Product Guide
Revision

McAfee SiteAdvisor Enterprise 3.5.0
for use with ePolicy Orchestrator 4.5—4.6
Contents

Preface 5
   About this guide .................................. 5
   Audience .................................. 5
   Conventions .................................. 5
   How to use this guide ............................. 6
   Finding product documentation ...................... 6

1 Introducing SiteAdvisor Enterprise 7
   Benefits of using SiteAdvisor Enterprise ............. 7
   How safety ratings are compiled ...................... 8
   Safety icons and balloons protect during searches . 8
      Using site safety balloons ......................... 9
   SiteAdvisor menu protects while browsing ........... 9
      Using the SiteAdvisor menu ......................... 10
   Safety reports provide details ....................... 10
      Viewing site reports ............................. 11
   Administrators customize policy settings ............ 11

2 Setting up a Browsing Security Strategy 13
   Guidelines for creating a strategy ................... 13
   Select the right policy options and features ........ 14
   Information that SiteAdvisor Enterprise sends ....... 15

3 Configuring Policies 17
   How policies work ................................ 17
   Types of policy categories .......................... 18
   Default policy settings ............................. 19
   Creating and editing policies ....................... 20
   General policy options and what they control ....... 21
      Configuring proxy settings ....................... 22
      Enabling observe mode ............................ 23
      Setting the control panel option ................. 23
      Enforcing file downloads ......................... 23
      Annotating email clients ........................ 24
      Adding private IP address range ................... 24
      Enabling web gateway enforcement ................ 24
   Hardening policy for SiteAdvisor Enterprise ......... 25
      Protecting SiteAdvisor Enterprise ................. 25
      Blocking use of browsers ........................ 26
   Block and warn sites by ratings ..................... 27
      Configuring access based on ratings ............... 27
   Use Authorize and Prohibit lists for sites .......... 29
      How site patterns work ........................... 29
      How multiple-instance policies work .............. 31
      Working with Authorize lists .................... 31
Preface

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

Contents

- About this guide
- Finding product documentation

About this guide

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

Audience

McAfee documentation is carefully researched and written for the target audience. The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

- **Book title or Emphasis**: Title of a book, chapter, or topic; introduction of a new term; emphasis.
- **Bold**: Text that is strongly emphasized.
- **User input or Path**: Commands and other text that the user types; the path of a folder or program.
- **Code**: A code sample.
- **User interface**: Words in the user interface including options, menus, buttons, and dialog boxes.
- **Hypertext blue**: A live link to a topic or to a website.
- **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.

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

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introducing SiteAdvisor Enterprise

McAfee® SiteAdvisor® Enterprise is a browser protection solution that can be deployed and managed by using McAfee ePolicy Orchestrator server.

The client software runs on managed systems to protect users from threats they encounter while searching and browsing websites with Internet Explorer, Firefox, or Google Chrome or downloading files with Internet Explorer. SiteAdvisor® Enterprise is integrated with McAfee advanced protection solutions.

This guide provides information that you need to create a browsing security strategy for your business and configure SiteAdvisor® Enterprise policy options.

Contents

- Benefits of using SiteAdvisor Enterprise
- How safety ratings are compiled
- Safety icons and balloons protect during searches
- SiteAdvisor menu protects while browsing
- Safety reports provide details
- Administrators customize policy settings

Benefits of using SiteAdvisor Enterprise

As SiteAdvisor Enterprise runs on each managed system, it notifies users about threats they might encounter when searching or browsing websites by displaying the following:

Safety rating for each site

- When searching, safety ratings as per the colors indicating the degree of safety appear next to each site listed on a search results page.
- When browsing, the SiteAdvisor menu button appears in the browser window in the color that matches the safety rating for the current site.

Safety report for each site

- The report includes a detailed description of test results and feedback submitted by users and site owners.
- Users access safety reports to learn more about how the safety rating for a site was calculated.

Using the ePO Policy Catalog, administrators can create SiteAdvisor Enterprise policies that determine which sites managed systems can access. They can assign actions to sites based on their SiteAdvisor rating (for example, block red sites and warn users trying to access yellow sites). They can create lists of authorized and prohibited sites based on URLs and domains. Administrators can also customize the messaging that SiteAdvisor Enterprise displays to managed systems, and prevent users from disabling the client software on managed systems.
With the addition of the Web Filtering for Endpoint extension, you can expand safety ratings to include site content and track pages viewed on domain sites. With the addition of Web Reporter you can create detailed reports on websites.

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

The only difference in functionality between the browsers is that Firefox does not allow users to hide the SiteAdvisor button with the View | Toolbars command or check file downloads.

---

**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 signup forms to check 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.

