Product Guide

McAfee SiteAdvisor Enterprise 3.5 Patch2

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement

Contents

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

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.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
i	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
!	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

How to use this guide

This guide provides information on configuring and using your product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introducing SiteAdvisor Enterprise

SiteAdvisor Enterprise is a browser-protection solution that monitors web searching and browsing activity on client computers to protect against threats on web pages and in file downloads.

You use McAfee® ePolicy Orchestrator (McAfee ePO) to deploy and manage SiteAdvisor Enterprise on client computers.

Client software adds features that display in the browser window on client computers to notify users about threats.

SiteAdvisor Enterprise provides features for controlling access to websites. Policy options enable administrators to control access to sites based on their safety rating, the type of content they contain, and their URL or domain name.

Contents

SiteAdvisor Enterprise features

As SiteAdvisor Enterprise runs on each managed system, it notifies users about threats when searching or browsing websites.

A McAfee team analyzes each website and assigns a color-coded site safety ratings based on test results. The color indicates the level of safety for the site.

SiteAdvisor Enterprise uses the test results to notify users about web-based threats they might encounter.

- **On search results pages**, an icon appears next to each site listed. The color of the icon indicates the safety rating for the site. Users can access more information with the icons.
- **In the browser window**, a menu button appears in the upper-right corner. The color of the button indicates the safety rating for the site. Users can access more information with the button. The menu button also:
  - Notifies users when communication problems occur and provides quick access to tests that help identify common issues.
  - Allows users to enable and disable the browser protection service. (Available only when the policy assigned to the computer makes this feature available.)
- **In safety reports**, details show how the safety rating was calculated based on types of threats detected, test results, and other data.

Using the McAfee ePO, administrators create SiteAdvisor Enterprise policies to:

- Enable and disable SiteAdvisor Enterprise, and prevent or allow users to disable the client software, on managed systems.
- Control user access to sites, pages, and downloads, based on their safety rating or type of content.

  For example, block red sites and warn users trying to access yellow sites.
- Identify sites as authorized or prohibited, based on URLs and domains.
- Prevent managed node users from uninstalling or changing SiteAdvisor Enterprise files, registry keys, registry values, services, or processes.
- Customize the notification that SiteAdvisor Enterprise displays when users attempt to access a blocked website.
- Track pages viewed on domain sites with Web Filtering for Endpoint.

  With McAfee Web Reporter, you can create detailed reports on websites.

The SiteAdvisor Enterprise client software supports Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome browsers.

- Firefox does not allow users to hide the SiteAdvisor Enterprise button with the **View | Toolbars** command or check file downloads.
- Chrome does not display safety balloons while browsing pages.

How safety ratings are compiled

A McAfee team derives safety ratings by testing a variety of criteria for each site and evaluating the results to detect common threats.

Automated tests compile safety ratings for a website by:

- Downloading files to check for viruses and potentially unwanted programs bundled with the download.
- Entering contact information into sign-up forms and checking for resulting spam or a high volume of non-spam emails sent by the site or its affiliates.
- Checking for excessive popup windows.
- Checking for attempts by the site to exploit browser vulnerabilities.
- Checking for deceptive or fraudulent practices employed by a site.

The team assimilates test results into a safety report that can also include:

- Feedback submitted by site owners, which might include descriptions of safety precautions used by the site or responses to user feedback about the site.
- Feedback submitted by site users, which might include reports of phishing scams, bad shopping experiences, and selling services that can be obtained without cost from other sources.
- Additional analysis by McAfee professionals.

Site ratings and reports are stored on a dedicated server maintained by McAfee.

Safety icons show threats while searching

When users type keywords into a popular search engine such as Google, Yahoo!, MSN, Ask, or AOL.com, color-coded safety icons appear next to sites listed in the search results page. The color of the menu button corresponds to the site's safety rating.

✓ Tests revealed no significant problems.

! Tests revealed some issues users should know about. For example, the site tried to change the testers' browser defaults, displayed pop-ups, or sent them a significant amount of non-spam email.

✗ Tests revealed some serious issues that users should consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download.

⊘ This site is blocked by a **Prohibit List**, **Rating Actions**, or **Content Actions** policy option.

? This site is unrated.

View site report while searching

Use the safety icon on a search results page to view additional information about the site.

Task

1 Place the cursor over the safety icon. A safety balloon displays a high-level summary of the safety report for the site.

2 Click the **Read site report** link (in the balloon) top open a detailed site safety report in another browser window.

SiteAdvisor Enterprise button shows threats while browsing

When users browse to a website, a color-coded SiteAdvisor Enterprise button appears in the upper-right corner of the browser. The color of the button corresponds to the site's safety rating.

ℹ If you are using the Google Chrome browser, smaller buttons appear in the address bar, for example, M.

This button...	With this color...	Indicates this...
McAfee	Green	The site is safe.
McAfee	Yellow	There might be some issues with the site.
McAfee	Red	There might be some serious issues with the site.
McAfee	Gray	No rating is available for the site.
McAfee	Orange	A communication error occurred with the SiteAdvisor Enterprise website that contains rating information.
McAfee	Blue	No information is available to rate the site. This could be an internal site or private IP range.
McAfee	Black	The site is a phishing site. ℹ Phishing is a way of attempting to acquire sensitive information such as user names, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

This button...	With this color...	Indicates this...
McAfee	White	The site is allowed by a policy setting.
McAfee	Silver	SiteAdvisor Enterprise is disabled by a policy setting.

Access SiteAdvisor Enterprise features while browsing

Access SiteAdvisor features from the button on the browser.

The button works a little differently depending on the browser you are using.

- **Internet Explorer and Firefox**:
  - Hold the cursor over this button to display a safety balloon that summarizes the safety report for the site.
  - Click the button to display the detailed safety report.
  - Click the button next to the icon to display menu options for features.
- **Chrome** — Click the button to display menu options for features.

> In Chrome browsers, you can't display safety balloons with the menu button. Safety balloons are available only from search results pages.

Task

1 From the menu, select options:

Option	To do this...	Notes
View Site Report	Display the safety report for the current site. You can also click **Read site report** link in the site safety balloon.	Available only when SiteAdvisor Enterprise is enabled.
Show Balloon	Display the safety balloon for the current site.	Available only when SiteAdvisor Enterprise is enabled and for browsers other than Chrome.
Disable/Enable SiteAdvisor	Turn off or on the SiteAdvisor Enterprise client software.	Available only when an **Enable/ Disable** policy option is configured to allow this functionality.
About	Display a brief description of SiteAdvisor Enterprise, licensing, and privacy policy.	

2 If the communication error button appears, show the balloon for the site, and click **Troubleshoot**.

The connection status page that appears indicates the possible cause of the communication error.

Troubleshoot communication problems from the browser

Run tests from the browser on the client computer to determine the reason for problems communicating with the server that provides safety ratings information.

Communication problems are indicated by an orange button in the upper-right corner of the browser.

> Communication troubleshooting is not available in Chrome browsers. To perform these tests, you must use Internet Explorer or Firefox.

Task

1. In Internet Explorer or Firefox browsers, hold the cursor over the orange button to display the safety balloon.
2. In the safety balloon, click **Troubleshooting** to run some tests and display the results.

   A connection status page displays the reason for the communication error and provides information on possible resolutions after these tests are completed.

Test	Checks for...	A failed test means...
Internet Access	Does the browser have internet access?	Your computer cannot access the Internet. This might indicate that your network connection is down or the proxy settings are configured incorrectly in the browser protection policy. Contact your administrator.
SiteAdvisor Enterprise Server Availability	Is the SiteAdvisor Enterprise server down?	The SiteAdvisor Enterprise servers are down.

3. Check the results when they are displayed and follow any instructions to resolve the problem.
4. After attempting to resolve the problem, retest the connection by clicking **Repeat Tests**.

   The **Repeat Tests** button enables you to see if the error persists or has been corrected while the page is open.

Site reports provide details

Users can view the site report for a website for details about specific threats discovered by testing.

Site reports are delivered from a dedicated McAfee SiteAdvisor Enterprise server and provide the following information:

This item	Indicates...
Overview	The overall rating for the website. We determine this rating by looking at a wide variety of information. First, we evaluate a website's email and download practices using our proprietary data collection and analysis techniques. Next, we examine the website itself to see if it engages in annoying practices such as excessive pop-ups or requests to change your home page. Then we perform an analysis of its online affiliations to see if the site associates with other suspicious sites. Finally, we combine our own review of suspicious sites with feedback from our Threat Intelligence services and alert you to sites that are deemed suspicious.
Online Affiliations	How aggressively the site tries to get you to go to other sites that we've flagged with a red rating. A common practice on the Internet is for suspicious sites to have many close associations with other suspicious sites. The primary purpose of these *feeder* sites is to get you to visit the suspicious site. A site can receive a red rating if, for example, it links too aggressively to other red sites. In effect, a site can become *red by association* due to the nature of its relationship to red-flagged domains.

This item	Indicates...
Web Spam Tests	The overall rating for a website's email practices, based on the test results. We rate sites based on both how much email we receive after entering an address on the site, and how much like spam the email looks. If either of these measures is higher than considered acceptable, we'll rate the site as yellow. If both measures are high, or one of them looks particularly egregious, we'll rate the site red.
Download Tests	Download Tests results indicate the SiteAdvisor Enterprise overall rating about the impact a site's downloadable software had on our testing computer. Red flags are given to sites that have virus-infected downloads or that add unrelated software which many people would consider adware or spyware. The rating also takes note of the network servers a program contacts during its operation, as well as any modifications to browser settings or a computer's registry files. The overall rating for the impact a site's downloadable software had on our testing computer, based on the test results. We give red ratings to sites that have virus-infected downloads or that add unrelated software that many people would consider adware or spyware. The rating also takes note of the network servers a program contacts during its operation, as well as any modifications to browser settings or computer registry files.

View site reports

View site reports to obtain more information about a site's safety rating.

