Migration Guide

McAfee Web Gateway Cloud Service

McAfee SaaS Web Protection to McAfee Web Gateway Cloud Service

For use with McAfee ePolicy Orchestrator Cloud
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 OR THE PLACE OF PURCHASE FOR A FULL REFUND.
5 Migrating a hybrid deployment

What is a hybrid deployment? ............................ 29
Getting started with a hybrid deployment ............... 29
Migration tasks for a hybrid deployment .................. 30
  Create a Client Proxy policy using McAfee ePO Cloud . 30
  Set up Web Gateway in a preproduction environment .... 31
  Create a Client Proxy policy using McAfee ePO .......... 31
  Test and roll out the hybrid configuration ............... 32

Index .................................................................... 35
Preface

This guide provides the information you need to work with your McAfee product.

Contents

› About this guide
› Find product documentation

About this guide

This information describes the guide’s target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

• **Administrators** — People who implement and enforce the company’s security program.

Conventions

This guide uses these typographical conventions and icons.

| **Italic** | Title of a book, chapter, or topic; a new term; emphasis |
| **Bold** | Text that is emphasized |
| **Monospace** | Commands and other text that the user types; a code sample; a displayed message |
| **Narrow Bold** | Words from the product interface like options, menus, buttons, and dialog boxes |
| **Hypertext blue** | A link to a topic or to an external website |

**Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method

**Tip:** Best practice information

**Caution:** Important advice to protect your computer system, software installation, network, business, or data

**Warning:** Critical advice to prevent bodily harm when using a hardware product
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.
This guide is intended for McAfee® Web Gateway Cloud Service (McAfee® WGCS) customers, who are migrating from the Control Console user interface to the McAfee® ePolicy Orchestrator® Cloud (McAfee® ePO® Cloud) management platform. New customers and hybrid customers, who use McAfee WGCS with McAfee® Web Gateway in an integrated solution, can also use this guide as a reference.

Contents

- **New product name**
- **Benefits of the Cloud Services platform**
- **Differences between the new service and the legacy service**
- **Setting up the products in the recommended order**
- **High-level migration tasks**

### New product name

The name of McAfee® SaaS Web Protection is changing to McAfee Web Gateway Cloud Service.

In this guide, the following terms are used to refer to the products.

- Legacy service — Refers to SaaS Web Protection.
- New service — Refers to McAfee WGCS.
- Cloud service — Refers to the legacy service, the new service, or both.
- Control Console — Refers to the legacy SaaS Web Protection user interface.
- Management console — Refers to the new McAfee WGCS user interface.

### Benefits of the Cloud Services platform

When you migrate to the new service, you benefit from the full functionality and flexibility that the Cloud Services platform offers.

The new service is delivered using the Cloud Services platform, which consists of globally distributed nodes called *points of presence* (PoP). The Global Routing Manager (GRM) is a DNS service that is responsible for intelligent traffic routing, load sharing, and failover. The GRM routes traffic to the best available point of presence.
Differences between the new service and the legacy service

The new service features a new policy model, management platform, and user interface. The new service also supports a different feature set than the legacy service.

New policy model

The new policy model is based on one policy that is applied globally across all users and groups in your organization. To customize the application of the policy to specific users or groups, you configure exceptions to the rules that make up the policy.

New management platform and user interface

The new service is delivered using the McAfee ePO Cloud management platform and console. The management console replaces the Control Console, as follows:

- The new service is configured using the management console.
- Cloud-based instances of McAfee® Client Proxy are configured using the management console.

Supported features

In this table, you can compare the features supported in the McAfee ePO Cloud management console with the features supported in the Control Console.

Table 1-1  Control Console versus McAfee ePO Cloud

<table>
<thead>
<tr>
<th>Features</th>
<th>Control Console</th>
<th>McAfee ePO Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Global Threat Intelligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL filtering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Website reputation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Gateway Anti-Malware Engine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature-based anti-virus technology</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Behavior emulation technology</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web filtering catalogs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Category</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Application</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Media Type</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee® Client Proxy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP address range</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAML 2.0</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Explicit user</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Account management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with Active Directory</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Local user group creation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 1-1  Control Console versus McAfee ePO Cloud (continued)

<table>
<thead>
<tr>
<th>Features</th>
<th>Control Console</th>
<th>McAfee ePO Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Console reports and forensics</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>McAfee ePO Cloud queries and reports</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Other features</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPsec on mobile devices</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

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

---

**Setting up the products in the recommended order**

McAfee WGCS works with McAfee ePO Cloud and McAfee Client Proxy. We recommend setting up these products in the following order.

1. **McAfee ePO Cloud** — This cloud platform features a management console, where you can manage McAfee WGCS and Client Proxy policies, authentication, and reporting. After creating an account in McAfee ePO Cloud, you can use the management console to set up the other products.
   
   For more information, see the *McAfee ePolicy Orchestrator Cloud Product Guide*. Or you can set up and manage Client Proxy using McAfee ePO on-premise. For more information, see the *McAfee ePolicy Orchestrator Product Guide*.

2. **McAfee WGCS** — McAfee hosts and updates this service in the cloud. Because McAfee WGCS is a cloud service, you do not need to install or upgrade the software. For accessing the management console, you need the email address and password that you provided when you created your McAfee account.

3. **McAfee Client Proxy** — Setup depends on whether you are using the McAfee ePO or McAfee ePO Cloud. For both management platforms, setup includes deploying the client software to the endpoint computers in your organization, configuring a Client Proxy policy, and pushing the policy to the endpoint.

   For more information, see the *McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator* or *McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator Cloud*.

   *McAfee WGCS can also be deployed without Client Proxy.*

---

**High-level migration tasks**

To test the new policy and roll it out gradually, perform these high-level migration tasks in the specified order.

