

# McAfee Web Protection Hybrid

## Introduction

McAfee<sup>®</sup> Web Protection provides the licenses and software for you to deploy McAfee<sup>®</sup> Web Gateway, McAfee<sup>®</sup> SaaS Web Protection, or a hybrid deployment using both on premise and SaaS technologies.

This document discusses using both Web Gateway and SaaS Web Protection, together with other components, to provide hybrid web scanning for your users.

---

## How the McAfee Web Protection hybrid deployment works

As devices become more mobile, it becomes increasingly difficult to design and enforce web security policies for your users. Web Protection hybrid deployments help address these difficulties by enforcing your web policies regardless of where your users are located.

The Web Protection hybrid deployment uses several McAfee products and components to enable you to define web usage policies that are enforced wherever your users are. Your users can be in-office, working from home, when connected to your networks using virtual private networks (VPN), or when traveling.

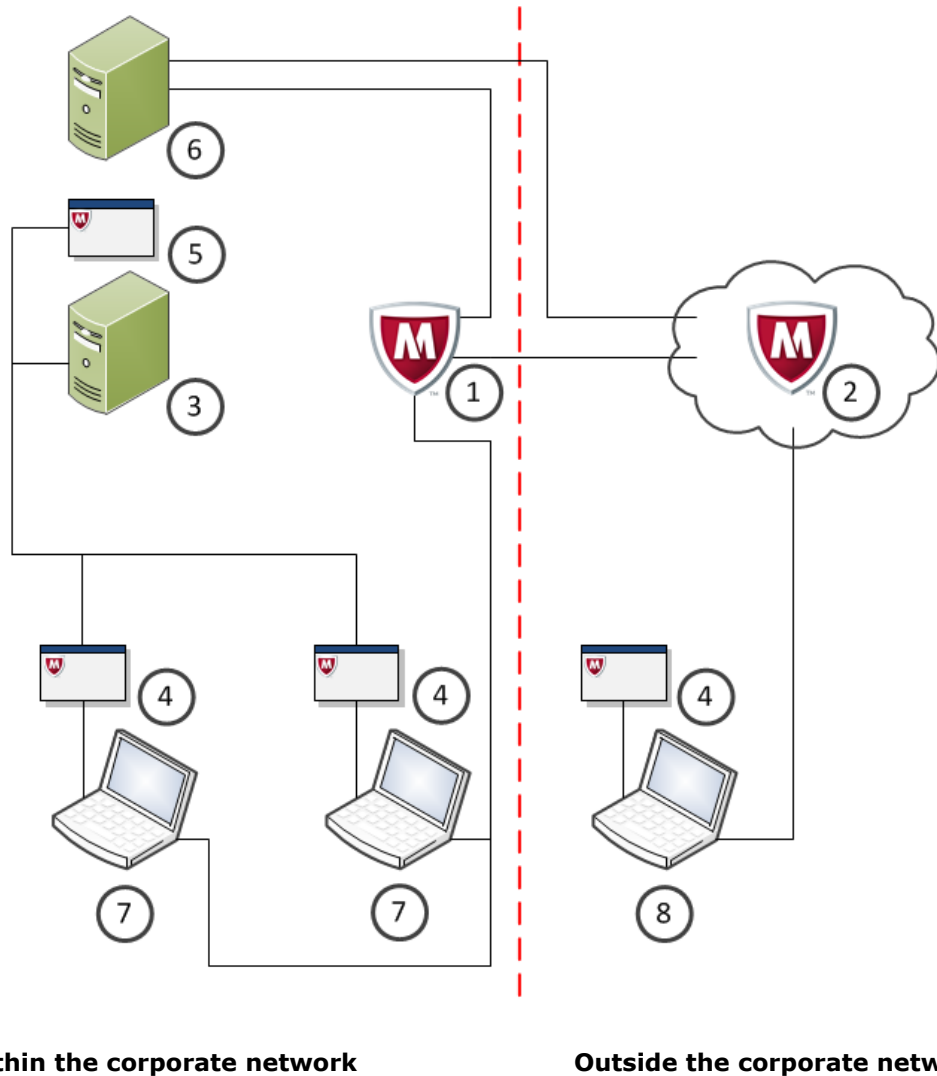
When your users are within your corporate environment, you configure complex security policies and defenses that enforce compliance with your web usage strategies.

When your users take devices outside the corporate environment, these web security policies and defenses within your network no longer work.