---

**Safety icons and balloons protect during searches**

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:

- ![Green checkmark](https://example.com/checkmark) Tests revealed no significant problems.
- ![Exclamation mark](https://example.com/exclamation) Tests revealed some issues users should know about. For example, the site tried to change the testers’ browser defaults, displayed popups, or sent them a significant amount of non-spam email.
- ![Red x](https://example.com/red-x) 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.
- ![Red circle](https://example.com/red-circle) This site is blocked by a Prohibit List, Rating Actions, or Content Actions policy option.
- ![Question mark](https://example.com/question-mark) This site is unrated.

Placing the cursor over an icon displays a safety balloon that summarizes the safety report for a site. Click More Info or a report link for a detailed safety report.
Using site safety balloons

Use this task to view additional information available through a site’s safety icon listed in a search results page.

Task

1. Hold the cursor over the site’s safety icon. A safety balloon displays a high-level summary of the site’s safety report.

2. Click a safety report link or the More info link in the safety balloon to view details of the site's safety report.

SiteAdvisor menu protects while browsing

When users browse to a website, a color-coded menu button appears in the top-left corner of the window. The color of the button corresponds to the site’s safety rating. Placing the cursor over this button displays a safety balloon that summarizes the safety report for the site, with a link to the detailed site report page. The menu button next to the icon displays the SiteAdvisor menu.

<table>
<thead>
<tr>
<th>This button...</th>
<th>With this color...</th>
<th>Indicates this...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The site is safe.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>There might be some issues with the site.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>There might be some serious issues with the site.</td>
</tr>
<tr>
<td><img src="image" alt="Gray" /></td>
<td>Gray</td>
<td>No rating is available for the site.</td>
</tr>
<tr>
<td><img src="image" alt="Orange" /></td>
<td>Orange</td>
<td>A communication error occurred with the SiteAdvisor website that contains rating information.</td>
</tr>
<tr>
<td><img src="image" alt="Blue" /></td>
<td>Blue</td>
<td>This could be an internal site or private IP range.</td>
</tr>
<tr>
<td><img src="image" alt="White" /></td>
<td>White</td>
<td>The site is authorized by ePO administrator.</td>
</tr>
<tr>
<td><img src="image" alt="Silver" /></td>
<td>Silver</td>
<td>The site is disabled by ePO administrator or policy.</td>
</tr>
<tr>
<td><img src="image" alt="Black" /></td>
<td>Black</td>
<td>The site is a phishing site. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.</td>
</tr>
</tbody>
</table>

If the gray communication error button appears, a troubleshooting link in the site's safety balloon opens to a connection status page. This page displays the reason for the communication error and provides information on possible resolutions. Clicking this link runs these tests with these results:

<table>
<thead>
<tr>
<th>Test</th>
<th>What this means</th>
<th>Explanation if there is an issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Access</td>
<td>Does the browser have internet access?</td>
<td>Your computer cannot access the Internet. This might indicate the SiteAdvisor policy for proxy settings are configured incorrectly. Contact your administrator.</td>
</tr>
<tr>
<td>SiteAdvisor Server Availability</td>
<td>Is the SiteAdvisor server down?</td>
<td>The SiteAdvisor servers appear to be down.</td>
</tr>
</tbody>
</table>
The Repeat Tests button allows the user to see if the error persists or has been corrected while the page is open.

**Using the SiteAdvisor menu**

Use this task to display the options for accessing SiteAdvisor features on managed systems.

**Task**

1. Click the down arrow on the SiteAdvisor menu button to view the SiteAdvisor menu and do any of the following:

<table>
<thead>
<tr>
<th>Select this command...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Site Report</td>
<td>Display the safety report for the current site (not available when SiteAdvisor Enterprise is disabled). You can also click Read site report in the site safety balloon.</td>
</tr>
<tr>
<td>Show Balloon</td>
<td>Display the current site’s safety balloon (not available when SiteAdvisor Enterprise is disabled). The balloon disappears after a few seconds, or you can click the close button. • The site safety balloon also appears by placing the cursor over the menu button. • The site safety balloon doesn't appear in Google Chrome.</td>
</tr>
<tr>
<td>Disable/Enable SiteAdvisor</td>
<td>Turn the SiteAdvisor Enterprise client software off or on (available only when an Enable/Disable policy option is configured to allow this functionality).</td>
</tr>
<tr>
<td>About</td>
<td>Access a brief description of browser protection, its license agreement, and its privacy policy.</td>
</tr>
</tbody>
</table>

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.

**Safety reports provide details**

Users can supplement the color-coded safety information for a site by viewing its detailed safety report. These reports describe specific threats discovered by testing and include feedback submitted by site owners and users.