1. **Subscribe to the new service, activate it, and log on to McAfee ePO Cloud.** Navigate to the welcome page, and save your new **Customer ID** and **Customer Specific Proxy** value.

2. **Set up communication with Client Proxy.**

3. **Configure the new policy.**
4 Configure authentication.

5 Test the new policy and roll it out gradually.

**Best practice: Configuring the new policy before authentication**

In the management console, configure the new policy before you configure authentication. When the end user is authenticated using the method you configure in the management console, the new policy is applied. If the new policy is not configured yet, the default policy settings that come with the new service are applied.

For each authentication method, we provide steps that you can take to roll out the new policy gradually.

For information about migrating a hybrid deployment, see the chapter: *Migrating a hybrid deployment.*
Getting started

The McAfee ePO Cloud welcome page provides the information you need to integrate McAfee WGCS with other products, such as Client Proxy and Web Gateway.

Contents
- Before activating the new service
- After activating the new service
- Log on to McAfee ePO Cloud
- Managing Client Proxy with McAfee ePO or McAfee ePO Cloud
- Configuring redirection with Client Proxy
- Related product documentation and KB articles
- Useful links

Before activating the new service

Review information about whitelisting IP address ranges in your firewall and using a geolocation prefix.

Whitelisting IP address ranges in your firewall

If you are using a firewall to restrict Internet access, configure the firewall to allow traffic to all points of presence in your geographic area. For a complete list of IP address ranges in each area, visit: trust.mcafee.com.

Using a geolocation prefix

When configuring McAfee WGCS as the proxy server, you can include a prefix that specifies the geographic location you want the Global Routing Manager to use when routing your traffic. For more information and use cases, see KB article KB87631.

After activating the new service

After you activate the new service, you can still run your legacy policies and use the Control Console. You can view the Control Console while you configure a new policy in the McAfee ePO Cloud management console. And, as a customer of the new service, you benefit from the full functionality and flexibility that the Cloud Services platform offers.
Log on to McAfee ePO Cloud

Subscribe to the new service and activate it. Create an account in McAfee ePO Cloud, log on, and locate the welcome page.

When logging on to McAfee ePO Cloud for the first time, you create an account. The email address and password that you provide are your McAfee ePO Cloud credentials. If you are migrating a hybrid deployment, you need these values when updating the hybrid configuration for the new service in Web Gateway.

The welcome page provides this information:

- **Customer ID** — Uniquely identifies the customer in the system.
- **Customer Specific Proxy** — Specifies the domain name that other products use when connecting to your instance of the new service.

  The domain name has the form: \(c<\text{customer_id}\.\text{saasprotection.com}\).

**Example:** \(c12345678\.\text{saasprotection.com}\)

Save these values. Client Proxy uses the customer-specific proxy to connect to your instance of the new service. Hybrid customers need the customer ID when configuring policy synchronization in the Web Gateway user interface.

**Task**

1. Subscribe to the new service.

   The system sends you a welcome email.

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

3. On the activation page, enter your email address and a password.

   The service is activated.

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

   The management console opens.

5. Click the menu icon in the upper-left corner, then select **Web Protection | Getting Started**.

   The welcome page opens.

Managing Client Proxy with McAfee ePO or McAfee ePO Cloud

Client Proxy management depends on whether you are using the on-premise and cloud version of McAfee ePO.

**Managing Client Proxy with McAfee ePO**

If you plan to continue managing Client Proxy using McAfee ePO or you are managing Client Proxy using McAfee ePO for the first time, synchronize the policy with McAfee ePO Cloud:
1 Using McAfee ePO Cloud, create a Client Proxy policy for the new service. Export the credentials you configured for the policy to an .xml file.

2 Using McAfee ePO, create a Client Proxy policy for the new service. Configure the credentials by importing them from the .xml file you created earlier.

For more information, see the McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator.

Managing Client Proxy with McAfee ePO Cloud

If you plan to manage Client Proxy with McAfee ePO Cloud, first install a fresh instance of McAfee Agent:

1 Install a fresh instance of the McAfee Agent on the computers of end users in your organization, as follows.
   • Using McAfee ePO Cloud, create an installation URL.
   • Send the installation URL and steps to end users, who can then access the URL and complete the installation steps.

2 Using McAfee ePO Cloud, create a Client Proxy policy for the new service.

For more information, see the McAfee Client Proxy Product Guide for use with McAfee ePolicy Orchestrator Cloud.

Configuring redirection with Client Proxy

Configure a Client Proxy policy and assign it to the end-user computers in your organization. When the shared password is synchronized with McAfee WGCS, the policy takes effect, and Client Proxy starts redirecting network traffic to McAfee WGCS.

In the McAfee ePO or McAfee ePO Cloud management console:

1 Configure a Client Proxy policy, including these settings.

   a Proxy Server Address — To configure McAfee WGCS as the proxy server, specify the Customer Specific Proxy from the welcome page as the proxy server address.

   b Unique Customer ID — (McAfee ePO only) Specify your customer ID.

   c Shared Password — Specify the shared password that Client Proxy and McAfee WGCS use to communicate.

   d 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 the end user’s computer is located outside the network and not connected by VPN.

2 Deploy the Client Proxy software to the computers of end users in your organization.

3 Assign the Client Proxy policy to the end-user computers.

Changing the shared password

After you assign the Client Proxy policy to the end-user computers 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 computers of end users in your organization. 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.

![Warning]
The shared password must be synchronized with McAfee WGCS, or authentication fails.

---

**Related product documentation and KB articles**

These product guides and KB articles provide information about the new service and the products that integrate with it. They are available on the ServicePortal.

