee WGCS and Client Proxy.

How the hybrid components are managed

This table summarizes how the hybrid components are managed with McAfee ePO and McAfee ePO Cloud.

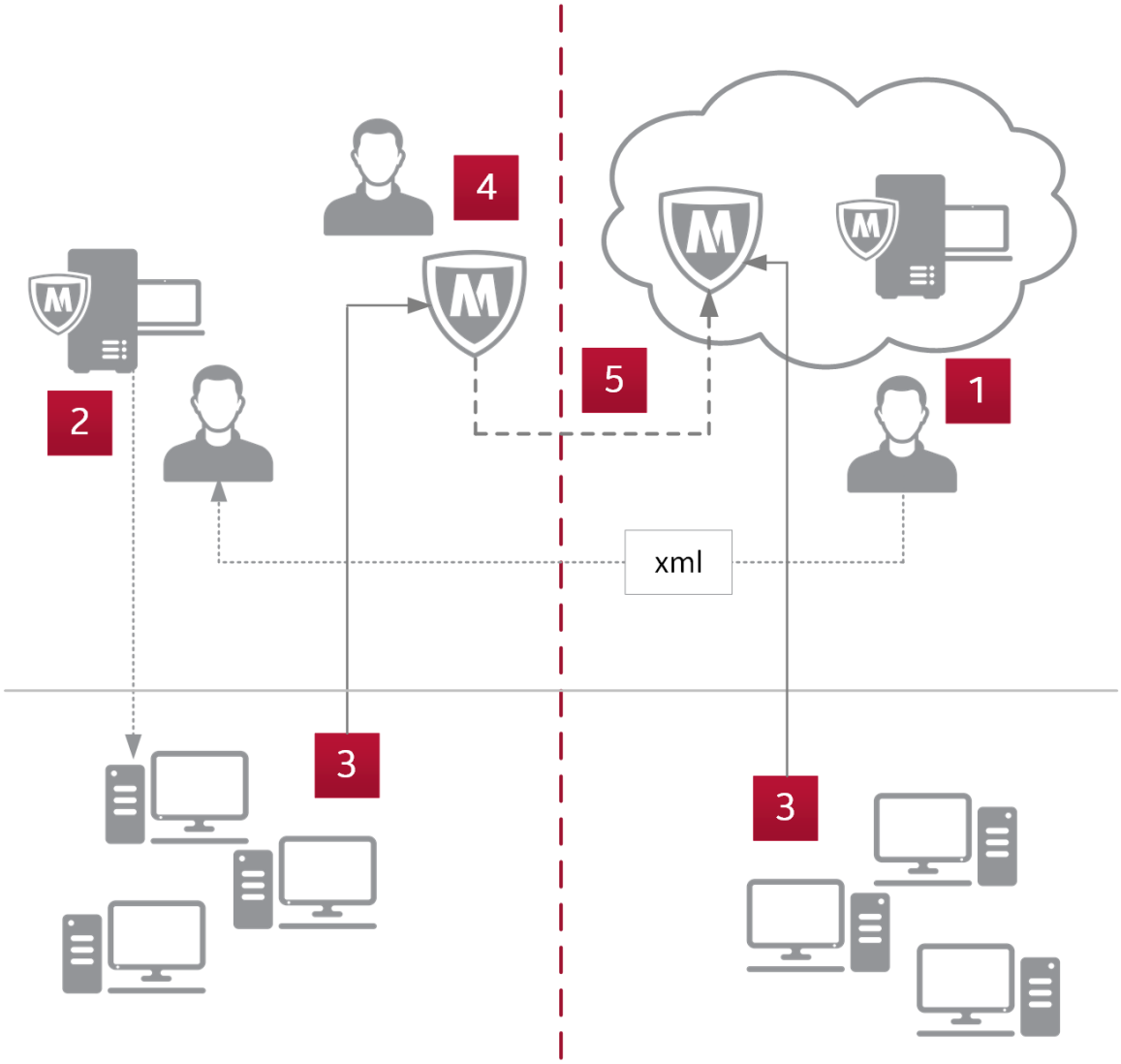
Hybrid component	Managed with McAfee ePO	Managed with McAfee ePO Cloud
Web Gateway	no	no
McAfee WGCS	no	yes
Client Proxy	yes	yes
Content Security Reporter	yes	no

How the hybrid solution works

The on-premise and cloud components of the hybrid solution work together to protect your organization from threats that might arise when users access the web from inside or outside the network.