Safety reports for sites are delivered from the McAfee SiteAdvisor and provide the following information:
<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>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 sites flagged as red. 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.</td>
</tr>
<tr>
<td><strong>Online Affiliations</strong></td>
<td>Examines how aggressively the site tries to get you to go to other sites that we’ve flagged with red verdicts. It is a very common practice on the Internet for suspicious sites to have many close associates 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 warning 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.</td>
</tr>
<tr>
<td><strong>Web Spam Tests</strong></td>
<td>Web Spam Tests results are SiteAdvisor's overall rating for a Web site's e-mail practices. We rate sites based on both how much e-mail we receive after entering an address on the site as well as how spammy the e-mail we receive looks. If either of these measures is higher than what we consider acceptable, we'll give the site a yellow warning. If both measures are high, or one of them looks particularly egregious, we'll give the site a red warning.</td>
</tr>
<tr>
<td><strong>Download Tests</strong></td>
<td>Download Tests results indicate SiteAdvisor's 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.</td>
</tr>
</tbody>
</table>

**Viewing site reports**

Use this task to view site reports to obtain more information about a site’s safety rating.

**Task**

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

<table>
<thead>
<tr>
<th>From this location...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>• Click the SiteAdvisor menu button and select View Site Report.</td>
</tr>
<tr>
<td></td>
<td>• Click the SiteAdvisor button.</td>
</tr>
<tr>
<td>Search results page</td>
<td>Click the safety icon following the web page link.</td>
</tr>
</tbody>
</table>

**Administrators customize policy settings**

Administrators create SiteAdvisor Enterprise policies in the ePO Policy Catalog and assign them 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.

Configure policies in SiteAdvisor Enterprise to achieve the right level of browsing protection for your users. Note that 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.
<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize List (A multiple-instance policy)</td>
<td>• Create a list of sites that are approved for users to access.</td>
</tr>
<tr>
<td></td>
<td>• Configure access to site resources, such as file downloads and phishing pages, on approved sites.</td>
</tr>
<tr>
<td></td>
<td>• Specify whether an Authorize list has precedence over Prohibit lists.</td>
</tr>
<tr>
<td>Enable/Disable</td>
<td>• Disable and then re-enable the SiteAdvisor Enterprise client software for all ePO managed systems using this policy.</td>
</tr>
<tr>
<td></td>
<td>• Allow the disabling and re-enabling of the SiteAdvisor Enterprise client software from the browser on managed systems and configure whether or not this functionality requires a password.</td>
</tr>
<tr>
<td>Enforcement Messaging</td>
<td>Create messages, which can include your own logo or image, for users who attempt to access:</td>
</tr>
<tr>
<td></td>
<td>• Blocked sites • Prohibited sites</td>
</tr>
<tr>
<td></td>
<td>• Warned sites • Phishing pages</td>
</tr>
<tr>
<td></td>
<td>• Authorized sites • File downloads</td>
</tr>
<tr>
<td>Event Tracking</td>
<td>• Report on domain site visits.</td>
</tr>
<tr>
<td></td>
<td>• Report on internal domain site visits.</td>
</tr>
<tr>
<td></td>
<td>• Report on page views on all domain sites. (Available with the additional Web Filtering for Endpoint extension.)</td>
</tr>
<tr>
<td>General</td>
<td>• Specify proxy server settings required to contact the Internet by managed systems running the client software.</td>
</tr>
<tr>
<td></td>
<td>• Enable Observe mode to evaluate policy settings before implementing them.</td>
</tr>
<tr>
<td></td>
<td>• Specify whether users can use Add/Remove Programs to remove SiteAdvisor Enterprise.</td>
</tr>
</tbody>
</table>

See *Configuring Policies* for more information.
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. This section provides an overview of features that assist you in customizing policy settings that are specific to your business needs. The following topics provide details about using these features.

Contents
- Guidelines for creating a strategy
- Select the right policy options and features
- Information that SiteAdvisor Enterprise sends

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 under Configuring Policies.

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 Using Dashboards, Monitors, and Reports.

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 the Configuring Policies chapter for more information.
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* under *Configuring Policies*.

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 *Using Dashboards, Monitors, and Reports* and *Configuring Policies*.

---

### Select the right policy options and 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 would like 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.

<table>
<thead>
<tr>
<th>If this is your security or productivity goal...</th>
<th>Use this feature...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SiteAdvisor ratings to control access to sites, download files, or phishing pages.</td>
<td>Rating Actions policy</td>
</tr>
<tr>
<td>Block particular sites or domains.</td>
<td>Prohibit List policy</td>
</tr>
<tr>
<td>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.</td>
<td>Authorize List policy</td>
</tr>
<tr>
<td>Prevent data about intranet sites from being reported to the SiteAdvisor website’s servers.</td>
<td>Event Tracking policy</td>
</tr>
<tr>
<td>Communicate to users why a site is blocked or how to protect against threats on a site.</td>
<td>Enforcement Messaging policy</td>
</tr>
<tr>
<td>Control who can disable or enable the SiteAdvisor Enterprise client software.</td>
<td>Disable/Enable policy</td>
</tr>
<tr>
<td>Evaluate the effect of policy settings before they are implemented.</td>
<td>Observe mode (part of General policy)</td>
</tr>
</tbody>
</table>
If this is your security or productivity goal... | Use this feature...
---|---
Enter information on any proxy server needed for Internet access. | Proxy Server (part of General policy)
Obtain information for and track activity on private domain servers. | Event Tracking policy
Obtain information for and track visits to non-private domain servers. | Event Tracking policy
Obtain information for and track each page accessed from domain servers. | Event Tracking policy
Monitor the effect of current policy settings. | Queries and monitors
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 with Web Filtering for Endpoint extension
Obtain detailed reports based on site content. | Web Reporter with Web Filtering for Endpoint extension