**Product documentation**

- McAfee Client Proxy 2.3.0 Product Guide for ePolicy Orchestrator
- McAfee Client Proxy 2.3.0 Product Guide for ePolicy Orchestrator Cloud
- McAfee ePolicy Orchestrator 5.3.0 Product Guide
- McAfee ePolicy Orchestrator Cloud 5.9.0 Product Guide
- McAfee Web Gateway 7.7.0 Product Guide
- McAfee Web Gateway Cloud Service Product Guide
- McAfee Web Gateway Cloud Service Release Notes

**KB articles to review before you begin**

- KB87232 Web Gateway Cloud Service IP addresses/ranges to whitelist in your firewall
- KB87631 How to configure Web Gateway Cloud Service country-specific and region-specific prefixes

**KB articles for customers who are new to McAfee ePO Cloud**

- KB78045 FAQs for ePolicy Orchestrator Cloud
- KB84630 How to deploy products using ePolicy Orchestrator Cloud

---

**Useful links**

Use these links to integrate other products, open the Control Console and McAfee ePO Cloud logon pages, and open the tool for converting policy lists. You can also see an overview of the Cloud Services platform and access related McAfee Community articles.

**Proxy service domain name**

The cloud service is a proxy service. Use the proxy service domain name when configuring other products that integrate with the new cloud service.

- saasprotection.com — Specifies the domain name of the new cloud proxy service.
- c<customer_id>.saasprotection.com — Specifies the customer-specific domain name of the new cloud proxy service.
Useful links

• Open the Control Console logon page:
  portal.mcafeesaaS.com

• Open the McAfee ePO Cloud logon page:
  manage.mcafee.com

• Open the tool for converting policy lists:
  contentsecurity.mcafee.com/migration-tools

• See an overview of the Cloud Services platform:
  trust.mcafee.com

• Access related McAfee Community articles:
  community.mcafee.com/community/business/expertcenter/products/wgcs
Policy migration

To configure a new policy, you can start with the standard policy options and gradually customize them for your organization. You can export your trusted sites lists from the Control Console, format and organize them using a conversion tool, and then import them using the McAfee ePO Cloud management console.

Contents
- Policy Management user interface
- Using the standard policy options
- Migrating policy lists
- Organizing trusted sites lists
- Migrating allow and deny settings

Policy Management user interface

In the new user interface, standard policy options are provided as templates for each policy configuration area.

For more information, see the Policy management chapter in the McAfee Web Gateway Cloud Service Product Guide.

Policy Browser

Instead of configuring many policies in a tabbed interface, as you do in the Control Console, you configure one policy in an integrated interface called the Policy Browser.

In the Policy Browser, you expand and collapse policy configuration areas, such as Web Reputation, as needed, allowing you to view more than one area at a time. In each area, you can select a rule and view the Rule Details pane alongside the other rules configured for that area.

To open the browser, click the menu icon in the upper-left corner of the McAfee ePO Cloud management console. Then select Unified Security Policy | Policy Management.

Policy configuration areas

While the policy configuration areas are the same in the Control Console and in the Policy Browser, they are organized differently.

In the Policy Browser, each configuration area or feature includes one or more standard policy options that you can select and change. For example, the Web Category Filter area includes the following policy options:
These names are similar to the names of the sample policies that come with the Control Console. However, the standard policy options have been updated to reflect how customers edit the default settings.

**Table 3-1 Policy configuration areas**

<table>
<thead>
<tr>
<th>Control Console (tabs)</th>
<th>Policy Browser (configuration areas or features)</th>
<th>Standard policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Policy Name — One policy applies globally and is not named. Owner — You can add user groups to allow and block rules.</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat</td>
<td>Web Reputation</td>
<td>Restrictive Permissive</td>
</tr>
<tr>
<td></td>
<td>Anti-Malware Filter</td>
<td>Basic Protection</td>
</tr>
<tr>
<td>Category</td>
<td>Web Category Filter</td>
<td>Restrictive Limited Permissive Very Permissive</td>
</tr>
<tr>
<td>Applications</td>
<td>Web Application Filter</td>
<td>Restrictive Limited Permissive</td>
</tr>
<tr>
<td>Media</td>
<td>Media Type Filter</td>
<td>Restrictive Limited Permissive</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL Scanner</td>
<td>Basic Protection</td>
</tr>
</tbody>
</table>
| Blocked Sites          | **Global Settings** consists of these global URL lists:  
|                        | • Global URL Whitelist  
|                        | • Global URL Blacklist  | Basic Rules |
| Notifications          | For each configuration area and policy option, you can configure a block page. You can copy your block messages from the **Notifications** tab in the Control Console and paste them in the **New Block Page** dialog box in the Policy Browser. | N/A                     |
Rule order
Each standard policy option consists of an ordered list of rules. Rules in the list are applied from top to bottom. When you configure a policy area, you place higher priority rules above lower priority ones.

The first rule in each list is a URL whitelist for you to configure. Most lists include a catch-all rule at the bottom. Any unprocessed web requests are allowed or blocked depending on the configuration of the catch-all rule. In general, the catch-all rule for a permissive policy might allow the remaining requests, while the catch-all rule for a restrictive policy might block them.

URL whitelists and blacklists
In the Policy Browser, trusted sites lists and blocked sites lists are called URL whitelists and URL blacklists, respectively.

Locating lists in the Policy Browser
This table shows how the lists that you export from the Control Console map to the lists in the Policy Browser.