Task

- Do any of the following to view the report for a site:

From this location...	Do this...
Website	• Select **View Site Report** from the SiteAdvisor menu. • Click the safety balloon. • Click the **Read site report** link in the safety balloon.
Search results page	Click the safety icon following the web page link.

ePolicy Orchestrator features that SiteAdvisor Enterprise leverages

SiteAdvisor Enterprise leverages these features in the ePolicy Orchestrator environment.

Table 1-1 McAfee ePO features that SiteAdvisor Enterprise leverages

ePolicy Orchestrator feature	SiteAdvisor Enterprise ...
Automatic Responses	Adds: • SiteAdvisor Enterprise events for which you can configure automatic responses. • SiteAdvisor Enterprise Event Groups and Event Types that you can use to create automatic responses.
Client tasks	Adds the **Send Web Reporter Logs (Web Filtering for Endpoint)** predefined client task to the **Client Task Catalog**. Use this task to transfer log files of browsing data from the client systems to the McAfee Web Reporter server.
Dashboards and monitors	Adds predefined dashboards and monitors to **Dashboards**.

Table 1-1 McAfee ePO features that SiteAdvisor Enterprise leverages *(continued)*

ePolicy Orchestrator feature	SiteAdvisor Enterprise ...
Permission sets	Adds the SiteAdvisor Enterprise, SiteAdvisor Enterprise Events, and Web Filtering for Endpoint permission group to each permission set.
Policies	Adds predefined policies to the **Policy Catalog**.
Queries and reports	Adds: • Predefined queries to the **Query** list in **Queries and Reports**. SiteAdvisor Enterprise query names are prepended with the SiteAdvisor Enterprise name or abbreviation to facilitate filtering. • Predefined Feature Groups, Result Types, and Properties to use when creating custom queries.
Server tasks	Adds the **Purge SiteAdvisor Enterprise Events** action to the Server Task Builder to periodically remove SiteAdvisor Enterprise events from the McAfee ePO database.
Threat Event Log	Adds SiteAdvisor Enterprise properties that you can filter and view in the Threat Event Log.

Using permission sets with SiteAdvisor Enterprise

A *permission set* specifies all the permissions that apply to a single object and controls the level of access users have to features.

SiteAdvisor Enterprise adds these permission groups to each permission set:

- SiteAdvisor Enterprise
- SiteAdvisor Enterprise Events
- Web Filtering for Endpoint

These define the access rights to the SiteAdvisor Enterprise features. ePolicy Orchestrator grants all permissions for all products and features to global administrators, who in turn assign user roles to existing permission sets or create new permission sets.

Table 1-2 Permissions required per feature

Feature	Required permissions
Automatic Responses	Automatic Responses, Event Notifications, Client Events
Client events and client rules	Systems, System Tree access, Threat Event Log
Dashboards and monitors	Dashboards, Queries
Policies	SiteAdvisor Enterprise Policy and Tasks SiteAdvisor Enterprise Events
Queries	Queries and Reports
Server tasks	Server Tasks
System Tree	Systems, System Tree access
Threat Event Log	Systems, System Tree access, Threat Event Log

For information on managing permission sets, see the ePolicy Orchestrator documentation.

Frequently asked questions

These questions address many typical issues that arise when deploying SiteAdvisor Enterprise to managed network systems.

Policy enforcement

How can users circumvent SiteAdvisor Enterprise policy settings and hide their browsing behavior?

Users can use several methods to hide browsing activity, including:

- Creating an application that browses the web or creating a frame page where the content of a frame loads websites.
- Disabling the SiteAdvisor Enterprise client software by using the **Add-ons** feature through the browser's **Tools** menu. However, this action can be performed only on a Google Chrome browser.

To protect against these situations:

- Check browsing behavior and browser usage regularly by using various queries that track browsing behavior. This lets you know when particular managed systems show no browsing data or less browsing data than expected.
- Check the functional status of the client software by using the **Functional Compliance** query. This lets you know when the software is disabled.

By setting up monitors that use the applicable queries, or frequently checking reports generated by these queries, you know when users are circumventing policy settings and can take immediate steps to ensure compliance. See *Monitoring browser protection and security* for more information.

Information tracking and reporting

If Microsoft Internet Explorer is the only browser installed on a managed system when SiteAdvisor Enterprise is deployed, does SiteAdvisor Enterprise need to be redeployed after installing Mozilla Firefox or Google Chrome?

No. The SiteAdvisor Enterprise client software detects Firefox when it is installed and immediately begins to protect searching and browsing activities in that browser, while continuing to provide protection for Internet Explorer.

Color coding

Why is the SiteAdvisor button gray?

Several causes are possible:

- The site is not rated.
- The SiteAdvisor Enterprise client software is disabled. If the administrator has not disabled it at the policy level (by configuring a Disable/Enable policy option), click the arrow on the menu button to display the **SiteAdvisor** menu, then select **Enable SiteAdvisor**. (If SiteAdvisor Enterprise is already enabled, the menu option changes to **Disable SiteAdvisor**. Neither menu option is available if the administrator has disabled them at the policy level.)
- The site is on the Authorize list and the **Track events** option is disabled (in the Authorize List policy). When authorized sites are not being tracked, the SiteAdvisor server does not receive data about the sites; therefore, it cannot display a color-coded rating for the sites.

Versions of SiteAdvisor software

What are the differences between the consumer version of SiteAdvisor and SiteAdvisor Enterprise?

SiteAdvisor Enterprise has been modified for management by an administrator with ePolicy Orchestrator. In addition, the automatic update feature has been removed to ensure that administrators control the version of the software running on managed systems.

General

Is it safe to use SiteAdvisor Enterprise as my only source of security against web-based threats?

No. SiteAdvisor Enterprise tests a variety of threats, and constantly adds new threats to its testing criteria, but it cannot test for all threats. Users should continue to employ traditional security defenses, such as virus and spyware protection, intrusion prevention, and network access control, for a multi-tiered defense.

Where to find more information

Several sources of additional information and support are available for using SiteAdvisor Enterprise under ePolicy Orchestrator.

ePolicy Orchestrator documentation

For detailed information on installing and managing applications under ePolicy Orchestrator, visit the McAfee ServicePortal website: https://mysupport.mcafee.com/Eservice/Default.aspx.

To view a complete listing of the ePolicy Orchestrator documentation available for download:

1. Under **Useful Links**, click **Product Documentation**.
2. Click **ePolicy Orchestrator** , then **ePolicy Orchestrator 4.5** or **ePolicy Orchestrator 4.6**.

SiteAdvisor Enterprise website

For the latest information about SiteAdvisor Enterprise and relevant white papers, visit: http://www.mcafee.com/us/products/siteadvisor-enterprise.aspx.

Online SiteAdvisor Enterprise forums

For the most current information on SiteAdvisor Enterprise issues and web threats, visit these McAfee online forums:

- https://community.mcafee.com/community/business/system/siteadvisor_enterprise
- http://www.mcafee.com/us/products/siteadvisor-enterprise.aspx

Threat Intelligence website

Visit the http://www.mcafee.com/threat-intelligence/site/default.aspx website which shows information on the URL's web reputation, affiliations, DNS servers and associations.

2 Setting up a browsing security strategy

SiteAdvisor Enterprise includes a default policy with settings recommended by McAfee to protect managed systems from most web-based threats. Customize these policy settings to address your business needs.

Contents

Guidelines for creating a strategy

Follow these guidelines to design and implement a browsing security strategy that fully protects your managed systems against web-based threats.

1 **Install SiteAdvisor Enterprise, enable Observe mode, and deploy the client software.**

Before deploying the client software, enable Observe mode (Action Enforcement tab on the General policy page). This prevents SiteAdvisor Enterprise from taking actions (such as blocking and warning) configured as part of the default policy, but tracks browsing behavior data that you can retrieve in reports.

See *Evaluate policy settings with Observe mode* and *Specify enforcement behavior for specific actions*.

2 **Evaluate browsing traffic and usage patterns (Reports).**

Run queries and review the results to learn about network browsing patterns. For example, what types of sites are users visiting and what tasks are they performing at these sites? What time of day is browsing traffic heaviest?

See *Monitoring browser protection and security*.

3 **Create policies.**

Configure policy options based on the browsing behavior revealed in the query results. Prohibit, block, or warn about sites or downloads that present threats, and authorize sites that are important to your users.

See *Configuring policies*.

4 **Test and evaluate policy settings (Observe mode).**

Enable Observe mode to track the number of users who access sites that would be affected by the policy settings you have configured. Run queries, then view and evaluate the tracked data. Are the settings comprehensive enough? Do they have any unintended consequences you need to resolve? Adjust the policy settings as needed, then disable Observe mode to activate them.

See *Evaluate policy settings with Observe mode*.

5 **Ensure compliance, productivity, and security with frequent monitoring.**

Run queries regularly. View results in reports or in monitors.

- Ensure that the SiteAdvisor Enterprise client software is enabled on all computers and can function properly (by using the Functional Compliance query).
- Check whether any sites or site resources, such as download files, that are required for business are blocked.
- Check visits to sites that contain threats.
- Update policy settings to address any problems.
- Run a purge task occasionally to clear out the reports database.

See *Monitoring browser protection and security* and *Configuring policies*.

Selecting the right policy options and features

Identify your browser security goals and deploy SiteAdvisor Enterprise features.

When developing a browsing security strategy:

- Assess the security concerns and vulnerabilities that apply to your business.
- Carefully consider any domains and sites that must be accessible to your managed systems and any that you want to block.
- Decide which network browsing activities you need to monitor.
- Determine your most effective and efficient forms of monitoring.

Use this list to identify which product features can help meet your goals.