See Configuring Policies for information about using the policy features. See Using Dashboards, Monitors, and Reports for information about queries and monitors.

Information that SiteAdvisor Enterprise sends
The client software sends the following information to the 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 website’s servers.

When a managed system visits a website, SiteAdvisor Enterprise tracks the URL which 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 website’s servers, unless specifically requested. See Tracking visits to domains and downloads under Configuring Policies for more information.
Configuring 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
- How policies work
- Types of policy categories
- Default policy settings
- Creating and editing policies
- General policy options and what they control
- Hardening policy for SiteAdvisor Enterprise
- Block and warn sites by ratings
- Use Authorize and Prohibit lists for sites
- Customize messages for users
- Enable or disable the software
- Track events for reports

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 meet your needs.

In general, a policy is applied to a group, and all systems in the group receive the same policy settings. If, however, you are working in an ePO 4.5/4.6 environment, where the ePO server is version 4.5/4.6 and the McAfee Agent on the client system is version 4.5/4.6, 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 ePO group in which the system is placed. For more information, see How Policy Assignment Rules Work in the ePolicy Orchestrator4.5 Product Guide.

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.

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 ePolicy Orchestrator Product Guide.
Types of policy categories

For the SiteAdvisor Enterprise software, configure these policy categories:

- **Authorize List** — Sites that users are authorized to access, and rules for accessing the individual resources on the sites. Several instances of this policy can be applied, resulting in one combined, effective policy.

- **Enable/Disable** — 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.

- **Enforcement Messaging** — Text displayed to users who attempt to access a site, phishing page, or file download that has been blocked, warned, or allowed.

- **Event Tracking** — Settings to track domain visits and downloads. If the Web Filtering for Endpoint extension and Web Reporter are installed, you can also track pages views and downloads within a domain and send information to Web Reporter for reports.

- **General** — Settings required for managed systems to access the Internet through a proxy server, to turn on Observe mode to tune enforcement rules, and to allow SiteAdvisor Enterprise to be removed with Add or Remove Programs.

- **Hardening** — Settings to prevent managed node users from uninstalling SiteAdvisor Enterprise and to prevent any unwanted changes to SiteAdvisor Enterprise files, registry keys, and registry values by restricting access.

- **Prohibit List** — Sites that users are blocked from accessing. Several instances of this policy can be applied resulting in one combined, effective policy.

- **Rating Actions** — Rules for user access based on the safety ratings and threat factors SiteAdvisor assigns to sites, pages on a site, or file downloads.

The Rating actions policies will be replaced by the content actions if Web Filtering extension is checked in. A Content Actions policy appears if the Web Filtering for Endpoint extension is installed. See the Web Filtering for Endpoint and Web Reporter Appendix for details.

For more information about using policies with ePolicy Orchestrator, see the ePolicy Orchestrator Product Guide.
Default policy settings