<table>
<thead>
<tr>
<th>List name in the Control Console</th>
<th>List name and location in the Policy Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Scan Bypass list</td>
<td>SSL Scanner</td>
</tr>
<tr>
<td>Category Filter Bypass list</td>
<td>Web Category Filter</td>
</tr>
<tr>
<td>Media Filter Bypass list</td>
<td>Media Type Filter</td>
</tr>
<tr>
<td>Anti-Malware Bypass list</td>
<td>Anti-Malware Filter</td>
</tr>
<tr>
<td>Blocked Sites list</td>
<td>Global Settings</td>
</tr>
</tbody>
</table>

New policy lists
The Policy Browser provides these additional URL whitelists for you to configure:

- Global Settings | Global URL Whitelist
- Web Reputation | Web Reputation URL Whitelist
- Web Application Filter | Web Application URL Whitelist

User groups
If your organization’s Active Directory is synchronized with McAfee ePO Cloud, you can add your Active Directory groups to allow and block actions for each policy rule.

For example, you might add a user group named executives to the allow action for the Streaming rule in the Web Category Filter area. If you want to allow executives, but no one else, you can configure this in one rule rather than having to create another policy, as is required in the Control Console. To do so, use the allow action for executives and the block action for everyone else.

When a policy configuration area is expanded, you can view which user groups are allowed and blocked for each rule in that area.

For information about synchronizing your organization’s Active Directory with McAfee ePO Cloud, see the McAfee ePO Orchestrator Cloud Product Guide.
Using the standard policy options

You can begin by using the standard policy options, then gradually customize them for your organization.

Select the standard policy option in each configuration area that best meets your organization's needs. Remember the following:

- Only one policy option is active per configuration area at a time.
- You can select the restrictive option for one configuration area and the permissive option for another.

Migrating policy lists

You can export your trusted sites and blocked sites lists from the Control Console to .csv files and then import the files when configuring the new policy in McAfee ePO Cloud.

1. In the Control Console, export these trusted sites lists to .csv files:
   - Anti-Malware Bypass list
   - Category Filter Bypass list
   - Media Filter Bypass list
   - SSL Scan Bypass list

2. In the Control Console, export the Blocked Sites list to a .csv file.

3. Format the .csv files for the new service.

4. In the McAfee ePO Cloud management console, import the .csv files.

For a step-by-step procedure, see Import a list of URLs in the McAfee Web Gateway Cloud Service Product Guide.

See also

Use the conversion tool when migrating policy lists on page 23

Formatting policy lists for the new service

When migrating policy lists from the Control Console to the McAfee ePO Cloud management console, format the lists for the new service.

Trusted sites and blocked sites lists are exported from the Control Console to .csv files, which are then imported using the management console. Before the lists are imported, they must be formatted to meet the requirements of the new service. Formatting can be done manually using a text editor or automatically using the conversion tool provided by McAfee.

Policy lists consist of domain names and IP addresses. The conversion tool verifies that the list entries are fully qualified domain names or valid IPv4 or IPv6 addresses.
How legacy and new policy lists differ

In the .csv files, legacy and new policy lists are formatted differently, as follows:

- **Legacy policy lists** — Consist of one column having the header `host` and values such as these.

  ```
  "host"
  "adp.com"
  "216.58.194.142"
  "ebay.com"
  "etrade.com"
  "java.com"
  "2607:f8b0:4005:805::200e"
  ```

- **New policy lists** — Consist of two columns having the header `URL,Subdomain(True/False)` and comma-separated values such as these.

  ```
  "URL","Subdomain(True/False)"
  "adp.com","True"
  "216.58.194.142","False"
  "ebay.com","True"
  "etrade.com","True"
  "java.com","True"
  "2607:f8b0:4005:805::200e","False"
  ```

McAfee WGCS accepts .csv files having this two-column format whether the values are enclosed in quotation marks or not.

Formatting a new policy list

When formatting a new policy list, consider the following information.

- **Header row** — The header row is optional. If you include a header row, select the **This file contains a header row** checkbox in the **Import List** dialog box.

- **URL column** — This column lists the domain names or IP addresses of the trusted or blocked sites.

- **Subdomain column** — These true/false values are required and specify the following. They are not case sensitive.
  - **True** — Specifies that all subdomains are trusted or blocked by the new service. In the Control Console, domain names always include the subdomains. So when converting legacy domain name entries, set the value in the subdomain column to true.
  - **False** — Specifies that the domain name alone is trusted or blocked by the new service. When converting legacy IP address entries, set the value in the subdomain column to false.

Formatting domain names for policy lists

Follow these guidelines when formatting domain names for URL whitelists and blacklists.

Formatting domain names for URL lists

McAfee WGCS supports domain names having these formats:
• host.domain.tld/path
• host.domain.tld
• domain.tld/path
• domain.tld

host — Specifies the DNS name of the host
domain — Specifies the name of the subdomain
tld — Specifies the top-level domain
path — Specifies the path to the web resource

McAfee WGCS automatically includes the path and any sub paths, which is the same as placing an asterisk after the path in the domain name:
• host.domain.tld/path*
• domain.tld/path*

But because the sub paths are always included, there is no need to add the asterisk.

All subdomains setting
This setting determines whether McAfee WGCS applies policy rules to the domain and all subdomains or to the domain only. You can specify all subdomains, as follows:
• In the Policy Browser user interface — Select the All subdomains checkbox when adding a URL to a URL list.
• In a .csv file specifying a URL list — Set the value in the Subdomain(True/False) column to True.

Specifying all subdomains has the same effect as adding "*." at the beginning of each domain name:
• *.host.domain.tld/path
• *.host.domain.tld
• *.domain.tld/path
• *.domain.tld

Benefits of using the conversion tool
The conversion tool simplifies migration of your policy lists from the Control Console to the McAfee ePO Cloud management console.