To enforce your web usage policies both within and outside your network, Web Protection hybrid deployments use:

- Web Gateway for when your users are within your corporate environment.
- SaaS Web Protection for when your users are outside of your protected networks.

As the administrator, you control the policies that are applied both within and outside your corporate organization.



**Table 1 Components in the Web Protection hybrid deployment**



Key	Description
1	Web Gateway
2	SaaS Web Protection
3	McAfee® ePolicy Orchestrator® (McAfee ePO™)
4	McAfee® Client Proxy or McAfee WDS installed on all supported endpoint devices that go outside your corporate environment
5	McAfee® Help Desk (running within McAfee ePO)
6	McAfee® Content Security Reporter or McAfee® Web Reporter
7	Endpoint devices operating within the corporate environment
8	Endpoint devices operating outside of the corporate environment

## Components of the McAfee Web Protection hybrid deployment

The Web Protection hybrid deployment uses several interacting components.

By using these components, key features and functions are added to the hybrid deployment.

**Table 2 McAfee Web Protection hybrid deployment components**

Component	Description	Location	Required
McAfee Web Gateway	<p>Web Gateway ensures comprehensive web security for users within your network.</p> <p>It protects your network against threats arising from the web, such as viruses and other malware, inappropriate content, data leaks, and related issues. It also ensures regulatory compliance and a productive work environment.</p>	Installed within your corporate network	Required
McAfee SaaS Web Protection	<p>SaaS Web Protection provides real-time protection against web-borne threats and inappropriate content at the network perimeter before they can enter the internal network.</p> <p>The browser traffic for users is redirected to SaaS Web Protection. As each request for web content is received, SaaS Web Protection checks the content against defined policies and, if enabled, checks for known worms and viruses.</p>	"In the cloud"	Required
McAfee® ePolicy Orchestrator® (McAfee ePO™)	<p>McAfee ePO is a scalable, extensible management platform that enables centralized policy management and enforcement of your security products and the systems on which they reside.</p> <p>In relation to McAfee Web Protection hybrid deployment, it also provides a method to deploy the Client Proxy and McAfee® Help Desk components.</p>	Installed within your corporate network	Optional
McAfee® Client Proxy	<p>Client Proxy enables the Web Protection hybrid deployments by providing location awareness features. It also redirects web traffic and network communications from laptops and other computers that are used when disconnected from the corporate network. Client Proxy also handles authentication for your end users.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Use either Client Proxy or WDS to authenticate your users with the McAfee Web Protection hybrid deployment.         </div>	Deployed to all protected computers via McAfee ePO or Control Console	Optional
McAfee WDS Connector	<p>To allow SaaS Web Protection to transparently authenticate users when they access the web, WDS Connector enables SaaS Web Protection to use the existing local domain credentials.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Use either WDS or Client Proxy to authenticate your users with the McAfee Web Protection hybrid deployment.         </div>	Installed within your corporate network	Optional

**Table 2 McAfee Web Protection hybrid deployment components** *(continued)*

Component	Description	Location	Required
McAfee® Help Desk	<p>Help Desk is an extension installed in McAfee ePO. Help Desk allows administrators to temporarily bypass security policies and to uninstall protected applications when there is a legitimate business need.</p> <p>Help Desk is not expected to be used as an everyday part of the workflow for the Web Protection hybrid deployment. It is used for emergency assistance in the event of circumstances that prevent web access from a specific computer.</p>	Installed within McAfee ePO	Optional
McAfee® Content Security Reporter	Content Security Reporter integrates with McAfee ePO, providing reporting tools that enable you to identify issues in your organization. These issues can include liability exposure, productivity loss, bandwidth overload, and security threats. You can use this information to modify web use policies and provide guidance for appropriate Internet use in your organization.	Installed within your corporate network	Optional
McAfee® Web Reporter	Web Reporter uses log files from both Web Gateway and SaaS Web Protection to provide the reporting tools without using McAfee ePO. These tools help identify issues in your organization such as liability exposure, productivity loss, bandwidth overload, and security threats. You can use this information to modify web use policies and provide guidance for appropriate Internet use in your organization.	Installed within your corporate network (non-McAfee ePO deployment)	Optional

For version information on each of these components, see <http://www.mcafee.com/us/downloads/downloads.aspx> and <https://contentsecurity.mcafee.com>.

## Location awareness

To provide location awareness, McAfee Client Proxy is installed on all supported endpoint computer systems — typically laptop computers — that are regularly taken out of the office.

