McAfee Web Protection Hybrid Integration Guide

Trellix

Contents

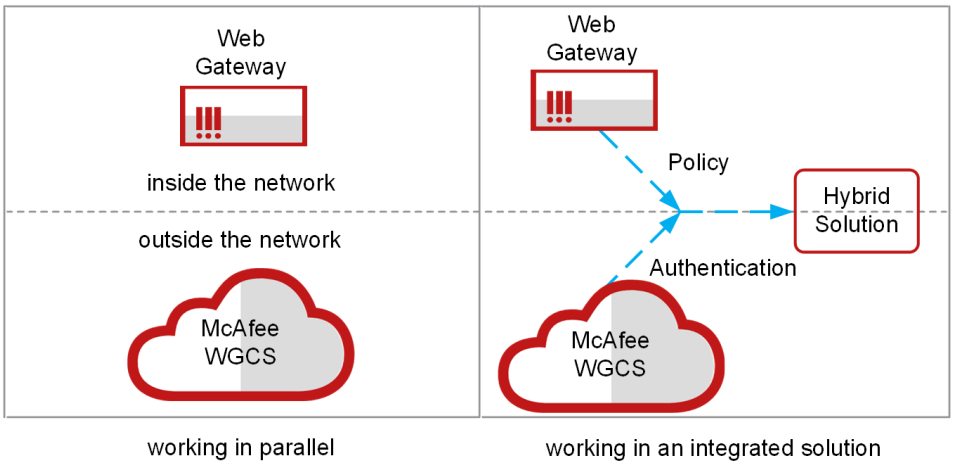
Product overview

Overview

The McAfee® Web Protection hybrid solution is the integration of McAfee® Web Gateway and McAfee® Web Gateway Cloud Service (McAfee® WGCS) in a hybrid deployment.

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.

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 policy is configured in the Web Gateway interface and pushed to McAfee WGCS at the synchronization interval you specify. Authentication is configured in the McAfee WGCS interface.



Hybrid components

A Web Protection license provides all components needed to set up a hybrid deployment. 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™)

Cloud-only vs. hybrid deployments

The type of deployment determines how the web protection policy is managed.

- **Cloud-only deployment** — The policy is managed with McAfee ePO Cloud and saved in the global policy store.
- **Hybrid deployment** — The policy is managed in the Web Gateway interface and synchronized with the cloud. When synchronized, the on-premise policy overwrites the policy configured in the cloud and saved in the global policy store.

Caution

After hybrid synchronization is enabled in the Web Gateway interface, the web protection policy in the cloud is overwritten. To disable synchronization and restore the default McAfee WGCS policy, you must contact Technical Support.

Key features

The Web Protection hybrid solution offers centralized management of one security policy across office locations and users working on premise and remotely.

- **Flexible deployment** — The solution can be deployed in a cloud-only or hybrid deployment and has the flexibility to meet security needs now and in the future.
- **Policy synchronization** — Manage and apply one web security policy across office locations and users working on premise and remotely.
- **User authentication** — Users requesting cloud access are authenticated using methods configured in the McAfee WGCS interface.
- **Centralized management** — Except for Web Gateway, hybrid components are managed with McAfee ePO and McAfee ePO Cloud.
- **Integration with McAfee web security technologies**
  - **Gateway Anti-Malware Engine** — Gateway Anti-Malware technology filters web traffic, detecting and blocking zero-day malware in-line using traditional anti-virus and behavior emulation technology.
  - **Sandboxing** — Sandboxing combines the static analysis of unknown files with behavioral analysis in a sandbox environment using McAfee® Advanced Threat Defense or McAfee® Cloud Threat Detection (McAfee® CTD).
  - **URL filtering** — The solution filters URLs using whitelists, blacklists, and reputation categories based on risk levels determined by McAfee® Global Threat Intelligence™ (McAfee GTI).
  - **Web filtering** — The solution simplifies policy rules by assigning similar websites, web applications, and file types to groups based on information provided by McAfee GTI.