Instead of manually formatting individual policy lists using a text editor, you can automatically format one or more lists for the new service using the conversion tool provided by McAfee. The conversion tool has these benefits.
• Formatting — The conversion tool formats the exported .csv files, so that the policy lists meet the formatting requirements of the new service.
• Option to merge multiple lists — Using the conversion tool, you can easily merge two or more lists. When merging lists, the tool removes duplicate entries.
• Validation — The conversion tool verifies that the list entries are fully qualified domain names or valid IPv4 or IPv6 addresses.
**Merging policy lists: an example**

When migrating policy lists from the Control Console to the management console, you might want to consolidate them. For example, you can consolidate the trusted sites lists on the Category tab in the Control Console across all your policies into one URL whitelist. Then, in the management console, you can import the consolidated list as the Web Category URL Whitelist.

**Use the conversion tool when migrating policy lists**

Use the conversion tool to format, optionally merge, and validate policy lists for the new service.

**Before you begin**

In the Control Console, export all policy lists that you want to import using the McAfee ePO Cloud management console to .csv files.

Save the .csv files in one folder that you can access easily.

**Task**

1. To open the conversion tool, click this link: [contentsecurity.mcafee.com/migration-tools](http://contentsecurity.mcafee.com/migration-tools).

2. Scroll down, click Browse, then navigate to the folder holding the .csv files whose format you want to convert.

3. Select one or more files to convert, then click Open.

   When multiple files are selected, they are merged by the conversion tool, which removes duplicate entries.

4. In the conversion tool, click Convert Files.

5. In the Opening migrated-list.csv dialog box, click Save File.

6. Specify a meaningful file name, then click Save.

   The .csv file is saved with a new header row and two-column format.

**Organizing trusted sites lists**

Organize your trusted sites into lists according to the URL whitelists you want configured in the Policy Browser. From these lists, create .csv files and import them in the Policy Browser.

By design, the Policy Browser has fewer URL whitelists to configure and maintain. You start by configuring one URL whitelist for each configuration area and policy option that you plan to use. For example, in the Web Reputation area, you might configure one URL whitelist for the restrictive policy option and another for the permissive option.

The Policy Browser comes configured with URL whitelist rules for the following configuration areas and policy options. The whitelists are empty and ready for you to configure. Except for the Web Reputation area, you can create and configure additional URL whitelist rules as needed.

- Global URL Whitelist
- Web Reputation, Restrictive
- Web Reputation, Permissive
- Anti-Malware, Basic
- Web Application, Restrictive
- Web Application, Limited
- Web Application, Permissive
- Media Type, Restrictive
Organizing your trusted sites into lists for the Policy Browser requires a different view of policy lists. Instead of configuring trusted sites for each user group, think of the configuration area and policy option. For example, which URLs do you want to bypass the Web Reputation filter when: The restrictive policy option is selected? The permissive policy option is selected?

Migrating allow and deny settings

Instead of configuring many separate rules for each Web Category, Web Application, and Media Type area, you can start by configuring one rule for each area and policy option you plan to use. Later, you can add and refine the rules.

In the following example, the settings on the Category tab in the Control Console are configured in the Web Category Filter area in the Policy Browser.

To view the categories in the Control Console, select the Category tab, then click Expand All. The categories, such as Business/Services and Drugs, are the names of lists and rules in the Policy Browser.

In the Policy Browser, create one list and rule for all categories that you want blocked. Configure the rule with a Block action. Although this rule applies across your organization, you can add exceptions to it.

In the Policy Browser, take these steps:

1. Expand the Web Category Filter area, select a policy option, then click a rule.
2. Click the Policy Browser menu icon.
3. From the drop-down list, select New Web Category Rule.
4. Click the Catalog menu icon, then click New List.
5. Specify a name for the list, then using the Search field to locate the categories you want to block, add each one to the list.
6. Click Save.
   The new list is added to the list of web categories.
7. Select the new list and add it to the Rule Details pane.
8. In the Rule Details pane, click the edit icon, set the primary rule action to Block, then click Save.
   The new list is added to the Web Category Filter area as a rule.
9. Optionally, add one or more user groups, which are allowed to access the blocked web categories.
Configuring authentication

For each authentication method, we provide an example of configuration steps that you can use to roll out the new policy gradually.

Contents
- Supported authentication methods
- When the new policy is applied depends on the authentication method
- Rolling out the new policy with Client Proxy authentication
- Rolling out the new policy with IP range authentication
- Rolling out the new policy with SAML authentication

Supported authentication methods

The following table shows which authentication methods are supported in the McAfee ePO Cloud management console and where they are configured.

### Table 4-1  Supported authentication methods

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Supported in Control Console</th>
<th>Supported in McAfee ePO Cloud</th>
<th>Where configured in McAfee ePO Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Proxy</td>
<td>yes</td>
<td>yes</td>
<td>Policy</td>
</tr>
<tr>
<td>IP address range</td>
<td>yes</td>
<td>yes</td>
<td>Web Protection</td>
</tr>
<tr>
<td>SAML 2.0</td>
<td>no</td>
<td>yes</td>
<td>n/a</td>
</tr>
<tr>
<td>Explicit user</td>
<td>yes</td>
<td>no</td>
<td>n/a</td>
</tr>
</tbody>
</table>

If you are using explicit user authentication in the Control Console, you must configure another authentication method in McAfee ePO Cloud. In addition to Client Proxy and IP address range authentication, you have the option of configuring SAML 2.0 authentication.

When the new policy is applied depends on the authentication method

The new policy is applied when the authentication result includes the new customer ID.

The cloud backend service processes end-user requests, as follows:

1. The service authenticates the user and, through the authentication process, identifies the customer.
2. If the customer ID is your old ID, the service applies your legacy policies. If the customer ID is your new ID, the service applies the new policy.