### McAfee Client Proxy

To work out the location of your users device, Client Proxy attempts to communicate with either your McAfee ePO, or with other servers within your corporate network. If this communication is successful, Client Proxy assumes that the device is within your corporate environment. It then stands down because it identifies that it is within the corporate network. In this case, all web requests are directed to your Web Gateway within your corporate environment.

If, however, Client Proxy cannot contact any of your servers, Client Proxy then directs relevant web requests to SaaS Web Protection.



Client Proxy can be deployed from within McAfee ePO, or use Microsoft System Management Server (SMS) to push Client Proxy to each computer that you specify.

## McAfee Help Desk

If a user outside of your network cannot access a vital web resource, a system administrator uses Help Desk to provide overrides to the current settings. These overrides include removing the Client Proxy service from that specific computer.



Help Desk is an McAfee ePO extension, installed and run from your McAfee ePO server.

## Reporting

The Web Protection hybrid deployment provides options for generating reports on your users web usage, regardless of where they browse the internet.

Depending on how you configure and roll out your Web Protection hybrid deployment, you use one of the following products to meet your reporting requirements:

- Content Security Reporter
- Web Reporter

Both these products serve a similar function; the main difference is that Content Security Reporter is used when the Web Protection hybrid deployment is used in-conjunction with McAfee ePO, whereas Web Reporter is used when McAfee ePO is not part of the Web Protection hybrid deployment.

These products are used to provide reporting on web usage from both your Web Gateway and your SaaS Web Protection, giving you comprehensive reporting on the web usage of all your users, regardless of their location.

---

## Deploying the Web Protection hybrid deployment

Deploy the components and services required to protect your web users regardless of their location.

### Purchase Web Protection

When you purchase Web Protection, you are acquiring the software licenses for Web Gateway, SaaS Web Protection, Client Proxy and the choice of the standard version of Content Security Reporter or Web Reporter.

In addition, if you require a hardware platform on which to run Web Gateway, this needs to be purchased using a different part number.

If you intend using McAfee ePO within the Web Protection hybrid deployment, this also needs to be purchased separately.

After you purchase Web Protection, you will receive by email the information required to access SaaS Web Protection and the Control Console.

### Locate and download the software

Locate the software components to install and configure the McAfee SaaS Web Protection hybrid deployment.

When you receive the Web Gateway license file, you are also given access to the McAfee Content and Cloud Security portal <https://contentsecurity.mcafee.com>.

From this portal, you can download the Web Gateway software.

To download Client Proxy, McAfee ePO and your chosen McAfee reporting product, go to <https://support.mcafee.com> and select **Patches and Downloads | Product Downloads**. Enter your grant number to access and download this software.

## Overview of the deployment process

Implementing the McAfee Web Protection hybrid deployment requires that all individual components are downloaded, installed, and configured. The "Software as a Service" components must also be accessible and configured to meet your requirements.

The following order is suggested for configuring the components.

- 1 Set up Web Gateway.
- 2 Set up the SaaS Web Protection.
- 3 Install McAfee ePO.
- 4 Deploy Client Proxy to your endpoint devices.
- 5 Configure Web Gateway and SaaS Web Protection communications.
- 6 Configure policies.
- 7 Configure reporting on web usage.

### Set up Web Gateway

Install and configure Web Gateway to provide the on-premise web scanning for your users.

The process to follow when installing your Web Gateway depends on your circumstances. You can install a new appliance, or reconfigure an existing appliance to provide hybrid web scanning.

#### Install a new Web Gateway

Web Gateway can be installed as a physical appliance on a suitable hardware platform, or as a virtual appliance running on a virtual machine within a suitable host system.

When installing a new Web Gateway as part of a hybrid web scanning solution, use the default rule set provided with the appliance. This default rule set provides the required rules for the hybrid configuration.



To configure Web Gateway for hybrid deployment alongside SaaS Web Protection, ensure that you install Web Gateway version 7.4.2 or later.

#### Configure an existing Web Gateway

When using an existing Web Gateway appliance to provide hybrid web scanning, consider the impact of the changes needed to the existing rules and policies.



Ensure that you upgrade to Web Gateway version 7.4.2 or later before configuring Web Gateway as part of a hybrid deployment.

#### High-level steps for setting up Web Gateway

To set up a Web Gateway appliance, complete the following high-level steps.

##### Task

- 1 Verify the requirements for the setup.
- 2 Review the default initial configuration settings.