If your security or productivity goal is...	Use this feature...
Use SiteAdvisor Enterprise ratings to control access to sites, download files, or phishing pages.	Rating Actions policy category
Block particular sites or domains.	Prohibit List policy settings
Ensure access to particular sites. Control access to resources on these sites (such as download files). Track visits to these sites and access of site resources.	Authorize List policy settings
Prevent data about intranet sites from being reported to the SiteAdvisor Enterprise website's servers.	Event Tracking policy settings
Communicate to users why a site is blocked or how to protect against threats on a site.	Enforcement Messaging policy settings
Control who can disable or enable the SiteAdvisor Enterprise client software.	Disable/Enable policy settings
Evaluate the effect of policy settings before they are implemented.	Observe mode (part of General policy settings)

If your security or productivity goal is...	Use this feature...
Enter information on any proxy server needed for Internet access.	Proxy Server (part of General policy settings)
Obtain information for and track activity on private domain servers.	Event Tracking policy settings
Obtain information for and track visits to non-private domain servers.	Event Tracking policy settings
Obtain information for and track each page accessed from domain servers.	Event Tracking policy settings
Monitor the effect of current policy settings.	Dashboards, monitors, and queries
Ensure that the correct version of the SiteAdvisor Enterprise client software is installed on all managed systems and functions properly.	Functional Compliance query
Use site content to control access to sites.	Content Actions policy settings with Web Filtering for Endpoint extension
Obtain detailed reports based on site content.	McAfee Web Reporter with Web Filtering for Endpoint extension

See *Configuring SiteAdvisor Enterprise policies* for information about using the policy features. See *Monitoring browser protection and security* for information about dashboards, monitors, and queries.

Using safety ratings to control access

Configure the **Rating Actions** policy to use SiteAdvisor ratings to determine whether users can access a site, or resources on a site.

To block file downloads and phishing pages on sites included in an Authorize list, modify the settings on the **Advanced Options** tab of the **Authorize List** policy. See *Work with Authorize lists*.

- For each site, specify whether to allow, warn, or block the site, based on the rating.
- For each file download, specify whether to allow, warn, or block the file download, based on the rating.

  This enables a greater level of granularity in protecting users against individual files that might pose a threat on sites with an overall green rating.
- For each phishing page, specify whether to block or allow access.

  This enables a greater level of granularity in protecting users from pages that employ phishing techniques on a site with an overall green rating.

ℹ To ensure users can access specific sites that are important to your business, no matter how they are rated, add them to an Authorize list. Users can access sites that appear on an Authorize list even if you have configured other actions with their ratings.

Using content categories to control access

The Web Filtering for Endpoint module enables SiteAdvisor Enterprise to categorize the type of content that appears on a site. You can use policy options to allow, warn, or block access to sites based on the category of content they contain.

When you apply a **Content Actions** policy to client systems, SiteAdvisor Enterprise returns content classification ratings for a site. SiteAdvisor Enterprise applies **Content Actions** policy settings to block, warn, or allow the site based on content type on client systems. The approximately 100 site content categories are grouped by function and risk, which allows for easy application of the policy settings based on content alone or on content functional groups or risk groups.

The web filtering module uses more than 100 pre-defined content categories that are stored on the SiteAdvisor Enterprise server maintained by McAfee. These categories are listed on the Manage Category Actions tab of the Content Actions policy page.

For each category of content, the Manage Category Actions tab displays:

- Type of content (for example, shopping or gambling).
- Function it enables users to perform (for example, purchasing or entertainment).
- Risks it might present to your business (for example, a risk to security or productivity).

This allows you to configure policy settings based on content alone, or the functions that users can perform by accessing the content, or the risks that the content might present to your business.

- You can block, warn, or allow all sites that contain specific types of content.
- You can block, warn, or allow all sites that enable specific types of functions or present specific types of risks or functions.

Risk Groups

Each category is placed in a **Risk Group** that identifies the primary risk from accessing this content. Risk groups can help identify changes that need to be made with web-filtering policies and can be used in reporting. The Manage Category Actions tab lists these risk groups.

- **Bandwidth** — Web pages that feature content that consumes a large amount of bandwidth (such as streaming media or large files), which might affect the business-related flow of data on the network.
- **Communications** — Web pages that allow direct communication with others through the web browser.
- **Information** — Web pages that allow users to find information that might not be pertinent to their business or education.
- **Liability** — Allowing users to view web pages in this category might be criminal or lead to lawsuits by other employees.
- **Productivity** — Non-business sites that users visit for entertainment, social, or religious reasons.
- **Propriety** — Sites in this category are for mature users only.
- **Security** — Web pages that are a source of malware, which can damage computer software, get around network policies, or leak sensitive data.

Examples

You can use the filters at the top of the Manage Category Actions tab to assist you in locating all the content categories for which you might want to configure actions. Then select whether to **Allow**, **Warn**, or **Block** each category that meets your criteria.

- Select a **Functional Group** of **Risk/Fraud/Crime** and a **Risk Group** of **Security** to display all the categories of content that might pose a threat to user security due to fraud or criminal intent.

  > All sites containing content with a **Risk Group** of **Security** are blocked by default. This includes phishing pages, malicious downloads, malware, and spam.

- Select a **Functional Group** of **All** and a **Risk Group** of **Productivity** to display all the categories of content that might impact users' productivity adversely, such as online shopping or gaming.

- Select a **Functional Group** of **Lifestyle** and a **Risk Group** of **Propriety** to configure settings for social networking and dating sites.
- Select a **Functional Group** of **Information/Communication** and a **Risk Group** of **All** to display categories of content used for collaborating and exchanging information. Because some sites are geared for professional use and some for personal use, you can allow or block each content category individually. This provides the flexibility to enforce a company's or department's security standards for content such as **Instant Messaging**, **Forum/Bulletin Boards**, or **Blogs/Wiki** content, which have important business uses in some companies and not others.

Using URLs or domains to control access

SiteAdvisor Enterprise enables you to set up lists of URLs for sites that users can or cannot access.

- **Authorize lists** contain URLs or *site patterns* that users are always allowed to access, regardless of their safety rating or type of content. Use Authorize lists to ensure that managed systems can access sites that are important to your business. The button in the upper-right corner of the browser appears white for authorized sites.

  > By authorizing a site, SiteAdvisor Enterprise ignores the safety rating for that site. Users can access authorized sites even if threats have been reported on these sites and they have a safety rating of red. It is important to exercise caution when adding sites to Authorize lists.

  You can also specify actions for resources within authorized sites, such as file downloads and phishing pages. For example, if you evaluate a yellow site and determine that your users are not vulnerable to potential threats on the site, you can add the site to an Authorize list. If the site contains a phishing page or a red download file, you can authorize access to the site but block access to the phishing page and download file. This ensures that sites important to your business are accessible, but that your users are protected from potential threats on those sites.

- **Prohibit lists** contain URLs or *site patterns* that are blocked on all computers using the policy. Use Prohibit lists to block access to sites that are not related to job performance or do not conform to company security standards. The button in the upper-right corner of the browser appears black for prohibited sites.

The Authorize List and Prohibit List policy categories are *multiple-instance* policies. See *How multiple-instance policies work* for more information.

By default, if the same site appears on an Authorize list and a Prohibit list, the Prohibit list takes precedence and the site is blocked. You can configure a policy option to give an Authorize list priority instead.

> The Authorize List or Prohibit List policy settings override those in the Content Actions policy if this policy is available.

How site patterns work

Authorize lists and Prohibit lists use *site patterns* to specify a range of sites that are authorized or prohibited. This enables you to authorize or prohibit a particular domains or a range of similar sites without entering each URL separately.

When a managed system attempts to navigate to a site, SiteAdvisor Enterprise checks whether the URL matches any site patterns configured in an Authorize List or Prohibit List policy. It uses specific criteria to determine a match.

A site pattern consists of a URL or partial URL, which SiteAdvisor Enterprise interprets as two distinct components: *domain* with protocol information (for example, http://, https://, or ftp://) and *path*.

Site pattern: www.mcafee.com/us/enterprise	
http:// www.mcafee.com	This is the **domain**. The domain consists of two parts: • **Protocol.** In this case: **http://** • **Internet domain.** In this case: **www.mcafee.com** Domain information is matched from the *end*. A matching URL's domain must *end* with the site pattern's domain. The protocol can vary. These domains match: • http:// ftp.mcafee.com • https://mcafee.com • http://www.info.mcafee.com These domains do not match: • http:// www.mcafee.downloads.com • http://mcafee.net • http://www.mcafeeasap.com • http://us.mcafee.com
/us/enterprise	This is the **path**. The path includes everything that follows the / after the domain. Path information is matched from the *beginning*. A matching URL's path must *begin* with the site pattern's path. These paths match: • /us/enterpriseproducts • /us/enterprise/products/security These paths do not match: • /emea/enterprise • /info/us/enterprise

Site patterns must be at last three characters in length, and they do not accept wildcard characters. SiteAdvisor Enterprise does not check for matches in the middle or end of URLs.

Use the "." character at the beginning of a site pattern to match a specific domain. For convenience, the "." character disregards the protocol and introductory characters.

Example: **.mcafee.com**

Matches	Does not match
• http://www.info.mcafee.com • http://mcafee.com • http://ftp.mcafee.com	• http://www.mcafeeasap.com • http://salesmcafee.com • http://ftp.mcafee.net

See also

Work with Authorize lists on page 31

Configure additional enforcement rules on page 33

Work with Prohibit lists on page 34
Block or warn site access based on safety rating on page 36

How multiple-instance policies work

Authorize List and Prohibit List policies are called *multiple-instance policies* because you can assign multiple instances of an Authorize list or a Prohibit list under a single policy. The policy instances are automatically combined into one *effective policy*.

Content actions policy also supports *multiple-instance* similar to Authorize list or a Prohibit list.

Multiple-instance policies obey the ePolicy Orchestrator laws of inheritance within a System Tree (see *Organizing Systems for Management* and *Managing Products with Policies and Client Tasks* in the *ePolicy Orchestrator Product Guide*).

As an example, say that you configure one Authorize List policy for Group A, another for Group B, and another for Group C. If Group A contains Group B, and Group B contains Group C, then Group C's Authorize List policy would be an effective policy incorporating elements from all three Authorize List policies. The Authorize list for Group C might contain all the sites listed for Group A and Group B, and additional sites specific to Group C. By using an effective policy, there is no need to re-enter all the sites from Group A and Group B into the Authorize list for Group C.