After the solution is configured and enabled, the Web Gateway policy is pushed to the cloud at the specified synchronization interval. The **Policy Browser** interface, where the McAfee WGCS policy is configured in the McAfee ePO Cloud management console, is disabled. A **Policy Unavailable** message displays information about the hybrid synchronization, such as the date and time of the last sync.

The following diagram shows how the key hybrid components are set up and connected. The diagram assumes that Client Proxy is managed with McAfee ePO and that the Client Proxy software is already installed on the McAfee ePO server and the endpoint.



Inside your organization's network **Outside your organization's network**

Client Proxy credentials are configured using McAfee ePO Cloud, then exported and shared with McAfee ePO through an .xml file. These steps ensure that the Client Proxy policy is synchronized on premise and in the cloud.

1 Using the McAfee ePO Cloud management console, the administrator configures the Client Proxy shared password and exports the Client Proxy credentials to an .xml file.

2 Using the McAfee ePO management console, the administrator imports the Client Proxy credentials from the .xml file, then creates a Client Proxy policy for use with the hybrid solution. The administrator assigns the policy to all managed endpoints in the organization.

The administrator can configure multiple policies and assign each one to a different group of managed endpoints. Managed endpoints are the endpoint computers that you manage with McAfee ePO or McAfee ePO Cloud.

3 Managed endpoints can be located inside your organization's network, connected to your network by VPN, or located outside your network. A typical Client Proxy policy redirects web requests made by users inside your network (or connected by VPN) to a Web Gateway appliance installed on your network. For users working outside your network, a typical policy redirects web requests to McAfee WGCS.

4 In the Web Gateway interface, the administrator reviews the Web Protection policy and enables the rule sets to be pushed to the cloud.

5 In the Web Gateway interface, the administrator configures and enables the hybrid solution. When the deployment is enabled, the Web Gateway policy is pushed to the cloud at the specified synchronization interval. The **Policy Browser** interface in the McAfee ePO Cloud management console is disabled.

The hybrid solution doesn't change how the Client Proxy policy is applied. The Client Proxy software installed on the endpoint continues redirecting web requests as before.

Cloud-only vs. hybrid deployments

The type of deployment, cloud-only or hybrid, determines how the Web Protection policy is managed for users working outside the network.

- Cloud-only deployment — The McAfee WGCS policy is configured in the **Policy Browser** and saved in the policy store.
- Hybrid deployment — When the on-premise policy, which is configured in the Web Gateway interface, is pushed to the cloud, it overwrites the McAfee WGCS policy saved in the policy store.

After hybrid synchronization is enabled in the Web Gateway interface, it can't be disabled and the McAfee WGCS policy, which is overwritten, can't be restored. But you can manually control when the on-premise policy is synchronized with the cloud.

Setting up the hybrid components

After the initial setup of hybrid components is complete, you can configure the solution in the Web Gateway interface.

We recommend setting up the hybrid components in this order.

1 Web Gateway — Install and set up a new instance of the appliance or use an existing instance.

2 McAfee ePO — Install and set up a new McAfee ePO server or use an existing server. Use McAfee ePO to manage the on-premise components of the hybrid solution.

3 McAfee ePO Cloud — This cloud platform features a management console, where you can manage McAfee WGCS and Client Proxy policies. After creating an account in McAfee ePO Cloud, you can use the management console to set up the other products.

4 McAfee WGCS — McAfee hosts and updates this service in the cloud. Because it is a cloud service, you do not need to install or upgrade the software. To access the interface in the management console, you use your McAfee ePO Cloud credentials.

5 McAfee Client Proxy — Setup depends on whether you are using McAfee ePO or McAfee ePO Cloud. For both management platforms, deploy the client software to the managed endpoints in your organization, configure a Client Proxy policy, and push the policy to the endpoints.

6 Content Security Reporter — Install the extension on the McAfee ePO management platform, where you configure reporting and view reports.

Look up the hybrid-compatible versions of Web Gateway

Before you download the software, look up the versions of Web Gateway that are compatible with a hybrid deployment.