- 3 Install the appliance software.
  - When setting up Web Gateway as a physical appliance with pre-installed software, connect and turn on the appliance.
  - When setting up Web Gateway as a physical appliance with downloaded software:
    - Download the software and copy it to some installation media.
    - Connect the appliance, insert the installation media, and turn on the appliance.
    - Work with the Boot Manager to install the software.
  - When setting up Web Gateway as a virtual appliance:
    - Download the software and copy it to some installation media.
    - Insert the installation media into a suitable host system.
    - Create a virtual machine on the host system.
    - Start the new virtual machine.
- 4 Implement the initial configuration settings.
- 5 Log on to the user interface.
- 6 Review online documents and import a license.
- 7 Activate the product.

After completing the setup, you can work with the user interface of Web Gateway to perform more administration activities.



For information on how to upgrade Web Gateway, see the release notes that are provided with each new product version.

## Log on to the SaaS Web Protection service

Before you can configure your Web Protection hybrid deployment, you need to log on to SaaS Web Protection.

### Before you begin

To log on to the SaaS Web Protection service, you must first have your license key, provided when you purchased SaaS Web Protection.

### Task

- 1 Browse to <https://www.mcafeegasap.com>.
- 2 Select your required language for the user interface.
- 3 Enter your registered email address and password.
- 4 Click **Login**.

The Control Console is displayed.

### Tasks

- [High-level steps for configuring SaaS Web Protection on page 8](#)  
To set up the SaaS Web Protection service, complete the following high-level steps.

## High-level steps for configuring SaaS Web Protection

To set up the SaaS Web Protection service, complete the following high-level steps.

### Task

- 1 Configure your Web Protection authentication to use Client Proxy.
- 2 Add your users details for Client Proxy.
- 3 Configure the Client Proxy policies, defining how and where the traffic is redirected.

For more information, see the Client Proxy documentation on the Control Console under **Web Protection | Setup | McAfee Client Proxy**.

## Install McAfee ePolicy Orchestrator

McAfee ePO provides the environment for deploying Client Proxy and hosting Help Desk. Your McAfee ePO server also works with the Client Proxy deployments on your endpoint devices to provide part of the location-awareness features within the Web Protection hybrid deployment.

The exact process that you follow to install McAfee ePO depends on whether you are installing a new server, or if you are configuring an existing server as part of your Web Protection hybrid deployment.

### Installing a new McAfee ePolicy Orchestrator server

McAfee ePO needs to be installed within your corporate network, as detailed in the *McAfee ePolicy Orchestrator Installation Guide*. Once installed, use McAfee ePO to push Client Proxy to all computers that will be taken outside of your corporate environment.

### Using an existing McAfee ePolicy Orchestrator server

If you already have McAfee ePO set up within your organization, use the standard McAfee ePO work flows to push Client Proxy to all computers that will be taken outside of your corporate environment.

## Deploy McAfee Client Proxy

Each endpoint device that may be taken outside your corporate environment needs to have Client Proxy installed. Client Proxy provides the location awareness required to correctly direct your users web requests to either the Web Gateway or the SaaS Web Protection service.

### Tasks

- [Deploy McAfee Client Proxy using McAfee ePolicy Orchestrator on page 8](#)  
Use McAfee ePO to deploy Client Proxy to all endpoint devices that may be taken outside of your corporate environment.
- [Deploy McAfee Client Proxy using Microsoft System Management Server on page 9](#)  
For installations that do not use McAfee ePO, you can use Microsoft® System Management Server (SMS) to push the Client Proxy software and configuration to your endpoint computers.

### Deploy McAfee Client Proxy using McAfee ePolicy Orchestrator

Use McAfee ePO to deploy Client Proxy to all endpoint devices that may be taken outside of your corporate environment.

#### Before you begin

Ensure you have downloaded the Client Proxy extension. This extension is available from <https://contentsecurity.mcafee.com> or from <http://www.mcafee.com/us/downloads/downloads.aspx>.



## Task

- 1 Locate the previously downloaded Client Proxy extension.



The Client Proxy extension also contains the Help Desk extension.

- 2 Using the standard McAfee ePO workflows, install the Client Proxy extension within your McAfee ePO server.



Help Desk is also installed.

- 3 Follow the guidance given within the *McAfee Client Proxy Product Guide* to configure and install Client Proxy on your endpoint devices.

## Deploy McAfee Client Proxy using Microsoft System Management Server

For installations that do not use McAfee ePO, you can use Microsoft® System Management Server (SMS) to push the Client Proxy software and configuration to your endpoint computers.