How it works

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

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

Client Proxy credentials are configured with 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. From McAfee ePO Cloud, the administrator:
   - McAfee WGCS interface — Configures authentication
   - Client Proxy interface — Configures the shared password and exports the credentials to an .xml file
2. From McAfee ePO, the administrator:
   a. Imports the Client Proxy credentials from the .xml file
   b. Creates a Client Proxy policy for use with the hybrid solution
   c. Assigns the policy to all managed endpoints in the organization

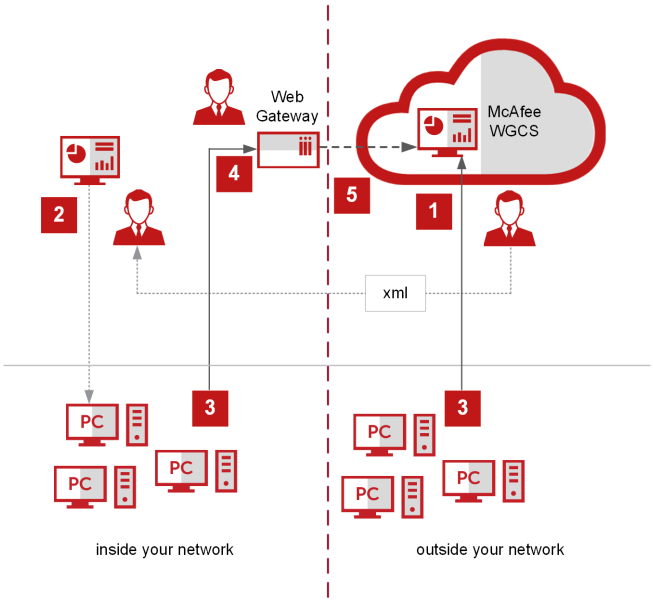
   Note

   The administrator can configure multiple policies and assign each one to a different group of managed endpoints.

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:
   - **Users working inside your network or connected by VPN** — Allows web requests to continue to a Web Gateway appliance installed on your network
   - **Users working outside your network** — Redirects web requests to McAfee WGCS
4. From the Web Gateway interface, the administrator:
   a. Reviews the web protection policy and enables the rule sets to be pushed to the cloud
   b. Configures and enables the hybrid solution
5. When the deployment is enabled:
   - The Web Gateway policy is pushed to the cloud at the specified synchronization interval.
   - The **Policy Browser**, where the McAfee WGCS policy is configured in the McAfee ePO Cloud UI, is disabled. Instead, a **Policy Unavailable** message displays information about the hybrid synchronization, such as the date and time of the last sync.

Note

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


Web
Gateway
McAfee
WGCS
2
4
5
1
xml
3
3
PC
PC
PC
PC
PC
PC
inside your network
outside your network

Setting up the hybrid solution

Components of the hybrid solution

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

Note

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 managed endpoints, is aware of the user's location and allows or redirects network traffic, accordingly:
    - Inside the network or connected to the network by VPN — Client Proxy allows network traffic to continue 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.

Managed endpoints are the client or user computers in your organization that are managed with McAfee ePO or McAfee ePO Cloud.

How the hybrid components are managed

This table summarizes how the hybrid components are managed with McAfee ePO, McAfee ePO Cloud, or both platforms.

Hybrid component	Managed with McAfee ePO	Managed with McAfee ePO Cloud
Web Gateway	no	no

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

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 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. Setup includes activating the service, logging on to McAfee ePO Cloud, and locating the getting-started information.
5. Client Proxy — Setup depends on whether you are using McAfee ePO or McAfee ePO Cloud. From either platform, you deploy the Client Proxy software to the managed endpoints in your organization, configure a Client Proxy policy, and assign 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.

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.

Note

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

Note

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.

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

Tip

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

Task

1. In the welcome email, click the **Activate** link.
2. On the activation page, specify your McAfee ePO Cloud credentials.

   Tip

   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. From the McAfee ePO Cloud menu, select **Web Protection** → **Getting Started**.

Results

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

Client Proxy workflow

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 Client Proxy for the hybrid solution.

You can manage Client Proxy policies using the McAfee ePO or McAfee ePO Cloud management platform or both platforms. 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.

   Note

   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.

   Note

   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.

Note

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 endpoints.
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 McAfee ePO or McAfee ePO Cloud, 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** — Specify your customer ID. (McAfee ePO)
   - **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 Client Proxy policy to the endpoints. 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.

Caution

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.

Configure McAfee WGCS as a log source for Content Security Reporter

After you configure Content Security Reporter to use McAfee WGCS as a log source, you can pull data from the cloud service and run queries and reports.

You configure Content Security Reporter in the McAfee ePO interface.

Note

For more information about using Content Security Reporter, see the product documentation in the **McAfee Documentation Portal**.