See also

Work with Authorize lists on page 31

Work with Prohibit lists on page 34
Block or warn site access based on safety rating on page 36

Information that SiteAdvisor Enterprise sends to the McAfee ePO server

The client software sends information to the McAfee ePO server, which can be used in queries.

The client software sends the following information to the McAfee ePO server for use in queries:

- Type of event initiated by the managed system (site visit or download).
- Unique ID assigned by SiteAdvisor Enterprise to the managed system.
- Time of event.
- Domain for event.
- URL for event.
- SiteAdvisor rating for the event's site.
- Site threat factor.
- Whether the event's site or site resource is on an Authorize list, a Prohibit list, or no list.
- Reason for action (allow, warn, or block) taken by SiteAdvisor Enterprise.
- Observe mode status (on or off).

SiteAdvisor Enterprise sends the complete URL of the website to the SiteAdvisor Enterprise website's servers.

The SiteAdvisor Enterprise sends the following information to the SiteAdvisor server maintained by McAfee:

- Version of the browser protection client software running on the client computer.
- Version of the operating system running on the client computer.
- Language and country locale selected for the operating system and browser running on the client computer.
- Host name and part of the URL for each website the client computer requests to access.
- MD5 algorithm for each application the client computer requests to download.

When a managed system visits a website, SiteAdvisor Enterprise tracks the URL. The URL is the smallest amount of information required for SiteAdvisor Enterprise to uniquely identify the URL being rated for security. The focus of SiteAdvisor Enterprise is protecting your managed systems; no attempt is made to track personal Internet usage.

> SiteAdvisor Enterprise does not send information on your company's intranet sites to the SiteAdvisor Enterprise website's servers, unless specifically requested. See *Tracking events for reports* for more information.

3 Configuring SiteAdvisor Enterprise policies

A policy is a collection of software settings that you configure and enforce on managed client systems. Policies ensure that security software products are configured and function as your organization requires.

For the purposes of this guide, we assume that you have installed ePolicy Orchestrator and have the necessary privileges to perform the steps described in this guide. For more information about ePolicy Orchestrator, refer to the product's documentation.

Contents

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator

Policies are collections of settings that you create, configure, apply, and then enforce.

Policies enable you to configure managed products and apply the configuration to systems in your network, all from a central location.

SiteAdvisor Enterprise adds the following categories to the Policy Catalog:

Table 3-1 SiteAdvisor Enterprise categories

Category	Description
Authorize List (Multiple-instance)	Specifies: • Lists of sites that users are authorized to access. • Access to individual resources, such as file downloads, on the sites. • Whether the Authorize list has precedence over Prohibit lists. Several instances of this policy can be applied, resulting in one combined, effective policy.
Enable/Disable	Configures whether the SiteAdvisor Enterprise client software is disabled or enabled for all managed systems assigned this policy, and whether it can be disabled on individual systems. Enables you to: • Disable and enable the SiteAdvisor Enterprise client software for all McAfee ePO managed systems using this policy. • Allow SiteAdvisor Enterprise client software to be disabled and enabled from the browser on managed systems, and whether a password is required.
Enforcement Messaging	Specifies messages, which can include your own logo or image, to display to users who attempt to access: • Blocked sites • Warned sites • Authorized sites • Prohibited sites • Phishing pages • File downloads
Event Tracking	Configures settings to track domain visits and downloads. If the McAfee Web Filtering for Endpoint extension and McAfee Web Reporter are installed, you can also track page views and downloads within a domain and send information to McAfee Web Reporter for reports.
General	Configures: • Proxy settings for managed systems running the client software to access the Internet. • Observe mode to evaluate and tune policy settings before implementing them. • Whether users can remove SiteAdvisor Enterprise using Add or Remove Programs.
Hardening	Configures settings to: • Prevent managed node users from uninstalling SiteAdvisor Enterprise or disabling the SiteAdvisor Enterprise browser plugin. • Prevent any unwanted changes to SiteAdvisor Enterprise files, registry keys, and registry values. • Prohibit specific supported and unsupported browsers.

Table 3-1 SiteAdvisor Enterprise categories *(continued)*

Category	Description
Prohibit List (Multiple-instance)	Specifies sites that users are blocked from accessing. Several instances of this policy can be applied resulting in one combined, effective policy.
Rating Actions / Content Actions	Configures rules for user access based on the safety ratings and threat factors that SiteAdvisor Enterprise assigns to sites, pages on a site, or file downloads. If McAfee Web Filtering for Endpoint is installed, **Content Actions** replaces **Rating Actions**. See *Using McAfee Web Filtering for Endpoint and McAfee Web Reporter* for details.

In each category, SiteAdvisor Enterprise provides predefined policies:

Table 3-2 SiteAdvisor Enterprise predefined policies

Policy	Description
McAfee Default	Defines the default policy that takes effect if no other policy is applied. You can duplicate, but not delete or modify, this policy.

For information on creating and using policies and the Policy Catalog, see the ePolicy Orchestrator documentation.

Comparing policies

You can compare all SiteAdvisor Enterprise policy settings using ePolicy Orchestrator Policy Comparison. See the ePolicy Orchestrator documentation for information.

How policies work

When SiteAdvisor Enterprise is installed, its preconfigured default policy is installed in the repository. You cannot change this default policy, but you can create a duplicate of this policy with a different name and configure it to achieve the right level of browsing protection for your users. .

You then assign the policy to managed systems running the SiteAdvisor Enterprise client software. You can assign the same policy settings to all managed systems, or to groups of managed systems that perform similar tasks and require the same type of access and protection.

User-specific policies

In general, a policy is applied to a group, and all systems in the group receive the same policy settings. However, you can create user-specific instead of system-specific policy assignments with policy assignment rules. These assignment rules are enforced on the client system for a particular user when that user logs on, regardless of the McAfee ePO group in which the system is placed. For more information, see *How policy assignment rules work* in the ePolicy Orchestrator documentation.

> Policy assignment rules are enforced only if the user logs on as the interactive user. If a user logs on with a `runas` command, or logs on to a remote desktop or terminal service where the user's logon is not set to interactive, the policy assigned to the system and not the one assigned to the user is enforced.

Multiple instance policies

Both the Authorize List and Prohibit List policies are multiple-instance policies. These policies allow for a profile of settings through the application of multiple policies under a single policy instance. This can be helpful if you want to apply a default list of sites, and add entries for a particular group or all groups. Instead of updating the entire list with the new entries, you can create a second policy instance for the new entries and apply it and the default list together. The effective policy is then the combination of the two policy instances.

For recommendations on selecting and implementing SiteAdvisor Enterprise policy settings, see *Setting up a browsing security strategy*.

For more information about using policies with ePolicy Orchestrator, see the ePolicy Orchestrator documentation.

Evaluate policy settings with Observe mode

Observe mode enables you to evaluate the effect that policy settings for warning or blocking access have on network browsing activity before you implement them.

To enable Observe mode, see *Specify enforcement behavior for specific actions*.

Use Observe mode to track:

- Visits to red, yellow, or unrated sites.
- Visits to sites you have configured to block or warn.
- Visits to phishing pages you have configured to block.
- Downloads you have configured to block or warn.

Information compiled in Observe mode is available by running queries, then viewing the results in reports or monitors. (See *Monitoring browser protection and security* for more information.) If you determine that network browsing patterns are adversely affected by any current settings, adjust them before disabling Observe mode. Policy settings are enforced when Observe mode is disabled.

Enable and disable SiteAdvisor Enterprise

Use settings in the **Enable/Disable** category to enable and disable SiteAdvisor Enterprise on all systems managed by the McAfee ePO server or allow users to disable SiteAdvisor Enterprise from the browser.

When the software is disabled, policy settings are not enforced, the site report cannot be displayed, the SiteAdvisor menu button is gray, and its menu option **Enable/Disable SiteAdvisor** does not appear.

> In general, McAfee does not recommend disabling SiteAdvisor Enterprise. However, you might find this feature useful when performing tests or troubleshooting network connection problems. Be sure to enable the software as soon as it is practical to do so.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Enable/Disable**.
3. Select one of these actions.

Action	Steps
Enable and disable SiteAdvisor Enterprise on all systems managed by the McAfee ePO server. The default setting is enabled.	From **SiteAdvisor policy enforcement**, select **Disable** or **Enable**.
Allow users to enable and disable SiteAdvisor Enterprise from the SiteAdvisor Enterprise menu in the browser. The default setting is to block disabling. Users can circumvent policy settings by using their browser's Add-ons feature (accessed on the **Tools** menu) to disable SiteAdvisor Enterprise. Detect this behavior by running the **Functional Compliance** query, which reports the functional status of the client software on managed systems.	1 From **SiteAdvisor menu option**, select **Enable**. 2 Select **Only allow with password** if a password is required. If you select this option, type and confirm the password.
Hide the SiteAdvisor Enterprise toolbar on the browser without disabling its functionality. This resolves third party compatibility issues. The SiteAdvisor Enterprise toolbar will be hidden on the new browser tab or window after the policy has been enforced on the system.	From **SiteAdvisor toolbar**, deselect **Enable**.

4. Click **Save**.
5. Run an agent wake-up call to apply the setting immediately, or wait for the next automatic agent-server communication.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

Protect SiteAdvisor Enterprise resources

Use settings in the Self Protection tab in the Hardening category to prevent users from uninstalling or changing SiteAdvisor Enterprise resources.

SiteAdvisor Enterprise integrates with VirusScan Enterprise to protect itself from being uninstalled or modified. Before configuring these settings, ensure that Access Protection in VirusScan Enterprise is enabled on all managed nodes. For details on enabling Access Protection, refer to *VirusScan Enterprise Product Guide*.

> Enabling hardening on managed nodes blocks the use of InPrivate browsing in Internet Explorer or Private Browsing in Mozilla Firefox. Hardening also blocks the use of the `-extoff` switch in Internet Explorer.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Hardening**.
3. Select one of these actions.