During installation, a default SiteAdvisor Enterprise policy is added to the ePO master repository and listed in the Policy Catalog. The default policy settings are:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Default policy settings</th>
</tr>
</thead>
</table>
| Authorize List | No Authorize list is set up.  
After a list is created, default settings for the advanced options are:  
  • **Track events**: Selected.  
  • **Block phishing pages**: Selected.  
  • **File downloads**:  
    • **Yellow**: Warn  
    • **Red**: Block  
    • **Unrated**: Allow  
  • **Give this Authorize list precedence**: Not selected. |
| Enable/Disable |  
  • **SiteAdvisor policy enforcement** — **Enable**: Selected. The client software is enabled on all systems managed with this policy.  
  • **SiteAdvisor menu option** — **Enable**: Not selected. The client software cannot be disabled from the managed system. |
| Enforcement Messaging | No custom messages or logos are displayed to users when they attempt to access allowed, warned, or blocked sites and site resources. |
| General |  
  • **No proxy settings are defined.**  
  • **Observe mode** — **Enable**: Not selected. Options configured for blocking or warning are enforced.  
  • **File download enforcement** — Not selected. Downloads with any safety rating.  
  • **Email annotation** — Not selected. Does not provide safety rating for the links in an instant message or an email.  
  • **Private IP range** — Not selected. Evaluates all websites including private IP addresses.  
  • **Web gateway interlock** — Not selected. Forces SiteAdvisor Enterprise to stand-down mode when a web gateway is detected on the client network.  
  • **Control Panel Option** — **Enable**: Not selected. to have SiteAdvisor Enterprise appear in the client system Add or Remove Programs control panel is not selected. |
| Hardening |  
  • **Protect SiteAdvisor resources** — Selected. Restricts unwanted changes to SiteAdvisor Enterprise files, registries, or services and prevents user from uninstalling the browser plug-in.  
    • **Files**: Selected  
    • **Registry**: Selected  
    • **Services**: Selected  
    • **Uninstall**: Selected  
  • **Protect SiteAdvisor browser plugin** — Selected. Prevents users from disabling the browser plugin.  
  • Allows use of supported browsers and prevents use of unsupported browsers. |
<p>| Prohibit List | No Prohibit list is set up. |</p>
<table>
<thead>
<tr>
<th>Policy</th>
<th>Default policy settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Tracking</td>
<td>• Domains and downloads — Track: Selected.</td>
</tr>
<tr>
<td></td>
<td>• Include traffic to internal sites: Set to Never.</td>
</tr>
<tr>
<td></td>
<td>• Capture logged-on user name in events — Not selected. Does not capture user name in the events forwarded to ePO from the client systems.</td>
</tr>
<tr>
<td></td>
<td>• Track content categories for all green sites: Selected. Only available if the Web Filtering for Endpoint extension is installed.</td>
</tr>
<tr>
<td></td>
<td>• Page views and downloads — Track: Not selected. Only available if the Web Filtering for Endpoint extension is installed.</td>
</tr>
<tr>
<td>Rating Actions</td>
<td>• Site access based on overall rating:</td>
</tr>
<tr>
<td></td>
<td>• Yellow: Warn</td>
</tr>
<tr>
<td></td>
<td>• Red: Block</td>
</tr>
<tr>
<td></td>
<td>• Unrated: Allow</td>
</tr>
<tr>
<td></td>
<td>• Page-level rating actions: Block phishing pages selected. Phishing pages detected on allowed sites are blocked.</td>
</tr>
<tr>
<td></td>
<td>• File download rating actions:</td>
</tr>
<tr>
<td></td>
<td>• Yellow: Warn</td>
</tr>
<tr>
<td></td>
<td>• Red: Block</td>
</tr>
<tr>
<td></td>
<td>• Unrated: Allow</td>
</tr>
</tbody>
</table>

Content Actions
(Only available when the Web Filtering for Endpoint extension is installed.)

By default, most of the content categories having a green rating are allowed; yellow are warned; and red are blocked. However, some unrated content categories are warned or blocked as per GTI recommendation.

Creating and editing policies

Use this general task to create a new policy and configure its settings, or to change the settings in an existing policy.

Details for configuring settings in specific policies are provided later in this section.

For option definitions, click ? in the interface.

Task
1. From ePolicy Orchestrator, click Menu | Policy | Policy Catalog.
2. From the Product list, select SiteAdvisor Enterprise 3.5.0.
3. From the Category list, select the policy.
4. Select New to configure settings for a new policy, or select Edit to change settings for an existing policy.
5. Click Save. Run an agent wake-up call to apply the setting immediately, or wait for the next automatic agent-server communication.
General policy options and what they control

The General policy category lets you apply general policy options that control proxy server settings, application of Observe mode, and whether the software can be removed from client systems using the Add or Remove Programs control panel.

Proxy server 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.

The Proxy Server tab on the General policy page includes settings to:
- Use no proxy server (default).
- Use Internet Explorer proxy server settings.
- Manually configure proxy server settings.

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

Supported 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

Observe mode action enforcement

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.

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. 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.

Control panel option

You can allow or prohibit the appearance of SiteAdvisor Enterprise in the Add or Remove Programs control panel on a client system. If it appears, users can remove SiteAdvisor Enterprise. You might find this option useful in troubleshooting, but McAfee does not recommend its application. By default, this option is set to prohibit the appearance of the application in the control panel.
Tasks

- **Configuring proxy settings** on page 22
  Use this task to configure SiteAdvisor Enterprise to access the Internet through proxy servers.

- **Enabling observe mode** on page 23
  Use this task to track browsing behavior that is affected by the policy settings configured to warn or block access. These policy settings are not enforced while observe mode is enabled.

- **Setting the control panel option** on page 23
  Use this task to allow SiteAdvisor Enterprise to appear 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, but McAfee does not recommend its application.

- **Enforcing file downloads** on page 23
  SiteAdvisor Enterprise enforces file downloads depending on various scenarios. It allows the managed node users to download files from internal sites without scanning the files for malicious content. You cannot download any files from website added in Prohibit List policy and from website that are considered Exploit sites. Likewise, managed node users can not download files from blocked and phishing sites. Managed node users can download files with warn rating.