Task

1. From the McAfee ePO menu, select **Configuration** → **Report Server Settings**.
2. From the **Setting Categories** menu, select **Log Sources**.
3. From the **Actions** drop-down list, select **New**.
4. On the **New Log Source** page, specify a name for the log source, then select **Enable log source**.
5. From the **Mode** drop-down list, select **Collect log files from**, then from the drop-down list, select **McAfee Web Gateway Cloud Service**.
6. On the **Source** tab, provide your customer ID, then in the **Logon name** and **Password** fields, provide your McAfee ePO Cloud credentials.
7. On the **User-Defined Columns** tab, configure up to four custom columns. For each column:
   a. Select **Populate this column**.
   b. From the **Log record** drop-down list, select a record.
   c. In the **Log file header** field, specify a name for the column.
8. On the **Schedule** tab, specify dates for beginning and ending log file collection, the frequency of collection, and a starting time.
9. On the **Processing** tab, configure how you want Content Security Reporter to process the log file data.
10. On the **Post-Processing** tab, configure how you want Content Security Reporter to handle log files after processing is complete.
11. Click **OK** to save the configuration.

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**.

Authentication considerations for the hybrid solution

McAfee WGCS authenticates users when they are working outside the network. Authentication settings configured on premise and in the cloud must be compatible.

Group name format

Web Gateway and McAfee WGCS use different formats for the names of user groups. We recommend updating the format of the group names used on premise to match the format used in the cloud. Otherwise, the policy rules configured on premise might apply differently to users when they are working outside the network.

Product	Group name formats used
Web Gateway	DomainName\GroupName GroupName
McAfee WGCS	DomainName\GroupName (recommended)

To make sure that the group names used on premise include the domain name, review the rules and rule sets that are enabled in the cloud. If you are using Client Proxy as the authentication method, configure the **Authentication with McAfee Client Proxy** rule and select **Keep domain name in group name**.

User name and user group properties

McAfee WGCS authenticates users when they are working outside the network and assigns values to the user name and user group properties according to the authentication method used. These properties correspond to the *Authentication.UserName* and *Authentication.UserGroups* properties in the Web Gateway interface.

Authentication methods used by McAfee WGCS

Authentication method	The user is authenticated when...	Policy decisions are based on...
Client Proxy	Client Proxy is installed on the managed endpoints, a policy is deployed to the endpoints, and the user sends a web request from an endpoint.	Group memberships returned by Client Proxy
IP range	One or more IP address ranges are configured and the user sends a web request from one of the configured ranges.	Configured IP address ranges in McAfee WGCS
SAML	SAML authentication is configured and the user sends a web request to the SAML service port: 8084.	Group ID attribute value in the SAML assertion
IPsec site-to-site	Web requests are received through the IPsec VPN tunnel configured between your network and McAfee WGCS.	Membership in your organization

Managing the hybrid solution

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 under *Configuration lists* in the *McAfee Web Gateway Interface Reference 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.

When you enable a rule set for hybrid synchronization, the rule set view determines whether nested rule sets are also enabled in the cloud.

- **Key elements view** — Nested rule sets are enabled.
- **Complete rules view** — When the rule set is enabled from the context menu, nested rule sets are enabled too. When the rule set is enabled in the configuration pane, nested rule sets are not enabled and must be enabled individually.

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**.

Results

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

Configure and enable the hybrid solution

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.

Caution

After hybrid synchronization is enabled in the Web Gateway interface, the web protection policy in the cloud is overwritten. To disable synchronization and restore the default McAfee WGCS policy, you must contact Technical Support.

Task

1. In the Web Gateway interface, select **Configuration** → **Appliances**.
2. On the **Cluster** branch of the appliances tree, click **Web Hybrid**.
   The hybrid settings open in the configuration pane.
3. Configure the settings as needed.
4. Click **Save Changes**.

Results

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

To verify that the hybrid solution is correctly configured and that policy synchronization succeeded, you can perform the synchronization manually.

Task

1. In the Web Gateway interface, select **Troubleshooting**, then under the name of the appliance, select **Synchronization to Cloud**.
2. In the expanded list, select **Synchronization to Cloud**.
3. In the **Synchronization to Cloud** pane, click **Synchronize**.

Results

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

Add hybrid information to a block page

You can add information to a block page that shows whether the on-premise appliance or cloud service blocked the user's request.