Action	Steps
Protect SiteAdvisor Enterprise resources.	From **Protect Site Advisor Resources**, select: • **Files** — Prevents managed node users from modifying the SiteAdvisor Enterprise databases, binaries, safe search files, and configuration files. • **Registry** — Prevents managed node users from modifying the SiteAdvisor Enterprise registry hive, COM components, and uninstalling using the registry value. • **Service** — Prevents managed node users from killing, renaming, and stopping or starting SiteAdvisor Enterprise services. • **Uninstall** — Prevents managed node users from uninstalling SiteAdvisor Enterprise using Add/Remove Programs in Control Panel or command prompt.
Protect SiteAdvisor Enterprise browser plug-in. Enabling this policy option re-enables the SiteAdvisor Enterprise plug-in immediately after it is disabled using the Manage add-ons option in the browser.	From **Protect SiteAdvisor browser plugin**, select **Enable**.

4 Click **Save**.

Display SiteAdvisor Enterprise in Add or Remove Programs

Use settings in the Control Panel Option tab in the General category to display SiteAdvisor Enterprise in the Add or Remove Programs control panel on client systems.

If you allow it to appear, users can remove SiteAdvisor Enterprise. You might find this option useful in troubleshooting; however, McAfee does not recommend enabling this option.

Task

For option definitions, click **?** in the interface.

1 From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **General**.

3 Click the **Control Panel Option** tab.

4 Select **Enable**.

5 Click **Save**.

See also
Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

Prohibit use of specific browsers

Use settings in the Browser Control tab in the Hardening category to prohibit the use supported or unsupported browsers on managed nodes.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Hardening**.
3. Click the **Browser Control** tab.
4. Select the browsers to block from being launched on the managed nodes.
5. Click **Save**.

Manage authorized and prohibited sites

Create Authorize and Prohibit lists to specify websites that are always allowed or blocked based on the URL or domain.

Tasks

- *Work with Authorize lists* on page 31
  An Authorize list contains a list of URLs or site patterns that are allowed on all computers using the policy. An Authorize list ensures that users can access sites you consider to be important for your business. Use **Authorize List** policy options to create and manage the contents of an Authorize list.
- *Work with Prohibit lists* on page 34
  A Prohibit list contains a list of URLs or site patterns that are blocked on all computers using the policy. A Prohibit list prevents managed systems from accessing sites considered to be inappropriate or non-compliant with company policy. Use **Prohibit List** policy options to create and manage the contents of a Prohibit list.

Work with Authorize lists

An Authorize list contains a list of URLs or site patterns that are allowed on all computers using the policy. An Authorize list ensures that users can access sites you consider to be important for your business. Use **Authorize List** policy options to create and manage the contents of an Authorize list.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Authorize List**.
3. Select one of these actions.

Action	Steps
Add a site to an Authorize list.	1 Click **Add**, then type a URL or partial URL (called a *site pattern*) that is at least three characters in length. 2 Type a comment or note to associate with the site (optional). 3 Click **OK**.
Add multiple sites to an Authorize list.	1 Click **Add Multiple**, then type a URL or partial URL (called a *site pattern*), then type a space or tab followed by a comment. URLs or site patterns must be at least three characters in length. ℹ The comment is optional. Spaces are allowed within a comment, but the first space on a line separates the site pattern from the comment. 2 On a new line, repeat the last step for each site you want to add to the Authorize list. 3 Click **OK**.
Delete sites from an Authorize list.	Select the checkbox next to a site, then click **Delete**.
Change information (URL, site pattern, or comment) in an Authorize list.	1 Select the checkbox next to a site, then click **Edit**. 2 Modify the site patterns or comments as needed. ℹ Comments are optional. Spaces are allowed within a comment, but the first space on a line separates the site pattern from the comment. Each site pattern must appear at the beginning of a new line. 3 Click **OK**.
Search an Authorize list. This feature is useful for finding sites in large lists.	Type a URL, site pattern, or text in the **Search** box, then click **Go**. SiteAdvisor Enterprise searches all site patterns and comments in the list and displays those that match. To clear the search criteria and again display the contents of the list, click **Clear**.

4 Test whether specific sites or site patterns are included in an Authorize list.

For example, when an Authorize list is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy. See *How multiple-instance policies work*.

a Click the **Test Site Patterns** tab.

b Type a URL or partial URL in the **Match URL** field.

c Click **Go**.

SiteAdvisor Enterprise displays any site patterns that match your entry. If no site patterns are displayed, the Authorize list allows access to the specified URL.

To clear the test criteria and results, click **Clear**.

5 Click **Save**.

Tasks

- *Configure additional enforcement rules* on page 33
  Use settings in the Advanced Options tab in the Authorize List category to configure additional enforcement rules.

See also

How site patterns work on page 21

How multiple-instance policies work on page 23

Configure additional enforcement rules

Use settings in the Advanced Options tab in the Authorize List category to configure additional enforcement rules.

> ℹ Use the **Enforcement Messaging** policy options to customize the message that is displayed to users for blocked and warned downloads. See *Customize user notifications for blocked content* .

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Authorize List**.
3. Select one of these actions.

Action	Description	Steps
Turn off tracking for visits to authorized sites.	When you turn off the tracking, events for sites and site resources are no longer collected, and site information from the SiteAdvisor server is not requested. Phishing page blocking and download rating actions are also disabled only when this option is disabled. McAfee recommends using this procedure to prevent private information about intranet sites from being sent to the SiteAdvisor website's servers. It also reduces the amount of data returned by certain reports because visits to authorized sites are not reported. ℹ The SiteAdvisor menu button appears gray when visiting sites that are not being tracked. This setting takes precedence over the one in the **Event Tracking** policy.	Deselect **Track events and request information from the SiteAdvisor server.** This effectively also disables phishing page blocking and download rating actions for sites on the list.
Block phishing pages on authorized sites.		1 Select **Track events and request information from the SiteAdvisor server.** 2 Select **Block phishing pages.**

Action	**Description**	**Steps**
Block or warn file downloads on authorized sites.	An authorized site with an overall rating of green can contain individual download files rated yellow or red. To protect users, specify an action that is specific to the rating for an individual file.	1 Select **Track events and request information from the SiteAdvisor server**. 2 Select an action (**Block**, **Warn**, or **Allow**) for **Red**, **Yellow**, and **Unrated** files.
Set list precedence.	By default, the Prohibit list has precedence over the Authorize list, which means that sites appearing on both are blocked. Select this option to ensure that users can access any site on the Authorize list, even if it also appears on a Prohibit list. Use caution when selecting this option. Check to ensure that sites on the Authorize list are safe so that managed systems remain protected from web-based threats.	1 Select **Track events and request information from the SiteAdvisor server**. 2 Select **Give this Authorize list precedence over Prohibit lists**.

4 Click **Save**.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25
How site patterns work on page 21

Work with Prohibit lists

A Prohibit list contains a list of URLs or site patterns that are blocked on all computers using the policy. A Prohibit list prevents managed systems from accessing sites considered to be inappropriate or non-compliant with company policy. Use **Prohibit List** policy options to create and manage the contents of a Prohibit list.

Task

For option definitions, click **?** in the interface.

1 From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Prohibit List**.

3 Select one of these actions.

Action	Steps
Add a site to a Prohibit list.	1 Click **Add**, then type a URL or partial URL (called a *site pattern*) that is at least three characters in length. 2 Type a comment or note to associate with the site (optional). 3 Click **OK**.
Add multiple sites to a Prohibit list.	1 Click **Add Multiple**, then type a URL or partial URL (called a *site pattern*), then type a space or tab followed by a comment. URLs or site patterns must be at least three characters in length. The comment is optional. Spaces are allowed within a comment, but the first space on a line separates the site pattern from the comment. 2 On a new line, repeat the last step for each site you want to add to the Prohibit list. 3 Click **OK**.
Delete sites from a Prohibit list.	Select the checkbox next to a site, then click **Delete**.
Change information (URL, site pattern, or comment) in a Prohibit list.	1 Select the checkbox next to a site, then click **Edit**. 2 Modify the site patterns or comments as needed. Comments are optional. Spaces are allowed within a comment, but the first space on a line separates the site pattern from the comment. Each site pattern must appear at the beginning of a new line. 3 Click **OK**.
Search a Prohibit list. This feature is useful for finding sites in large lists.	Type a URL, site pattern, or text in the **Search** box, then click **Go**. SiteAdvisor Enterprise searches all site patterns and comments in the list and displays those that match. To clear the search criteria and again display the contents of the list, click **Clear**.

4 Test whether specific sites or site patterns are included in a Prohibit list.

For example, when a Prohibit list is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy. See *How multiple-instance policies work*.

a Click the **Test Site Patterns** tab.

b Type a URL or partial URL in the **Match URL** field.

c Click **Go**.

SiteAdvisor Enterprise displays any site patterns that match your entry. If no site patterns are displayed, the Prohibit list allows access to the specified URL.

To clear the test criteria and results, click **Clear**.

5 Click **Save**.

See also

How site patterns work on page 21

How multiple-instance policies work on page 23

Block or warn site access based on safety rating

Configure settings in the Rating Actions category to block or warn sites, phishing pages, and file downloads based on safety ratings.

> Use the Enforcement Messaging policy options to customize the message that displays to users for blocked and warned sites, blocked phishing pages, and blocked and warned file downloads.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Rating Actions**.
3. Select one of these actions.

Action	Description	Steps
Block or warn sites based on overall ratings.	Block users from accessing sites that contain threats, or warn users about potential threats on sites.	1 Click the **Site** tab. 2 Select an action (**Block**, **Warn**, or **Allow**) for **Red**, **Yellow**, and **Unrated** sites.
Block phishing pages.	A site with an overall rating of green can contain phishing pages. To protect users, block access to these pages.	1 Click the **Site Resources** tab. 2 From **Page-level rating actions**, select **Block phishing pages**.
Block or warn file downloads based on ratings.	A site with an overall rating of green can contain individual download files rated yellow or red. To protect users, specify an action that is specific to the rating for an individual file.	1 Click the **Site Resources** tab. 2 From **File download rating actions**, select an action (**Block**, **Warn**, or **Allow**) for **Red**, **Yellow**, and **Unrated** files downloads.