McAfee WGCS can be deployed in hybrid mode with Web Gateway versions in this range: 7.4.2–x.y.z. You can look up the latest version in this range, as follows.

Task

1 To open the **Web Gateway Cloud Service** status page, go to: https://trust.mcafee.com.

2 From the **Setup** drop-down list, select **Hybrid Mode**.

The **Hybrid Mode** window displays the latest version of Web Gateway that can be deployed with McAfee WGCS in a hybrid mode, for example, 7.7.1.

3 Click **Close**.

Locate and download the on-premise software

Before setting up the hybrid solution, locate and download the on-premise software.

Task

1 Download the Web Gateway software:

a To open the **Content & Cloud Security Portal**, click https://contentsecurity.mcafee.com.

b From the **Products** drop-down list, select a Web Gateway version, then select **Downloads**.

2 Download the McAfee ePO, Client Proxy, and Content Security Reporter software:

a To open the **McAfee Business ServicePortal**, click https://support.mcafee.com.

b Click **Patches and Downloads** | **Product Downloads**, then click **Download**.

c Enter your grant number and the characters displayed, then click **Submit**.

Setting up Web Gateway

You can set up Web Gateway as a physical appliance on a hardware platform or as a virtual appliance on a virtual machine on a host system.

After completing the setup, you are ready to administer Web Gateway. For more information about the individual setup steps, see the *McAfee Web Gateway Installation Guide*.

1 Verify the setup requirements.

2 Review the default configuration settings.

3 Install the appliance software according to the appliance type.

- **Physical appliance with pre-installed software** — Connect and turn on the appliance.
- **Physical appliance with downloaded software** — Download the software in ISO or USB format from the **Content & Cloud Security Portal**. Copy the software to an installation medium. Connect the appliance, insert the installation medium, then turn on the appliance. Use the Boot Manager to install the software.
- **Virtual appliance** — Download the software in ISO format from the **Content & Cloud Security Portal** and copy it to an installation medium. Insert the installation medium into a suitable host system. Create a virtual machine on the host system and start the new virtual machine.

4 Customize the default configuration settings.

5 Log on to the Web Gateway interface.

6 Review the online documents and import a license.

7 Activate the product.

For information about upgrading an existing Web Gateway installation, see the release notes that are provided with each new version.

McAfee ePO management platforms

McAfee ePO and McAfee ePO Cloud provide platforms and consoles for managing all on-premise and cloud components of the hybrid solution except for Web Gateway.

McAfee ePO

After installing and setting up McAfee ePO locally on your network, you can use the McAfee ePO console to manage the on-premise components of the hybrid solution:

- Client Proxy
- Content Security Reporter

McAfee ePO Cloud

McAfee ePO Cloud is a cloud-based instance of McAfee ePO. As a cloud service, it is managed 24/7 by a team of McAfee security experts. After you purchase a subscription to the service, there is no hardware or software to install.

Using the McAfee ePO Cloud console, you can manage the cloud components of the hybrid solution:

- Client Proxy
- McAfee WGCS

Client Proxy can be managed using both McAfee ePO platforms at the same time.

Activate McAfee WGCS and access the Getting Started page

Activate McAfee WGCS, log on to McAfee ePO Cloud, and navigate to the **Getting Started** page.

Before you begin

- You have an active Web Protection license and subscription to McAfee WGCS.
- You received the welcome email that comes with your subscription.

Task

1 In the welcome email, click the **Activate** link.

2 On the activation page, enter your McAfee ePO Cloud credentials.

Save this email address and password. You need these values when configuring the hybrid solution in the Web Gateway interface.

McAfee WGCS is activated.

3 To log on to McAfee ePO Cloud, click manage.mcafee.com, then enter the email address and password you provided on the activation page.

4 In the McAfee ePO Cloud management console, click the menu icon in the upper-left corner, then select **Web Protection** | **Getting Started**.

The McAfee WGCS **Getting Started** page opens.

McAfee WGCS getting started information

The **Getting Started** page has the information you need to get started with McAfee WGCS and the hybrid solution.

- **Customer ID** — Uniquely identifies the customer in the system.
- **Customer Specific Proxy** — Specifies the domain name of your McAfee WGCS instance. The domain name has the form: c<customer_id>.saasprotection.com.