In a hybrid deployment, McAfee WGCS shares the block pages that are configured in the Web Gateway interface. Using the property *InTheCloud*, you can add information to a block page to show whether the blocked request was filtered on premise or in the cloud. This property returns a true value when McAfee WGCS filters and blocks the request.

In this task, you edit the default block page template named **URL Blocked**. The default template includes the title **Blocked by URL Filter Database** and the following standard text. Actual values for the properties in the template are written to the block page when it is generated.

> Your requested URL has been blocked by the URL Filter database module of McAfee Web Gateway. The URL is listed in categories that are not allowed by your administrator at this time.
>
> **URL:**
>
> **URL Categories:**
>
> **Reputation:**
>
> **Media Type:**

In the following steps, you add a line to the block page after **Media Type** using the suggested text or custom text that you specify.

Task

1. In the Web Gateway interface, select **Policy** → **Templates.**
2. Expand the template folders **Default Schema** → **URL Blocked** → **en**.
3. Click **html**.
   The **HTML Editor** opens and displays the contents of the URLBlocked.html file.
4. In the file, locate the line that begins: `<b>Media Type: </b>`.
5. Immediately following this line, add these lines:

```
<b>Filter: </b>
<script type="text/javascript">
   if ($InTheCloud$) {
      writeToDocument("McAfee Web Gateway Cloud Service");
   } else {
      writeToDocument("McAfee Web Gateway");
   }
</script>
```

6. Click **Save Changes**.
7. To view the output, click **Preview**.
   The preview opens in a new tab. A line labeled **Filter** is added after the line labeled **Media Type**.

   Tip

   To view the text in the preview that is written to the block page when it is generated, you can replace the property `($InTheCloud$)` with the value `(true)` or `(false)`. Click **Save Changes**, then click **Preview**. Depending on the value of *InTheCloud*, one of these lines is displayed.

   Filter: McAfee Web Gateway Cloud Service

   Filter: McAfee Web Gateway

Hybrid settings

When configured, the hybrid settings allow Web Gateway to connect to and communicate with McAfee WGCS.

Hybrid synchronization

The Web Gateway policy is synchronized with McAfee WGCS at the interval you specify in the hybrid settings. You can also perform synchronization manually. Manual synchronization doesn't affect the synchronization interval or schedule which continues as before.

Configuring the hybrid settings

The hybrid settings allow you to configure synchronization without a proxy server.

Web Hybrid Configuration

Option	Definition
Synchronize policy to Cloud	When selected, allows you to configure the **Web Hybrid** settings and enables the hybrid solution.
Appliance for Synchronization	From the drop-down list, select the Web Gateway appliance whose policy you want synchronized with McAfee WGCS. If you are running multiple appliances in a Central Management cluster, this setting ensures that the McAfee WGCS policy is always synchronized with the same appliance.
Cloud address	Specifies the address that Web Gateway uses to communicate with McAfee WGCS. **Value:** `https://msg.mcafeesaas.com`
Cloud administrator account name	Specifies your McAfee ePO Cloud user name.
Cloud administrator account password	Specifies your McAfee ePO Cloud password. To change the password, click **Set**, then enter the new password and click **OK**.
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 (recommended) **Range:** 10–60 minutes

Configuring the advanced hybrid settings

The advanced hybrid settings allow you to add a proxy server to the configuration.

Advanced Synchronization Settings

Option	Definition
Verify server certificate on SSL connections	When selected, Web Gateway verifies the proxy server certificate for SSL connections.
Use a proxy for synchronization	When selected, allows you to configure the proxy server settings. When the settings are configured, the Web Gateway policy is pushed to McAfee WGCS through the proxy server.
Proxy host	Specifies the IP address or host name of the server which is used as a proxy.
Proxy port	Specifies the port number on the proxy server that listens for Web Gateway requests to transfer synchronization data. **Default:** 8080
Proxy user	Specifies the user name that Web Gateway sends to the proxy server when transferring synchronization data.
Proxy password	Specifies the password that Web Gateway sends to the proxy server when transferring synchronization data. To change the password, click **Set**, then enter the new password and click **OK**.

McAfee Mobile Cloud Security

Adding mobile devices to your protected endpoints

The McAfee® Mobile Cloud Security solution allows you to add mobile devices to the endpoints that are protected by McAfee WGCS.

The mobile cloud security solution requires configuration in these interfaces:

1. Web Gateway UI — Upload the CA certificate used by the Mobile Device Management (MDM) server software to sign the device certificates. For more information, see the topic *Managing certificates for cloud use* in the *Web Gateway Product Guide*. Then synchronize the configuration with the cloud.