4. Click **Save**.

See also

How site patterns work on page 21
How multiple-instance policies work on page 23

Block or warn unknown URLs and file downloads

Zero day protection allows you to block, warn, or allow the URLs and file downloads that is unknown to or unrated by Global Threat Intelligence server.

Configure **Zero Day Protection** setting in **General** policy to block, warn, or allow an unknown site.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **General**.
3. On the **Action Enforcement** tab, select the **Zero Day Protection** level as needed then click **Save**.

Block or warn site access based on content category

Configure settings in the Content Actions category to set the action for any site content category. By default, all content categories are set to Allow.

This policy is available only if you have installed the Web Filtering for Endpoint extension.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Content Actions**.
3. Select an item from a filter list or type the name of the item in the filter box to determine the display of content categories.
4. Select a content category and click **Warn** or **Block** to set the action for it. The default is **Allow**.
5. Click **Save**.

Block risky sites from appearing in search results

Secure Search configures the selected search engine as the default search engine on the client system. Secure search automatically filters the malicious sites in the search result based on their safety rating. SiteAdvisor Enterprise uses Yahoo as its default search engine.

Task

Configure settings on the Secure Search tab in the General category to automatically block risky sites from appearing in your search results.

> Secure search is supported only on Internet Explorer.

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **General**.
3. Click the **Secure Search** tab.
4. Select **Enable**, select the search engine, then specify whether to block links to risky sites.

   > If changing the default search engine, restart the browser after the policy has been enforced on the system.

   1

5. Click **Save**.

Specify enforcement behavior for specific actions

Use settings in the Action Enforcement tab in the General category to specify the behavior of SiteAdvisor Enterprise when it takes action in certain situations.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **General**.
3. Select one of these actions.

Action	Description	Steps	
Block malicious and warn sites in an iframe.	When selected, SiteAdvisor Enterprise blocks access to malicious (Red) and warn (Yellow) sites that appear in an iframe.	From **iframe Support**, select **Block Malicious and Warn sites in an iframe**. Select: • **Allow Warn sites** to allow access only to warn sites that appear in an iframe. • **Enable ePO event tracking for iframe URL navigation** to apply SiteAdvisor Enterprise Event Tracking policy for an iframe URL. ℹ Enabling this option significantly increases the number of McAfee ePO events generated.	
Block websites if the Global Threat Intelligence server fails to rate or can't be reached.		When selected, if accessing a website requires a McAfee GTI lookup and SiteAdvisor Enterprise can't look it up, SiteAdvisor Enterprise prevents opening the site. When not selected SiteAdvisor Enterprise opens the site even if it can't contact McAfee GTI.	From **Fail Close**, select **Enable**.
Apply Warn action for all URLs within the same domain.	When enabled, once a parent Warn domain is allowed, SiteAdvisor Enterprise allows all subdomains without warning. When disabled, SiteAdvisor Enterprise warns for each subdomain.	From **Accept Warn action at domain level**, select **Enable**.	
Enable Observe mode.	When enabled, SiteAdvisor Enterprise tracks browsing behavior that is affected by the policy settings configured to warn or block access. ❗ SiteAdvisor Enterprise does not enforce these policy settings while Observe mode is enabled.	From **Observe mode**, select **Enable**. See *Monitoring browser protection and security* to retrieve tracked information.	

Action	Description	Steps
Check file downloads based on their ratings.	When enabled, SiteAdvisor Enterprise enforces file downloads depending on various scenarios: • Prevents downloads from websites in the Prohibit list and Exploit sites. • Prevents downloads from blocked and phishing sites. • Allows downloads from internal sites without scanning. • Allows downloads from sites with warn rating. • Scans the file using the McAfee Artemis technology	From **File download enforcement**, select **Enable**. Select **Enable Artemis scan**, then select its enforcement range to scan the file using the McAfee Artemis technology.
Annotate browser-based email clients.	When a managed node user receives an email with URLs, SiteAdvisor Enterprise displays the rating annotations for the sites rated yellow or red. Annotations also appear for blocked sites (for example, sites added in the Prohibit List).	Select one of the following: • **Enable browser-based annotations** to receive annotations for URLs in browser-based email clients. • **Enable non browser-based annotations** to receive annotations for URLs in email management tools, such as Microsoft Outlook. Restart the email client after enforcing the policy to see annotations.

Action	Description	Steps
Specify a private IP address range.	When configured, SiteAdvisor Enterprise doesn't enforce site ratings for a specified private IP address range, such as addresses used in your organization.	For **Private IP range**, select **Enable**, then specify the private IP addresses used in the network.
Enable web gateway.	When configured, SiteAdvisor Enterprise doesn't enforce site ratings if the client is using a web gateway to enforce network traffic. To enforce network through a web gateway, you must configure the web gateway to block gateway.siteadvisor.com. See *How web gateway enforcement works*.	From **Web gateway interlock**, select **Enable**. Configure these options as required: • **Client is using one of your organization's default gateways** to specify the IP address of the default gateways used in the client network. • **Web gateway enforcement is detected** to allow SiteAdvisor Enterprise to detect whether network traffic is enforced by a web gateway. • **Enter DNS name for the Internal Landmark** to specify the DNS name of a client system or a domain. When SiteAdvisor Enterprise detects the specified DNS name of a client system or a domain as an internal landmark, it stands-down from its rating and enforcement actions.

4 Click **Save**.

Tasks

- *How web gateway enforcement works* on page 40

  Web gateways protect users from threats using proactive analysis to filter malicious content from web traffic. Gateways scan a web page's active content, understand its behavior, predict its intent, and protect against targeted attacks. If your organization uses a web gateway, SiteAdvisor Enterprise is scalable to enable you to customize how you enforce your network traffic.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

How web gateway enforcement works

Web gateways protect users from threats using proactive analysis to filter malicious content from web traffic. Gateways scan a web page's active content, understand its behavior, predict its intent, and protect against targeted attacks. If your organization uses a web gateway, SiteAdvisor Enterprise is scalable to enable you to customize how you enforce your network traffic.

You can configure SiteAdvisor Enterprise to not enforce site ratings when it detects a web gateway in the client environment. SiteAdvisor Enterprise detects the web gateway either by using client's default gateway IP address or by trying to retrieve content from an external domain.

When detecting a default gateway, SiteAdvisor Enterprise compares the client's default gateway IP address with the organization's gateway IP address specified in the policy. If the IP addresses match, SiteAdvisor Enterprise determines that the client is protected by a gateway.

When detecting a web gateway, SiteAdvisor Enterprise tries to retrieve data from gateway.siteadvisor.com. If it is unable to retrieve content from this domain, it determines that the client is protected by a gateway.

> The domain gateway.siteadvisor.com should be blocked in your web gateway.

Configure proxy settings

If proxy servers are set up as intermediaries between managed systems and the Internet, use policy settings to configure those proxy server settings for SiteAdvisor Enterprise. This enables SiteAdvisor Enterprise to access the Internet through the proxy servers.

> These proxy settings apply only to SiteAdvisor Enterprise. They are not used by other security software products managed by ePolicy Orchestrator.

SiteAdvisor Enterprise supports these proxy servers:

- Microsoft Proxy Server 2.0 - Anonymous
- Microsoft Proxy Server 2.0 - Chap
- Microsoft Proxy Server 2.0 - NTLM
- Blue Coat ProxySG
- Oracle iPlanet Web Proxy Server

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **General**.
3. Click the **Proxy Server** tab.
4. Select the type of proxy server settings to use and any authentication information.
5. Click **Save**.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

Customize user notifications for blocked content

Use settings in the Enforcement Messaging category to create notifications that display when users attempt to access site content that you have blocked.

The notifications appear when users access a site you have blocked by ratings or by content, or sites that are included in the Authorize or Prohibit lists. Instead of navigating to the site, users are redirected to a page displaying the customized notification. You might use the notification to explain why the site is blocked.

The notification appears on client computers in the language configured for the client software, if you create the notification in that language.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Enforcement Messaging**.
3. Select one of these actions.

Action	Appears when users attempt to access	Steps
Create a message for rated sites.	A site for which you have associated an action with the site's rating.	1 Click the **Site** tab. 2 Select a language. 3 Type a message (up to 50 characters) for each type of site action. 4 Type explanation messages (up to 1000 characters) for sites that are warned and blocked sites by ratings or content.
Create a short message for file downloads.	A download file that you have configured to block or warn users.	1 Click the **Site Resources** tab. 2 Select a language. 3 Type a message (up to 50 characters) for each type of file download action.
Create a short message for phishing pages.	A blocked phishing page.	1 Click the **Site Resources** tab. 2 Select a language. 3 Type a message (up to 50 characters) for blocked phishing pages.
Create a short message and longer explanation for sites on the Authorize or Prohibit lists.	Sites that you added to an Authorize list or Prohibit list.	1 Click the **Authorize and Prohibit Lists** tab. 2 Select a language. 3 Type a message (up to 50 characters) and explanation (up to 1000 characters) to display for sites on the Authorize list. 4 Type a message (up to 50 characters) and explanation (up to 200 characters) to display for sites on the Prohibit list.
Create a short message and longer explanation for sites blocked when SiteAdvisor Enterprise can't obtain Global Threat Intelligence ratings.	Sites that require a McAfee GTI lookup if SiteAdvisor Enterprise can't contact McAfee GTI.	1 Click the **Fail Close** tab. 2 Select a language. 3 Type a message (up to 50 characters) to display for blocked sites. 4 Type an explanation (up to 1000 characters) to display for blocked sites. See *Specify enforcement behavior for specific actions*.

4 Add an image, such as your company logo, to warn or block pages: click the **Images** tab, then type the URL link for the image to display in the message pages.