When the new policy is applied depends on the authentication method. For this reason, we recommend a different migration path for each method.
## Authentication method

<table>
<thead>
<tr>
<th>The new policy is applied when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP range</td>
</tr>
<tr>
<td>One or more IP address ranges are configured in McAfee ePO Cloud and an end user sends a web request from one of the configured ranges.</td>
</tr>
<tr>
<td>SAML 2.0</td>
</tr>
<tr>
<td>SAML authentication is configured and an end user sends a web request to the new SAML service port: 8084.</td>
</tr>
<tr>
<td>Client Proxy</td>
</tr>
<tr>
<td>1 The shared password is reset in McAfee ePO or McAfee ePO Cloud.</td>
</tr>
<tr>
<td>2 The new Client Proxy policy is deployed to the client computers in your organization.</td>
</tr>
<tr>
<td>3 An end user sends a web request from one of these computers.</td>
</tr>
</tbody>
</table>

## Rolling out the new policy with Client Proxy authentication

You can roll out the new policy gradually when configuring Client Proxy authentication.

In this topic, the new policy is referred to as the new cloud policy to differentiate it from the Client Proxy policy.

### How Client Proxy authentication is configured

The new service supports Client Proxy deployment using McAfee ePO (on-premise) or McAfee ePO Cloud.

<table>
<thead>
<tr>
<th>If you are using...</th>
<th>You can...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit authentication configured in the Control Console</td>
<td>Create a Client Proxy policy from scratch using McAfee ePO or McAfee ePO Cloud.</td>
</tr>
<tr>
<td>Client Proxy authentication configured in the Control Console</td>
<td>Configure the Client Proxy policy using McAfee ePO or McAfee ePO Cloud.</td>
</tr>
<tr>
<td>Client Proxy authentication configured in McAfee ePO</td>
<td>Configure the Client Proxy policy using McAfee ePO or McAfee ePO Cloud.</td>
</tr>
</tbody>
</table>

If you are using McAfee ePO, make sure that you update the following settings in your existing policy:

- **Proxy Servers** — Add your customer-specific proxy to the top of the list.
- **Unique Customer ID** — Specify your new customer ID.
- **Shared Password** — Reset your shared password.

### Applying the new cloud policy

When the Client Proxy software sends web requests from end users to the cloud service, the requests include the customer ID. If the customer ID is the new ID, the cloud service applies the new cloud policy.
Best practice: Rolling out the new cloud policy gradually

1. Open the McAfee ePO or McAfee ePO Cloud management console.
2. From the main menu, select Policy | Policy Catalog.
3. In the Policy Catalog, configure and save the Client Proxy policy.
4. From the main menu, select Systems | System Tree.
5. In the System Tree, select one or more groups in your organization on which you want to test the new cloud policy. If needed, you can set up a test group for this purpose.
6. On the Assigned Policies tab, assign the policy to the selected group or groups.
7. On the Assigned Client Tasks tab, schedule the policy deployment.

   Allow time for the policy to be deployed and the password to be shared with the cloud service. For information about how much time to allow, see Configuring redirection with McAfee Client Proxy in the Getting started chapter.

8. When you are satisfied that your new cloud policy works as you intend, you can deploy the Client Proxy policy across your organization.

Rolling out the new policy with IP range authentication

You can roll out the new policy gradually when configuring IP range authentication.

IP address ranges are stored in one database and can only be used by one customer. As both an existing customer with one ID and a new customer with another ID, you must migrate the IP ranges you want to use from the Control Console to the management console. Before adding an IP range to the configuration in the management console, you must remove it from the configuration in the Control Console.

When you add an IP range to the new list in the management console, the cloud service applies the new policy to requests coming from that IP range. Because IP ranges are cached, your legacy policies might be applied instead of the new policy for up to 24 hours.

Best practice: Rolling out the new policy gradually

Roll out the new policy gradually when configuring IP range authentication in the management console, using these steps as an example.

1. Prepare to configure the new policy:
   a. In the Control Console, export your policy lists to .csv files.
   b. In the management console, import your lists from the .csv files.

   Do not import the list of IP address ranges at this step in the process.

2. Configure the new policy.

3. Prepare to test the new policy with one IP address range:
   a. In the Control Console, remove the IP address range that you want to test from the list of configured ranges.
   b. In the management console, add this IP address range to the IP Range List.
4 Test the new policy with one IP address range.

5 To test the new policy with additional locations, migrate the corresponding IP address ranges from the Control Console to the management console.

6 When you are satisfied that the new policy works as you intend, you can migrate any remaining IP address ranges from the Control Console to the management console.

The new policy is applied across your organization.

---

**Rolling out the new policy with SAML authentication**

You can roll out the new policy gradually when configuring SAML authentication.

**High-level SAML configuration tasks**

SAML authentication requires these high-level configuration tasks:

1. Configure SAML authentication in your identity provider.
2. Configure SAML authentication in McAfee ePO Cloud.
3. Configure SSL scanning in McAfee ePO Cloud.
4. Configure the proxy server setting in the browsers of client computers in your organization, as follows:
   
   c<customer_id>.saasprotection.com:8084
   
   Where:

   customer_id — Specifies your customer ID.

   saasprotection.com — Specifies the domain name of the new cloud service.

   8084 — Specifies the port number of the cloud SAML service.

   **Do not update the proxy server setting in the client browsers until you are ready to test and roll out the new policy.**

**Applying the new policy**

When you configure SAML authentication in the McAfee ePO Cloud management console, you specify the domain names that identify your organization. To identify the customer, the SAML service extracts the domain name from the end user’s email address and compares it to the names that you provide. When there is a match, the service applies the new policy.