   The solution comes enabled with Web Gateway versions 9.1 or later.

2. Administrator interface of your MDM solution — Configure an identity certificate profile for the device and a VPN profile.

Note

You must upload the CA certificate in the Web Gateway UI before configuring the MDM solution.

Supported operating system platforms and MDM solutions

McAfee Mobile Cloud Security supports these operating system platforms and MDM solutions. MDM software consists of client software that is installed on the mobile devices and server software that administrators configure to manage the devices.

Supported platforms	Supported MDM solutions
Android	• AirWatch • Microsoft Intune • MobileIron
iOS	• AirWatch • Microsoft Intune • MobileIron

Configuring the MDM software

You can use the AirWatch, Microsoft Intune, or MobileIron MDM solution to manage your users' Android or iOS devices. For configuration details, see these McAfee Community articles:

- Configuring the AirWatch MDM solution for Android devices
- Configuring the AirWatch MDM solution for iOS devices
- Configuring the Microsoft Intune MDM solution for Android devices
- Configuring the Microsoft Intune MDM solution for iOS devices
- Configuring the MobileIron MDM solution for Android devices
- Configuring the MobileIron MDM solution for iOS devices

Components needed to protect your mobile devices

The mobile cloud security solution consists of these McAfee and customer-provided components.

McAfee components

- Web Gateway — Provides the user interface where administrators configure the mobile cloud security solution and synchronize the configuration with the cloud.
- VPN Gateway — Separates the mobile cloud security infrastructure from McAfee WGCS and the internet. The VPN Gateway runs inline with McAfee WGCS.
- McAfee WGCS — Filters HTTP/HTTPS traffic for your organization's mobile devices according to the policy you configure.

Customer-provided components

- MDM solution — The Mobile Device Management server and client software
- Mobile devices — Android or iOS endpoints with MDM client software installed

How the mobile cloud security solution protects devices

After you set up the mobile cloud security solution, software on the mobile device redirects HTTP/HTTPS traffic to McAfee WGCS for filtering.

Open the Web Gateway UI.

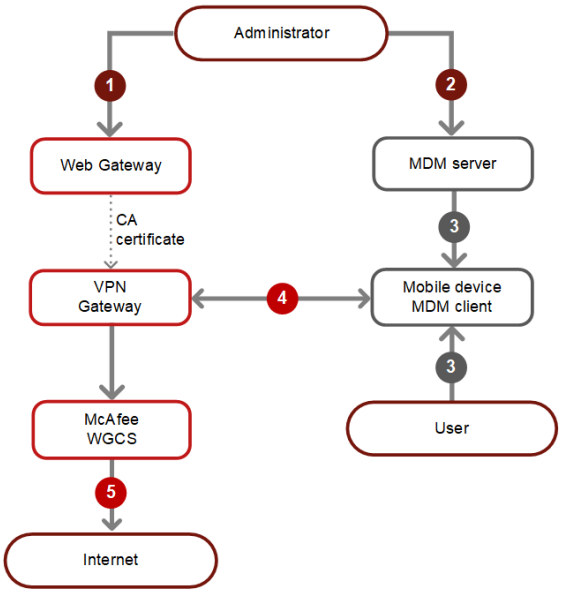
1. In the UI, the administrator configures the mobile cloud security solution by:
   a. Uploading the customer CA certificate, whose private key is used to sign the device certificates
   b. Specifying the names of the fields that identify the user name and user group in the device certificates

   Note

   You must upload the CA certificate before configuring the MDM solution.

2. In the administrator interface of the MDM solution, the administrator:
   a. Configures an identity certificate profile for the device.

   b. Configures the VPN profile which references the identity certificate profile.
3. When the user logs on to the device and registers it with the MDM server, the software:
   a. Signs the identity or device certificate with the CA certificate.
   b. Downloads the signed certificate and VPN profile to the device.
4. After the following steps are completed, the software on the device starts redirecting HTTP/HTTPS traffic to McAfee WGCS through the VPN gateway.
   a. The device uses the signed certificate to authenticate to the VPN gateway.
   b. The VPN gateway creates a secure VPN tunnel with the device.
5. McAfee WGCS filters the HTTP/HTTPS traffic, allowing or blocking web requests according to your policy.



COPYRIGHT

Trellix