5 Click **Save**.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

Track browsing events to use for reports

Use the **Event Tracking** policy settings to configure SiteAdvisor Enterprise events sent from client systems to the ePolicy Orchestrator database to use for queries and reports.

Task

For option definitions, click **?** in the interface.

1 From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Event Tracking**.

3 Select one of these actions.

Action	Steps
Track visits to domains and domain resources, such as downloads.	1 From **Domain and downloads**, select **Track** . 2 Under **Include traffic to internal site**, change the default setting (if required) to either **Only when the client system is disconnected from the corporate network** or **Always**.
Track content categories for all green sites. By default, SiteAdvisor Enterprise only tracks a green site if it is on a Prohibit list or has an assigned rating or content action.	From **Domains and downloads**, select **Track content categories for all green sites**. This option is available only if you have installed the McAfee Web Reporter extension and McAfee Web Reporter. See *Using McAfee Web Reporter and McAfee Web Reporter*.

Action	Steps
Capture the logged-on user name in the events sent from the client system to the ePolicy Orchestrator server.	From **Capture user name**, select **Capture logged-on user name in events**.
Track domain page views and downloads accessed from a single domain, then send the results to the McAfee Web Reporter database for queries and reports. By default, visits to private domains on your local intranet are not tracked. The following IP ranges and URLs are always treated as private domains: • 10.0.0 - 10.255.255.255 • 172.6.0.0 - 172.31.255.255 • 192.168.0.0 - 192.168.255.255 • localhost or 127.0.0.1 Tracking visits to private domains can greatly increase the size of log files and the ePolicy Orchestrator server database, where this information is stored. The **Advanced Options** tab of the **Authorize List** policy category also has a tracking option, which takes precedence over the tracking options in this policy. See *Configure additional enforcement rules*.	1 From **Page views and downloads**, select **Track**. 2 Under **Include traffic to internal site**, change the default setting to either **Only when the client system is disconnected from the corporate network** or **Always**. 3 Enter McAfee Web Reporter access information if you use McAfee Web Reporter: • Path to the location of McAfee Web Reporter • Password to access McAfee Web Reporter • Number of days to store the information This option is available only if you have installed the Web Filtering for Endpoint extension and McAfee Web Reporter. See *Using McAfee Web Reporter and McAfee Web Reporter*.

4 Click **Save**.

See also

Using SiteAdvisor Enterprise policies in ePolicy Orchestrator on page 25

4 Monitoring browser protection and security

Use ePolicy Orchestrator dashboards and monitors to monitor browser protection and security. Use queries to retrieve SiteAdvisor Enterprise data from the McAfee ePO database to create reports.

After running queries and reports over an extended period of time, you should occasionally purge the McAfee ePO database of SiteAdvisor Enterprise data to ensure proper generation of queries and reports.

Contents

Using McAfee ePO dashboards and monitors to track SiteAdvisor Enterprise activity

Dashboards are collections of *monitors* that track activity in your ePolicy Orchestrator environment.

Use ePolicy Orchestrator dashboards to monitor SiteAdvisor Enterprise.

SiteAdvisor Enterprise provides predefined dashboards and monitors. You can use predefined dashboards as is, modify predefined dashboards to add or remove monitors, or create new dashboards using ePolicy Orchestrator. For information on permissions required to create custom dashboards, see *Permission sets*.

For information on creating and using dashboards, see the ePolicy Orchestrator documentation. See also *Common dashboards*.

SiteAdvisor Enterprise provides the following predefined dashboards and monitors:

Table 4-1 SiteAdvisor Enterprise predefined dashboards and monitors

Dashboard	Monitor
SAE: Activity	Top 100 Red Sites
	Top 100 Yellow Sites
	Top 100 Unrated Sites
	Top 100 Red Downloads
	Top 100 Yellow Downloads
	Top 100 Unrated Downloads
SAE: Authorize/Prohibit Lists	Top 100 Sites on Authorize List
	Top 100 Sites on Prohibit List

Table 4-1 SiteAdvisor Enterprise predefined dashboards and monitors *(continued)*

Dashboard	Monitor
	Top 100 Red Sites on Authorize List
SAE: Security Summary	Visits by Rating
	Visits by Action
	Downloads by Rating
	Downloads by Action
SAE: Warned/Blocked	Top 100 Blocked Sites
	Top 100 Blocked Red Sites
	Top 100 Warned-Cancelled Sites
	Top 100 Warned-Continued Sites

Using McAfee ePO queries and reports to monitor SiteAdvisor Enterprise

Queries are questions that you ask ePolicy Orchestrator, which returns answers as charts and tables. *Reports* enable you to package one or more SiteAdvisor Enterprise queries into a single PDF document, for access outside of ePolicy Orchestrator.

Use ePolicy Orchestrator queries to retrieve information about browsing activity on managed systems. You can export, download, combine queries into reports, and use most queries as dashboard monitors.

Similar information is available by accessing activity logs from the SiteAdvisor Enterprise Console on individual systems.

SiteAdvisor Enterprise provides predefined queries. You can use predefined queries as is, edit predefined queries, or create queries from events and properties in the ePolicy Orchestrator database. To create custom queries, your assigned permission set must include the ability to create and edit private queries.

You can restrict access to reports using groups and permission sets in the same way you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this allows for consistent access control.

For information on creating and using queries and reports, see the ePolicy Orchestrator documentation.

Predefined queries

SAE: Download Log

SAE: Downloads by Action

SAE: Downloads by Rating

SAE: Functional Compliance

SAE: Top 100 Blocked Red Sites

SAE: Top 100 Blocked Sites

SAE: Top 100 Red Downloads

SAE: Top 100 Red Sites

SAE: Top 100 Red Sites on Authorize List

SAE: Top 100 Unrated Sites

SAE: Top 100 Warned-Cancelled Sites

SAE: Top 100 Warned-Continued Sites

SAE: Top 100 Yellow Downloads

SAE: Top 100 Yellow Sites

SAE: Top Sites Grouped by Content

SAE: Visit Log

SAE: Visits by Action

SAE: Visits by Action Grouped by Content

SAE: Top 100 Sites on Authorize List

SAE: Top 100 Sites on Prohibit List

SAE: Top 100 Unrated Downloads

SAE: Visits by Content

SAE: Visits by Rating

Custom queries

SiteAdvisor Enterprise provides a predefined Result Type (included in the **SiteAdvisor Enterprise** Feature Group) that you can use when creating custom queries. In addition, for each Result Type, SiteAdvisor Enterprise provides properties to use to narrow the scope of data that the query retrieves and displays.

Table 4-3 SiteAdvisor Enterprise result types and properties

Feature Group	Result Type	Property (Column)	Property (Column)
SiteAdvisor Enterprise	SiteAdvisor Enterprise Events	Action	email
		Affiliations	Event Type
		Annoyances	Exploits
		Content	List Type
		Count	Observe Mode
		Date/Time	Rating
		Domain	Reason
		Download	URL
		E-Commerce	User Name
	SiteAdvisor Enterprise Client Properties	Functional in Chrome	Functional in Internet Explorer
		Functional in Firefox	Nonfunctional for Users
	SiteAdvisor Enterprise Properties	Hotfix/Patch Version	Product Version
		Language	Service Pack

Using McAfee ePO server tasks to purge SiteAdvisor Enterprise events from the database

Server tasks are scheduled management or maintenance tasks that you run on your ePolicy Orchestrator server.

Server tasks enable you to schedule and automate repetitive ePolicy Orchestrator tasks. Use ePolicy Orchestrator server tasks to monitor your server and the SiteAdvisor Enterprise software. For example, you can configure a server task to periodically remove SiteAdvisor Enterprise events from ePolicy Orchestrator database.

You can use predefined server tasks as is, edit predefined server tasks, or create new server tasks using ePolicy Orchestrator. For information on permissions required to create custom server tasks, see *Permission sets*.

To create a custom SiteAdvisor Enterprise server task, in the **Server Task Builder**, select the following from the **Action** drop-down list.

Table 4-4 SiteAdvisor Enterprise predefined Action

Action	Description
Purge SiteAdvisor Enterprise Events	Purges SiteAdvisor Enterprise records older than a specified date.

For information about creating and using server tasks, see the ePolicy Orchestrator documentation.

5 Reference

This section answers some frequently asked questions and explains how to find more information about using SiteAdvisor Enterprise.

Contents

Frequently asked questions

These questions address many typical issues that arise when deploying SiteAdvisor Enterprise to managed network systems.

Policy enforcement

How can users circumvent SiteAdvisor Enterprise policy settings and hide their browsing behavior?

Users can use several methods to hide browsing activity, including:

- Creating an application that browses the web or creating a frame page where the content of a frame loads websites.
- Disabling the SiteAdvisor Enterprise client software by using the **Add-ons** feature through the browser's **Tools** menu. However, this action can be performed only on a Google Chrome browser.

To protect against these situations:

- Check browsing behavior and browser usage regularly by using various queries that track browsing behavior. This lets you know when particular managed systems show no browsing data or less browsing data than expected.
- Check the functional status of the client software by using the **Functional Compliance** query. This lets you know when the software is disabled.

By setting up monitors that use the applicable queries, or frequently checking reports generated by these queries, you know when users are circumventing policy settings and can take immediate steps to ensure compliance. See *Monitoring browser protection and security* for more information.

Information tracking and reporting

If Microsoft Internet Explorer is the only browser installed on a managed system when SiteAdvisor Enterprise is deployed, does SiteAdvisor Enterprise need to be redeployed after installing Mozilla Firefox or Google Chrome?

No. The SiteAdvisor Enterprise client software detects Firefox when it is installed and immediately begins to protect searching and browsing activities in that browser, while continuing to provide protection for Internet Explorer.

Color coding

Why is the SiteAdvisor button gray?