### Before you begin

You must have Microsoft System Management Server (SMS) installed within your corporate network, and understand how to create software installation packages using this software.

When you have created your software installation package, together with the installation scripts needed in control the installation process, use your defined work flows for pushing Client Proxy to your endpoint computer systems. See the *McAfee Client Proxy Product Guide* for further details on deploying Client Proxy.

## Configure hybrid web policies

Several steps are required to configure Web Gateway and SaaS Web Protection so that they provide a co-ordinated scanning policy for your users, regardless of the users location.

The *McAfee Web Gateway Product Guide* includes a chapter on configuring Web Gateway and SaaS Web Protection so that they work together to provide a hybrid deployment.

This includes configuring the setting on the Web Gateway, and selecting suitable rule sets for use by both products.

## Configure reporting

The McAfee products, Content Security Reporter, and Web Reporter, are available to provide comprehensive reporting on your Web Protection hybrid deployment. Use Content Security Reporter with deployments managed by ePolicy Orchestrator, or Web Reporter for non-ePolicy Orchestrator deployments.

Refer to the relevant documentation for your exact deployment scenario.

## Tasks

- [High-level steps for configuring Content Security Reporter on page 10](#)  
To set up Content Security Reporter, complete the following high-level steps.
- [High-level steps for configuring Web Reporter on page 10](#)  
To set up Web Reporter, complete the following high-level steps.

## High-level steps for configuring Content Security Reporter

To set up Content Security Reporter, complete the following high-level steps.

### Task

- 1 Install the Content Security Reporter software on a computer where you configure it to run with ePolicy Orchestrator.
- 2 install the Content Security Reporter extension within ePolicy Orchestrator.
- 3 Register the report server within ePolicy Orchestrator.
- 4 Configure the Content Security Reporter database.
- 5 Configure the log sources for Content Security Reporter.
- 6 Configure your Content Security Reporter queries.
- 7 Run the reports from Content Security Reporter.

For more information, see the *Content Security Reporter Product Guide*.

## High-level steps for configuring Web Reporter

To set up Web Reporter, complete the following high-level steps.

### Task

- 1 Install the Web Reporter software on a computer where you use it.
- 2 Start the Web Reporter software and log on.
- 3 Configure the Web Reporter database.
- 4 Configure the log sources for Web Reporter.
- 5 Process the log files.
- 6 Run the reports from Web Reporter.

For more information, see the *Web Reporter Product Guide*.

---

## Download product documentation

This guide provides an overview of the McAfee Web Protection hybrid deployment. It is outside the scope of this document to detail all aspects of deploying each component to provide a fully functioning web security policy.

Each component within the Web Protection hybrid deployment has its own comprehensive set of documentation.

Key documents within these documentation sets are highlighted in the table.

**Table 3 Useful documents**

<b>Component</b>	<b>Useful documents</b>
McAfee Web Gateway	<i>McAfee Web Gateway Product Guide</i>
McAfee SaaS Web Protection and the WDS Connector	<a href="#">Account Management Administrator Guide</a> <a href="#">McAfee SaaS Web Protection Service Setup Guide</a> <a href="#">WDS Connector Setup Guide</a> (and, for organizations located outside of the Americas, <a href="#">Supplemental WDS Connector Configuration Guide</a> )
McAfee ePolicy Orchestrator	<i>McAfee ePolicy Orchestrator Installation Guide</i> <i>McAfee ePolicy Orchestrator Product Guide</i>
McAfee Client Proxy	<i>McAfee Client Proxy Product Guide</i> <i>McAfee Client Proxy SaaS Configuration and Implementation Product Supplement</i> <i>McAfee Client Proxy Release Notes</i>
McAfee Help Desk	<i>McAfee Help Desk Product Guide</i>
McAfee Content Security Reporter	<i>McAfee Content Security Reporter Quick Start Guide</i> <i>McAfee Content Security Reporter Product Guide</i>
McAfee Web Reporter	<i>McAfee Web Reporter Quick Start Guide</i> <i>McAfee Web Reporter Product Guide</i>

These documents can be found on <https://contentsecurity.mcafee.com>, <http://www.mcafee.com/us/downloads/downloads.aspx>, [https://portal.mcafeesaas.com/wds/configuration/mcpdownload.php?d\\_mcp\\_pdf](https://portal.mcafeesaas.com/wds/configuration/mcpdownload.php?d_mcp_pdf) or on <https://mysupport.mcafee.com/Eservice/Default.aspx>.

Copyright © 2014 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.