  Example: c12345678.saasprotection.com

Save these values for later use. You need them when configuring Client Proxy policies. Hybrid customers need the customer ID when configuring policy synchronization in the Web Gateway interface.

Client Proxy workflow

You can set up, manage, and configure Client Proxy policies using the McAfee ePO or McAfee ePO Cloud management platform or both platforms.

Management platform	Configuration
McAfee ePO	You must configure the Client Proxy password in McAfee ePO Cloud, then export the credentials to a file.
McAfee ePO Cloud	No configuration is required in McAfee ePO.

Setting up Client Proxy

A McAfee ePO server, installed on your network or in the cloud, provides a platform and console where you can set up and manage Client Proxy for the hybrid solution.

Setting up Client Proxy with McAfee ePO involves the following high-level tasks. Not all tasks are required when Client Proxy is managed with McAfee ePO Cloud.

1 Install the Client Proxy extension on the McAfee ePO server.

The extension comes installed with McAfee ePO Cloud.

2 Check in the Client Proxy client software package to the Master Repository on the McAfee ePO server.

The client software package comes checked in to the Master Repository with McAfee ePO Cloud.

3 Deploy the software to the managed endpoints running Windows or Mac OS X in your organization.

4 Configure Client Proxy policies.

5 Assign each policy to a group of managed endpoints.

Managing Client Proxy

High-level steps depend on whether you are managing Client Proxy with the on-premise or cloud version of McAfee ePO.

Managing Client Proxy with McAfee ePO

1 Using McAfee ePO Cloud, configure the Client Proxy password, then export the credentials to an .xml file.

2 Using McAfee ePO, import the Client Proxy credentials from the .xml file, then create a policy for the hybrid solution.

Importing your McAfee ePO Cloud credentials on-premise ensures that the Client Proxy policy is synchronized on premise and in the cloud.

Managing Client Proxy with McAfee ePO Cloud

1 Install a fresh instance of McAfee Agent on the endpoint.

2 Using McAfee ePO Cloud, create a Client Proxy policy for the hybrid solution.

Configuring redirection in Client Proxy policies

Client Proxy redirects web requests to Web Gateway or McAfee WGCS according to the settings in the Client Proxy policies you configure and deploy.

1 In the McAfee ePO or McAfee ePO Cloud management console, create a Client Proxy policy and configure these settings.

- **Proxy Server Address** — To configure McAfee WGCS as the proxy server, specify the **Customer Specific Proxy** from the getting-started page as the proxy server address.
- **Unique Customer ID** — (McAfee ePO only) Specify your customer ID.
- **Shared Password** — Specify the shared password that Client Proxy and McAfee WGCS use to communicate.
- **Traffic Redirection** — Configure this setting based on whether McAfee WGCS is deployed as a cloud-only or hybrid solution. In a cloud-only deployment, Client Proxy always redirects network traffic to McAfee WGCS for filtering. In a hybrid deployment, Client Proxy only redirects network traffic to McAfee WGCS when a managed endpoint is located outside the network and not connected by VPN.

2 Assign the Client Proxy policy to the managed endpoints.

When the Client Proxy policy takes effect

After you assign a Client Proxy policy to the managed endpoints in your organization, allow time for the following steps to complete and the policy to take effect.

1 McAfee ePO or McAfee ePO Cloud deploys the updated Client Proxy policy to the endpoint. The time this step takes depends on the value configured for the **Policy enforcement interval** set in your McAfee® Agent policy.

2 The Client Proxy software shares the password with McAfee WGCS. This step can take up to 20 minutes.

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

Setting up Content Security Reporter

Content Security Reporter is managed with McAfee ePO.

Setting up Content Security Reporter involves these high-level steps in the McAfee ePO console.

1. Installing the Content Security Reporter extension on the McAfee ePO server.
2. Registering the report server with Content Security Reporter.
3. Configuring the log sources for Content Security Reporter.
4. Configuring a database for Content Security Reporter.
5. Creating queries to run on the log data.
6. Running reports.

Managing the hybrid solution

After setting up the hybrid components, you manage the solution in the Web Gateway interface.