Several causes are possible:

- The site is not rated.
- The SiteAdvisor Enterprise client software is disabled. If the administrator has not disabled it at the policy level (by configuring a Disable/Enable policy option), click the arrow on the menu button to display the **SiteAdvisor** menu, then select **Enable SiteAdvisor**. (If SiteAdvisor Enterprise is already enabled, the menu option changes to **Disable SiteAdvisor**. Neither menu option is available if the administrator has disabled them at the policy level.)
- The site is on the Authorize list and the **Track events** option is disabled (in the Authorize List policy). When authorized sites are not being tracked, the SiteAdvisor server does not receive data about the sites; therefore, it cannot display a color-coded rating for the sites.

Versions of SiteAdvisor software

What are the differences between the consumer version of SiteAdvisor and SiteAdvisor Enterprise?

SiteAdvisor Enterprise has been modified for management by an administrator with ePolicy Orchestrator. In addition, the automatic update feature has been removed to ensure that administrators control the version of the software running on managed systems.

General

Is it safe to use SiteAdvisor Enterprise as my only source of security against web-based threats?

No. SiteAdvisor Enterprise tests a variety of threats, and constantly adds new threats to its testing criteria, but it cannot test for all threats. Users should continue to employ traditional security defenses, such as virus and spyware protection, intrusion prevention, and network access control, for a multi-tiered defense.

Where to find more information

Several sources of additional information and support are available for using SiteAdvisor Enterprise under ePolicy Orchestrator.

ePolicy Orchestrator documentation

For detailed information on installing and managing applications under ePolicy Orchestrator, visit the McAfee ServicePortal website: https://mysupport.mcafee.com/Eservice/Default.aspx.

To view a complete listing of the ePolicy Orchestrator documentation available for download:

1. Under **Useful Links**, click **Product Documentation**.
2. Click **ePolicy Orchestrator** , then **ePolicy Orchestrator 4.5** or **ePolicy Orchestrator 4.6**.

SiteAdvisor Enterprise website

For the latest information about SiteAdvisor Enterprise and relevant white papers, visit: http://www.mcafee.com/us/products/siteadvisor-enterprise.aspx.

Online SiteAdvisor Enterprise forums

For the most current information on SiteAdvisor Enterprise issues and web threats, visit these McAfee online forums:

- https://community.mcafee.com/community/business/system/siteadvisor_enterprise
- http://www.mcafee.com/us/products/siteadvisor-enterprise.aspx

Threat Intelligence website

Visit the http://www.mcafee.com/threat-intelligence/site/default.aspx website which shows information on the URL's web reputation, affiliations, DNS servers and associations.

6 Using McAfee Web Reporter

With the McAfee Web Reporter reporting tool, you can define your browsing environment based on site content categories and create detailed reports on web usage.

Contents

How web content filtering works

The Web Filtering for Endpoint extension provides extra filtering ability. When installed, a **Content Actions** policy category becomes available. When a policy in this category is applied to client systems, SiteAdvisor Enterprise also returns content classification ratings for a site. SiteAdvisor Enterprise applies **Content Actions** policy settings to block, warn, or allow the site based on content type on client systems.

The approximately 100 site content categories are grouped by function and risk, which allows for easy application of the policy settings based on content alone or on content functional groups or risk groups.

Policy additions with web content filtering

When you install the Web Filtering for Endpoint extension, you add the following policy options:

- **Content Actions** policy settings with all content filtering options.

  See *Apply the Content Actions policy*.

- These **Event Tracking** policy settings:
  - Track website pages viewed and files downloaded (for public or private domains)
  - Track allowed green site content categories
  - Enter McAfee Web Reporter access information

  See *Tracking events for reports*.

Report and dashboard additions with web content filtering

When you install the Web Filtering for Endpoint extension, you add content-related queries for reports and dashboards.

See *Monitoring browser protection and security* for more information on working with reports and dashboards.

You can use queries as the basis for dashboard monitors, or you can run them separately.

The predefined Web Filtering for Endpoint queries, which appear in the list of reports as a SiteAdvisor Enterprise (SAE) reports, include:

Query Name	Description
Top Sites Grouped by Content	Top sites grouped by content over the last 30 days.
Visits by Content	Pie chart depicting the number of visits over the last 30 days grouped by site content.
Visits by Action Grouped by Content	Bar chart depicting the number of visits to each content category over the last 30 days, grouped by policy-based actions.

How McAfee Web Reporter works

McAfee Web Reporter provides reports showing web usage and trends in your organization. Used in connection with Web Filtering for Endpoint, McAfee Web Reporter provides the reports that help manage access to the web to protect against liability exposure, productivity loss, bandwidth overload, and security threats.

The McAfee Web Reporter server collects and processes log files and imports the data from the log file to the database. After the log file data is transferred to the database, reports are generated. Log files are generated by running a SiteAdvisor Enterprise client task from the ePolicy Orchestrator server on all managed systems.

These groups of people are involved in the McAfee Web Reporter environment:

- Web users who have SiteAdvisor Enterprise installed and enabled in their browser
- Reporting users who create and view the reports
- Reporting administrator who installs, configures, and maintains the McAfee Web Reporter server

The reporting users log on to the McAfee Web Reporter server with a web-based interface to view reports. A reporting administrator uses the same Web-based interface to manage how McAfee Web Reporter is used in the organization; including creating login accounts, managing delegated reporting, configuring email settings, managing mapped columns, and managing the database, directories, and log sources.

McAfee Web Reporter environment

The McAfee Web Reporter environment comprises these areas:

- **McAfee Web Reporter** is the server-based software with a web-based user interface and configuration settings that create detailed reports.
- **Log sources** are devices on the network set up to generate or store log files. Log files contain web filtering data, including information such as user names, IP addresses, URLs, time stamps, and protocol types. McAfee Web Reporter collects and processes the log files and then imports the data into its database. A log source can be a directory on the McAfee Web Reporter report server, an FTP Server, or NetCache.
- **Database** stores data from each log source, and reports are generated using the data. Supported external database platforms include Microsoft SQL 2000 and 2005, MySQL 5.0, and Oracle 9 and 10.

Send McAfee Web Reporter logs

The McAfee Web Reporter server needs to collect and process log files of browsing data. After the log file data is transferred to the database, reports can be generated. To get the log files to the McAfee Web Reporter server, you must run an ePolicy Orchestrator server client task. Use this task to set up the client task to run on managed systems.

Before you begin

The client task to send McAfee Web Reporter logs is available only after the Web Filtering for Endpoint extension has been installed. Also, the settings in the Event Tracking policy for access to the McAfee Web Reporter server must be in place.

When the task takes place, SiteAdvisor Enterprise sends any and all McAfee Web Reporter data to the McAfee Web Reporter configured in the Event Tracking policy. SiteAdvisor Enterprise collects all data logs from the secure SiteAdvisor Enterprise database and sends McAfee Web Reporter logs on page view and file downloads to the appropriate McAfee Web Reporter server, based on user- or system-based policy.

Because of the amount of data that can be transferred when the logs are sent, setting the client task to run on a randomized schedule is highly recommended.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Systems** | **System Tree**.
2. On the **Client Tasks** tab, click **New Task**.
3. Name the task, and from the Type menu select **Send Web Reporter Logs (Web Filtering for Endpoint)**.
4. Click **Next**, then click **Next** again.
5. On the Schedule page set the schedule for the task. Select **Enable Randomization** and set the randomization period.
6. Click **Next**, then click **Save**.

Block or warn site access based on content category

Configure settings in the Content Actions category to set the action for any site content category. By default, all content categories are set to Allow.

This policy is available only if you have installed the Web Filtering for Endpoint extension.

Task

For option definitions, click **?** in the interface.

1. From ePolicy Orchestrator, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **SiteAdvisor Enterprise 3.5.0**; from the **Category** list, select **Content Actions**.
3. Select an item from a filter list or type the name of the item in the filter box to determine the display of content categories.
4. Select a content category and click **Warn** or **Block** to set the action for it. The default is **Allow**.
5. Click **Save**.

Work with McAfee Web Reporter

For detailed information on how to configure and use McAfee Web Reporter to generate reports, see the McAfee Web Reporter documentation.

Topics in the *McAfee Web Reporter Installation and Configuration Guide* and the *McAfee Web Reporter Product Guide* include:

- Entering license information
- Connecting to the database
- Defining directories
- Configuring log sources
- Customizing a log format
- Setting up email delivery
- Managing login accounts
- Configuring options
- Optimizing performance
- Maintenance
- Running reports

7 Enforcing network traffic through a web gateway

Web gateways use proactive analysis to filter malicious content from web traffic. They scan a web page's active content, understand its behavior, predict its intent, and protect against targeted attacks.

If your organization uses a web gateway, SiteAdvisor Enterprise is scalable to enable you to customize how you enforce your network traffic.

Contents

How web gateway enforcement works

Web gateways protect users from threats using proactive analysis to filter malicious content from web traffic. Gateways scan a web page's active content, understand its behavior, predict its intent, and protect against targeted attacks. If your organization uses a web gateway, SiteAdvisor Enterprise is scalable to enable you to customize how you enforce your network traffic.

You can configure SiteAdvisor Enterprise to not enforce site ratings when it detects a web gateway in the client environment. SiteAdvisor Enterprise detects the web gateway either by using client's default gateway IP address or by trying to retrieve content from an external domain.

When detecting a default gateway, SiteAdvisor Enterprise compares the client's default gateway IP address with the organization's gateway IP address specified in the policy. If the IP addresses match, SiteAdvisor Enterprise determines that the client is protected by a gateway.

When detecting a web gateway, SiteAdvisor Enterprise tries to retrieve data from gateway.siteadvisor.com. If it is unable to retrieve content from this domain, it determines that the client is protected by a gateway.

> The domain gateway.siteadvisor.com should be blocked in your web gateway.

Policy options with web gateway enforcement

With web gateway enforcement, SiteAdvisor Enterprise provides options in the **General** policy under **Action Enforcement** tab.

- Client is using one of organizations default IP address
- Web gateway enforcement is detected

For details on applying web gateway enforcement, see *Enabling web gateway enforcement*.

Index