- **Annotating email clients** on page 24
  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).

- **Adding private IP address range** on page 24
  SiteAdvisor Enterprise can be configured to stand-down from its enforcement and site rating operations if it detects that the IP address of site you are accessing is within a range of specified private IP addresses.

- **Enabling web gateway enforcement** on page 24
  SiteAdvisor Enterprise can be configured to stand-down from its enforcement and site rating operations if it detects that your organization enforces network traffic through a web gateway. This option is disabled by default. SiteAdvisor Enterprise uses two methods to determine if the network traffic is enforced through a web gateway. We recommend that you use both the options to enable web gateway enforcement.

**Configuring proxy settings**

Use this task to configure SiteAdvisor Enterprise to access the Internet through proxy servers.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click Edit.
4. Click the Proxy Server tab.
5. Select the type of proxy server settings to use.
6. Specify any additional required information.
7. Click Save.
Enabling observe mode
Use this task to track browsing behavior that is affected by the policy settings configured to warn or block access. These policy settings are not enforced while observe mode is enabled.

See Using Dashboards, Monitors, and Reports for information on retrieving tracked information.

For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. Click the Action Enforcement tab.
5. Select Enable.
6. Click Save.

Setting the control panel option
Use this task to allow SiteAdvisor Enterprise to appear 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, but McAfee does not recommend its application.

For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. Click the Control Panel Option tab.
5. Select Enable.
6. Click Save.

Enforcing file downloads
SiteAdvisor Enterprise enforces file downloads depending on various scenarios. It allows the managed node users to download files from internal sites without scanning the files for malicious content. You cannot download any files from website added in Prohibit List policy and from website that are considered Exploit sites. Likewise, managed node users can not download files from blocked and phishing sites. Managed node users can download files with warn rating.

Task
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. For the policy you want to edit, click Edit, then click Action Enforcement.
4 Enable File download enforcement.
5 Click Save.

Annotating 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).

Task
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 For the policy you want to edit, click Edit, then click Action Enforcement.
4 Do one of the following:
   • Enable browser-based annotations — Select this to receive annotations for URLs in browser-based email clients.
   • Enable non browser-based annotations — Select this to receive annotations for URLs in email management tools such as Microsoft Outlook.
5 Click Save.

Restart the email client after enforcing the policy to see annotations.

Adding private IP address range
SiteAdvisor Enterprise can be configured to stand-down from its enforcement and site rating operations if it detects that the IP address of site you are accessing is within a range of specified private IP addresses.
Use this task to add a range of private IP addresses used in your organization.

Task
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 For the policy you want to edit, click Edit, then click Action Enforcement.
4 Enable the Private IP range, then specify the private IP addresses used in the client network.
5 Click Save.

Enabling web gateway enforcement
SiteAdvisor Enterprise can be configured to stand-down from its enforcement and site rating operations if it detects that your organization enforces network traffic through a web gateway. This option is disabled by default. SiteAdvisor Enterprise uses two methods to determine if the network
traffic is enforced through a web gateway. We recommend that you use both the options to enable web gateway enforcement.

**Task**

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. For the policy you want to edit, click **Edit**, then click **Action Enforcement**.
4. Enable **Web gateway interlock** and configure these options as required:
   - **Client is using one of your organization’s default gateways** — Specify the IP address of the default gateway(s) used in the client network.
   - **Web gateway enforcement is detected** — Select the option to allow SiteAdvisor Enterprise to detect whether or not network traffic is enforced by a web gateway.
   - **Enter DNS name for the Internal Landmark** — 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.

   To enforce network through a web gateway, you must configure the web gateway to block gateway.siteadvisor.com.

5. Click **Save**.

---

**Hardening policy for SiteAdvisor Enterprise**

SiteAdvisor Enterprise integrates with VirusScan Enterprise to protect itself from being uninstalled or modified. Hardening policy prevents managed node users from uninstalling SiteAdvisor Enterprise and prevents any unwanted changes to SiteAdvisor Enterprise files, registry keys, and registry values by restricting access. It also protects SiteAdvisor Enterprise processes by preventing users from stopping or killing them. Hardening policy can be configured to block the use of supported or unsupported browsers as required. The Administrator can disable and enable hardening on the managed node using a password.

Hardening is a system based policy which allows only administrators to modify the system components. Enabling hardening on managed nodes blocks the use of InPrivate browsing in Internet Explorer or Private Browsing in Mozilla Firefox.

Before enabling Hardening, ensure that Access Protection in VirusScan Enterprise is enabled on the managed nodes. For details on enabling Access Protection, refer to VirusScan Enterprise Product Guide.