**Best practice: Rolling out the new policy gradually**

After completing configuration tasks 1–3, you can test and roll out the new policy. To roll out the policy gradually, update the proxy server setting to the SAML service in a limited number of client browsers. Test the new policy using these client computers first. Continue updating the proxy server setting in your client browsers and testing the new policy until you are satisfied that it works as you intend. When the proxy server setting is updated in all client browsers, the new policy is applied across your organization.
Migrating a hybrid deployment

When migrating a hybrid deployment, consider the following information.

Contents
- What is a hybrid deployment?
- Getting started with a hybrid deployment
- Migration tasks for a hybrid deployment

What is a hybrid deployment?

In a hybrid deployment, Web Gateway and McAfee WGCS are deployed together. The web protection policy is configured in the Web Gateway user interface and pushed to McAfee WGCS at the synchronization interval you specify. Together, the on-premise and cloud components of the hybrid solution protect your organization from threats that might arise when users access the web from inside or outside your network.

Other components of a hybrid deployment include:
- **Client Proxy** — This software, when installed on the endpoint, is aware of the end user's location and redirects network traffic or lets it pass, accordingly:
  - Users working inside the network or connected to the network by VPN — Client Proxy lets network traffic pass to Web Gateway for filtering.
  - Users working outside the network — Client Proxy redirects network traffic to McAfee WGCS for filtering.
- **McAfee ePO** — Use this management platform to manage Client Proxy when the software is installed on your network.
- **McAfee ePO Cloud** — Use this management platform to manage McAfee WGCS and cloud-based instances of Client Proxy.

Getting started with a hybrid deployment

To get started with a hybrid deployment, you need your McAfee ePO Cloud credentials and your customer ID.

Follow the same initial steps as you do for a cloud-only deployment. When logging on to McAfee ePO Cloud for the first time, you create an account. The email address and password that you provide are your McAfee ePO Cloud credentials. Save these for later use.

To view your customer ID, locate the **Web Protection** welcome page. Save your ID for later use.
Migration tasks for a hybrid deployment

Create a Client Proxy policy for the new service, configure a hybrid deployment in a preproduction environment, test the hybrid configuration, then roll it out in the production environment.

These migration tasks assume that you are managing Client Proxy using McAfee ePO. For information about managing Client Proxy using McAfee ePO Cloud only, see the Getting Started chapter.

The following tasks set up synchronization among the hybrid components: Web Gateway, McAfee WGCS, Client Proxy, McAfee ePO, and McAfee ePO Cloud.

1. Using the McAfee ePO Cloud management console: Create a Client Proxy policy for the new service. Export the credentials to an .xml file. Save this file for import when creating the Client Proxy policy using McAfee ePO.

2. Set up an instance of Web Gateway in a preproduction environment with a production configuration. Configure the hybrid settings, then manually push the Web Gateway policy to McAfee WGCS. As a result of this task, Web Gateway is synchronized with McAfee WGCS.

3. Using the McAfee ePO management console: Create a Client Proxy policy for the new service. Import the credentials from the .xml file that you saved earlier. This task allows synchronization of Client Proxy software installed on your network with McAfee WGCS and McAfee ePO Cloud.

4. Test the hybrid configuration in the preproduction environment, then roll it out in the production environment.

Create a Client Proxy policy using McAfee ePO Cloud

In the McAfee ePO Cloud management console, create a Client Proxy policy for the new service.

You create the policy with a new shared password and export your Client Proxy credentials to an .xml file. This file contains the shared password and your customer ID. Later, you can import your credentials from the file when configuring the policy using McAfee ePO.

For more information, see the McAfee Client Proxy Product Guide for McAfee ePolicy Orchestrator Cloud.

Task

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

2. From the Product drop-down list, select the current version of McAfee Client Proxy.

3. To create a policy, duplicate the McAfee Default policy, specify a name for the new policy, then click OK. The policy is added to the policy list.

4. To configure the policy for the new service, click the name of the policy in the policy list.

   The Client Proxy Settings open.

5. In the Proxy Servers window, specify the customer-specific proxy from the Web Protection welcome page for the Proxy Server Address.

6. In the Client Configuration window, specify a new value for the Shared Password.

7. Export your customer credentials to an .xml file, and save the file for later use.

8. Configure other settings as needed, and save the policy.
Set up Web Gateway in a preproduction environment

After setting up a Web Gateway instance in a preproduction environment with a production configuration, configure the hybrid settings. Then manually push the Web Gateway policy to McAfee WGCS.

**Before you begin**

Using the back up and restore feature of Web Gateway, back up the production configuration to a file and restore it on the preproduction instance. When you restore the configuration, only restore the policy.

To locate this feature, select Troubleshooting, then select Backup/Restore below the name of the appliance.

When Web Gateway and McAfee WGCS are deployed using a hybrid configuration, the web protection policy is configured using Web Gateway. The policy is then pushed to the cloud at the synchronization interval you specify. For testing and validation purposes, you manually push the policy to the cloud.

For more information, see the Hybrid solution chapter in the McAfee Web Gateway Product Guide.

**Task**

1. In the preproduction environment, open the Web Gateway user interface, then select Configuration | Cluster | Web Hybrid.

   The Web Hybrid Configuration window opens.

2. To enable hybrid synchronization and configure the hybrid settings, select the Synchronize policy to SaaS checkbox.

3. Using your McAfee ePO Cloud credentials and McAfee WGCS customer ID, configure these hybrid settings.
   - **SaaS address** — Specifies the address that Web Gateway uses to communicate with McAfee WGCS.
     Value: https://msg.mcafeesaas.com:443
   - **SaaS administrator account name** — Specifies your McAfee ePO Cloud user name.
   - **SaaS administrator account password** — Specifies your McAfee ePO Cloud password.
   - **SaaS customer ID** — Specifies your McAfee WGCS customer ID.