Management tasks include:

- Identifying rule sets that aren't supported in the cloud
- Enabling compatible rule sets for synchronization with the cloud
- Configuring and enabling hybrid synchronization
- Verifying that policy synchronization succeeded

Identifying rule sets not supported in the cloud

Not all Web Gateway rule sets are compatible with the cloud. Incompatible rule sets can't be enabled in the cloud and synchronized with McAfee WGCS.

To identify which rule sets aren't supported in the cloud:

- View the rule sets in the Web Gateway interface — Select **Policy** | **Rule Sets**, then select an individual rule set. If the **Enable in Cloud** checkbox in the configuration pane is grayed out, the rule set isn't supported in the cloud.
- See the list of properties in Appendix A of the *McAfee Web Gateway Product Guide* — Any rule sets that use properties identified as *not SaaS-compatible* are not supported in the cloud.

Enable rule sets for hybrid synchronization

You must enable the Web Gateway rule sets that you want synchronized with McAfee WGCS.

> **Before you begin**
> Review the rule sets and decide which ones to enable in the cloud.

The default rule sets provide all rules needed for the hybrid solution.

Task

1. In the Web Gateway interface, select **Policy** | **Rule Sets**.
2. For each rule set that you want synchronized with McAfee WGCS, select it, then select **Enable in Cloud**.
3. Click **Save Changes**.

The selected rule sets are enabled for synchronization with the cloud.

Configure and enable the hybrid solution

In the Web Gateway interface, you configure the connection with McAfee WGCS and the synchronization interval.

Before you begin

The hybrid components are set up.

The Web Gateway rule sets that you want synchronized with McAfee WGCS are enabled in the cloud.

You have your McAfee ePO Cloud credentials and your McAfee WGCS customer ID.

After hybrid synchronization is enabled in the Web Gateway interface, it can't be disabled and the McAfee WGCS policy, which is overwritten, can't be restored. But you can manually control when the on-premise policy is synchronized with the cloud.

Task

1 In the Web Gateway interface, select **Configuration** | **Cluster** | **Web Hybrid**.

2 To enable hybrid synchronization and configure the hybrid settings, select **Synchronize policy to cloud**.

3 Configure these hybrid settings:

- **Cloud address** — Specifies the address that Web Gateway uses to communicate with McAfee WGCS.

  Value: `https://msg.mcafeesaas.com:443`

- **Cloud administrator account name** — Specifies your McAfee ePO Cloud user name.
- **Cloud administrator account password** — Specifies your McAfee ePO Cloud password.
- **Customer ID** — Specifies your McAfee WGCS customer ID.
- **Local policy changes will be uploaded within the same interval as defined below** — Specifies the synchronization interval.

  Default: 15 minutes

  Range: 10–60 minutes

4 Click **Save Changes**.

Hybrid synchronization is enabled, and the Web Gateway policy is pushed to McAfee WGCS at the specified synchronization interval or manually.

Verify that policy synchronization succeeded

Verify that the hybrid solution is correctly configured and that policy synchronization succeeded.

Task

1 In the Web Gateway interface, select **Troubleshooting**, then select the name of the appliance.

2 In the expanded list, select **Synchronization to Cloud** | **Synchronize**.

This message is displayed: *Policy synchronization successfully performed!*

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1 Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.

2 In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.

3 Select a product and version, then click **Search** to display a list of documents.

Related product documentation

For detailed information about each hybrid component, see the related product documentation.

Each hybrid component has its own set of product documentation. For each component, we recommend the following related documents in that documentation set.

Hybrid component	Related documentation
Web Gateway	*McAfee Web Gateway Installation Guide* *McAfee Web Gateway Product Guide*
McAfee WGCS	*McAfee Web Gateway Cloud Service Migration Guide* *McAfee Web Gateway Cloud Service Product Guide*
McAfee ePO Cloud	*McAfee ePolicy Orchestrator Cloud Installation Guide* *McAfee ePolicy Orchestrator Cloud Product Guide*
McAfee ePO	*McAfee ePolicy Orchestrator Installation Guide* *McAfee ePolicy Orchestrator Product Guide*
Client Proxy	*McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator* *McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator Cloud*
Content Security Reporter	*McAfee Content Security Reporter Quick Start Guide* *McAfee Content Security Reporter Product Guide*