**Protecting SiteAdvisor Enterprise**

Modifying SiteAdvisor Enterprise files, registries, or services can affect the functioning of the product. Hence it is important to protect these system components. The Self Protection tab in Hardening policy allows the administrator to restrict any unwanted changes to SiteAdvisor Enterprise files, registry entries, or services and prevent users from uninstalling the product.
Protecting SiteAdvisor Enterprise resources

You can configure this policy to prevent SiteAdvisor Enterprise uninstallation on client systems and protect SiteAdvisor Enterprise files, registry entries, and services.

Task
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. For the policy you want to edit, click **Edit**, then click **Self Protection**.
4. Select these options as required:
   - **Files** — To deny managed node users from modifying the SiteAdvisor Enterprise databases, binaries, safe search files, and configuration files.
   - **Registry** — To deny managed node users from modifying the SiteAdvisor Enterprise registry hive, COM components, and uninstalling using the registry value.
   - **Service** — To prevent managed node users from killing, renaming, and stopping or starting SiteAdvisor Enterprise services.
   - **Uninstall** — To prevent managed node users from uninstalling SiteAdvisor Enterprise using Add/Remove Programs in Control Panel or command prompt.
5. Click **Save**.

Protecting SiteAdvisor Enterprise browser plug-in

In previous versions of SiteAdvisor Enterprise managed node users were able to disable the plug-in on the browser. Hardening enables you to restrict users from disabling the 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.

Task
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. For the policy you want to edit, click **Edit**, then click **Self Protection**.
4. Enable **Protect SiteAdvisor browser Plugin**.
5. Click **Save**.

Blocking use of browsers

You can block the use supported or unsupported browsers on managed nodes as required.

Task
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. For the policy you want to edit, click **Edit**, then click **Browser Control**.
4. Select the browsers to block from being launched on the managed nodes.
5. Click **Save**.
Block and warn sites by ratings

The Rating Actions policy options let you use the SiteAdvisor ratings to determine whether users can access a site or resources on a site, such as download files. In addition, you can fine-tune site access by allowing the reaction to be less stringent for red and yellow sites when certain factors, such as email or downloads, are the cause for a site’s red or yellow status.

- For each yellow, red, or unrated site, specify whether to allow, warn, or block the site.
- For each yellow, red, or unrated download file, specify whether to allow, warn, or block the download. 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.

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.

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. See Ensure Access with Authorize Lists for more information.

Configuring access based on ratings

Use the Rating Actions policy settings to control access to sites or site resources based on their SiteAdvisor Enterprise rating (such as green, yellow, red, or unrated).

To control access to site resources on authorized sites, see Working with Authorize lists.

Tasks

- Blocking or warning site access based on ratings on page 27
  Use this task to block users from accessing sites that contain threats, or to warn users about potential threats on sites.

- Blocking or warning file downloads based on ratings on page 28
  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.

- Blocking phishing pages on page 28
  A site with an overall rating of green can contain phishing pages. To protect users, use this task to block access to these pages.

Blocking or warning site access based on ratings

Use this task to block users from accessing sites that contain threats, or to warn users about potential threats on sites.

Use the Enforcement Messaging policy options to customize the message that is displayed to users for blocked and warned sites.

For option definitions, click ? in the interface.

Task

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.
Block and warn sites by ratings

3 For the policy you want to edit, click Edit.
4 Click the Site tab.
5 For Site access based on overall rating, select an action for yellow, red, and unrated sites.
6 Click Save.

Blocking or warning 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. Use this task to block users from downloading files that contain threats or to warn users about potential threats from downloads.

- Use the Enforcement Messaging policy options to customize the message that is displayed to users for blocked and warned downloads.

For option definitions, click ? in the interface.

Task
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 For the policy you want to edit, click Edit.
4 Click the Site Resources tab.
5 For File download rating actions, select an action for yellow, red, and unrated files.
6 Click Save.

Blocking phishing pages
A site with an overall rating of green can contain phishing pages. To protect users, use this task to block access to these pages.

- Use the Enforcement Messaging policy options to customize the message that displays to users for blocked phishing pages.

For option definitions, click ? in the interface.

Task
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 For the policy you want to edit, click Edit.
4 Click the Site Resources tab.
5 For Page-level rating actions, select Block phishing pages.
6 Click Save.
Use Authorize and Prohibit lists for sites

Use Authorize lists to ensure that managed systems can access sites that are important to your business. Use Prohibit lists to block access to sites that are not related to job performance or do not conform to company security standards. An Authorize list contains a list of URLs or site patterns that users can access. A Prohibit list contains a list of URLs or site patterns that are blocked on all computers using the policy. See How site patterns work for more information.

If a managed system uses a policy that contains an Authorize list, the system can access sites on that list even when they are blocked or warned (by a Rating Actions policy) due to their safety rating. If a Rating Actions policy blocks red sites but a red site is added to the Authorize list, that site can be accessed. Therefore, it is important to exercise caution when adding sites to an Authorize list.

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.