4. If needed, update the rule sets that are enabled for the cloud.

   To locate these settings, select Policy | Rule Sets.

5. Configure other settings as needed, and save the policy.

6. Manually push the policy to McAfee WGCS.

   To locate this function, select Troubleshooting, then select SaaS Synchronization below the name of the appliance. In the SaaS Synchronization window, click Synchronize.

You can verify that McAfee WGCS is synchronized with Web Gateway. From the McAfee ePO Cloud menu, select Unified Security Policy | Policy Management. The Policy Browser opens to a Policy Unavailable message that provides information about the hybrid synchronization.

Create a Client Proxy policy using McAfee ePO

In the McAfee ePO management console, create a Client Proxy policy for the new service.

To configure the Unique Customer ID and Shared Password, you import the .xml file containing the credentials that you exported from McAfee ePO Cloud.
For more information, see the *McAfee Client Proxy Product Guide for McAfee ePolicy Orchestrator*.

**Task**

1. From the McAfee ePO menu, select **Policy > Policy Catalog**.

2. From the **Product** drop-down list, select the current version of McAfee Client Proxy.

3. To create a policy, duplicate the **McAfee Default** policy, specify a name for the new policy, then click **OK**. The policy is added to the policy list.

4. To configure the policy for the new service, click the name of the policy in the policy list. The **Client Proxy Settings** open.

5. In the **Proxy Servers** window, specify the customer-specific proxy from the welcome page for the **Proxy Server Address**.

6. In the **Client Configuration** window, import the .xml file that you exported from McAfee ePO Cloud. This file contains your customer ID and shared password.

7. Configure other settings as needed, and save the policy.

**Test and roll out the hybrid configuration**

After you test the hybrid configuration in a preproduction environment, you can roll it out in your production environment.

After setting up a hybrid configuration, you deploy it by assigning the new Client Proxy policy to the endpoint. The endpoint can be a few end-user computers in a preproduction environment or the end-user computers across your organization in a production environment.

Allow enough time for the policy to be updated on the endpoint and for the password to be shared with McAfee WGCS. After these steps complete, the new cloud policy is applied.

> The shared password must be synchronized with McAfee WGCS, or authentication fails. For more information, see *Configuring redirection with Client Proxy* in the **Getting Started** chapter.

**Testing the hybrid configuration in a preproduction environment**

Deploy the hybrid configuration in a preproduction environment.

1. Using McAfee ePO, assign the new Client Proxy policy to the endpoint computers that you are using to test the hybrid configuration.

2. When an end user sends a web request from one of these computers, the new Client Proxy policy is applied.

3. If the web request is from a computer located outside the network, Client Proxy directs the request to McAfee WGCS.

4. Because the request includes your new customer ID, the cloud service applies the new cloud policy.

**Rolling out the hybrid configuration in the production environment**

After you finish testing, roll out the hybrid configuration in the production environment.
1. In the preproduction environment, disable hybrid synchronization. This setting is located in the Web Gateway user interface.

2. In the production environment, enable hybrid synchronization and configure the hybrid settings. These settings are located in the Web Gateway user interface.

3. Using McAfee ePO, assign the new Client Proxy policy to the endpoint computers in your organization.

The new Client Proxy and cloud policies are applied across your organization.
Migrating a hybrid deployment
Migration tasks for a hybrid deployment
Index

A
about this guide 5
Active Directory 19
All subdomains setting 21
allow and deny settings, migrating 24
authentication methods
Client Proxy 26
IP range 27
SAML 28
supported 25

B
best practices
configuring the new policy 9
rolling out the new policy gradually 26–28
block pages 17

C
Client Proxy
configuring redirection 13
creating a policy using McAfee ePO 31
creating a policy using McAfee ePO Cloud 30
managing on McAfee ePO and McAfee ePO Cloud 12
Client Proxy authentication 25, 26
cloud service
differences between legacy and new 8
legacy and new 7
Cloud Services platform
benefits 7
link to status 14
Control Console 7
link to log on page 14
supported features 8
conventions and icons used in this guide 5
customer ID 29
Customer ID 12
Customer Specific Proxy 12, 13

D
documentation
audience for this guide 5
product-specific, finding 6
typographical conventions and icons 5

G
geolocation prefix, using 11

H
hybrid configuration
testing and rolling out 32
Web Gateway 31
hybrid deployment 12, 29, 30

I
IP address ranges, white-listing in your firewall 11
IP range authentication 25, 27

K
KB articles, related 14

L
lists, global URL 17

M
management console 7
McAfee Community
link to articles 14
McAfee ePO Cloud
credentials 12, 29
link to log on page 14
management platform and console 8
McAfee products
setting up in order 9
McAfee ServicePortal, accessing 6
merging policy lists 22
migration tasks
high-level 9
hybrid deployment 30

N
new policy
rolling out gradually 26–28
when applied 9, 25
new service
activating 12
after activating 11
Policy Browser, features 17
policy configuration areas and options 17
policy lists
  benefits of the conversion tool 22
  formatting for the new service 20
  link to conversion tool 14
  migrating 20
  using the conversion tool 23
Policy Management user interface 17
policy model, new 8
policy options, standard 20
product documentation, related 14
product name, new 7
proxy service domain name 14

reporting 8
Rule Details 17
rule order 19
rules, catch-all 19

SaaS synchronization 31

SAML authentication 25, 28
ServicePortal, finding product documentation 6
shared password
  changing 13
supported features, differences 8

technical support, finding product information 6
trusted sites lists, organizing 23

URL blacklists 19
URL lists
  formatting domain names 21
URL whitelists 19
user groups, adding to rule actions 19
user interface, new 8

Web Gateway 31
welcome page 12