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 affected by enforcement rules. This enables you to apply enforcement rules to particular domains or to 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 a site pattern as two distinct components: domain with protocol information (for example, http://, https://, or ftp://) and path.
Site pattern example: .acme.com/downloads:

<table>
<thead>
<tr>
<th>Domain component: .acme.com</th>
<th>Path component: /downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain information is matched from the end. A matching URL’s domain must end with the site pattern’s domain. The protocol can vary.</td>
<td>Path information is matched from the beginning. A matching URL’s path must begin with the site pattern’s path, which includes everything that follows the “/” after the domain.</td>
</tr>
<tr>
<td>These strings match the domain component of the site pattern:</td>
<td>These strings match the path component of the site pattern:</td>
</tr>
<tr>
<td>• <a href="http://www.acme.com">http://www.acme.com</a></td>
<td>• /downloads/news</td>
</tr>
<tr>
<td>• <a href="http://www.info.acme.com">http://www.info.acme.com</a></td>
<td>• /downloads/applications/setup.exe</td>
</tr>
<tr>
<td>• <a href="http://acme.com">http://acme.com</a></td>
<td>• /downloads/index.asp</td>
</tr>
<tr>
<td>These strings do not match the domain component of the site pattern:</td>
<td>These strings do not match the path component of the site pattern:</td>
</tr>
<tr>
<td>• <a href="http://www.myacme.com">http://www.myacme.com</a></td>
<td>• /download/news</td>
</tr>
<tr>
<td>• <a href="http://www.info.acme.net">http://www.info.acme.net</a></td>
<td>• /user/downloads/applications/setup.exe</td>
</tr>
<tr>
<td>• <a href="http://acme.com.tk">http://acme.com.tk</a></td>
<td></td>
</tr>
</tbody>
</table>

Use the "." character at the beginning of any site pattern to match a specific domain. This character disregards the protocol and introductory characters. For example, even though there is no dot before acme in http://acme.com, this pattern assumes www. and is thus a match.

You can also add port numbers after the domain (:8443, for example) as part of the site pattern to restrict access to a particular port, preventing or allowing access through the port depending on whether the site pattern is on a prohibit or authorize list. If no port number is given, all ports are matched.

Site patterns must be at least 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.

More examples:

<table>
<thead>
<tr>
<th>Site pattern</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.site.com/news">http://www.site.com/news</a></td>
<td>Matches:</td>
</tr>
<tr>
<td>The domain is <a href="http://www.site.com">http://www.site.com</a> and the path is /news. The URL string that matches this pattern must have a domain that ends with <a href="http://www.site.com">http://www.site.com</a> and a path that begins with /news.</td>
<td>• <a href="http://www.site.com/news/index.asp">http://www.site.com/news/index.asp</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="http://www.site.com:8443/news/pages/logo.gif">http://www.site.com:8443/news/pages/logo.gif</a></td>
</tr>
<tr>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td>• <a href="http://info.site.com:8443/news/pages/logo.gif">http://info.site.com:8443/news/pages/logo.gif</a></td>
</tr>
<tr>
<td>.acme.com:9090/downloads</td>
<td>Matches:</td>
</tr>
<tr>
<td>The domain is .acme.com:9090 and the path is /downloads. The URL string that matches this pattern must have a domain that ends with .acme.com:9090 and a path that begins with /downloads.</td>
<td>• <a href="http://www.acme.com:9090/downloads">http://www.acme.com:9090/downloads</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="http://acme.com:9090/downloads">http://acme.com:9090/downloads</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://news.acme.com:9090/downloads">https://news.acme.com:9090/downloads</a></td>
</tr>
<tr>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td>• <a href="http://www.myacme.com:9090/downloads">http://www.myacme.com:9090/downloads</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="http://acme.com/downloads">http://acme.com/downloads</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://news.acme.net:9090/downloads">https://news.acme.net:9090/downloads</a></td>
</tr>
</tbody>
</table>
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.

Working with Authorize lists

Use Authorize List policy options to create and manage the contents of an Authorize list, which ensures that users can access sites you consider to be important for your business.

Tasks

- Adding a site to an Authorize list on page 31
- Adding multiple sites to an Authorize list on page 32
- Deleting sites from an Authorize list on page 32
  Use this task to remove sites from an Authorize list.
- Editing information in an Authorize list on page 33
  Use this task to change a URL, site pattern, or comment that appears on an Authorize list.
- Searching an Authorize list on page 33
- Testing an Authorize list on page 33
  When Authorize List is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy (see How multiple-instance policies work).
- Blocking or warning file downloads on authorized sites on page 34
  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.
- Blocking phishing pages on authorized sites on page 34
  An authorized site can contain phishing pages. To protect users, use this task to block access to these pages.
- Turning off tracking for visits to authorized sites on page 34
  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.
- Setting list precedence on page 35
  By default, a Prohibit list has precedence over an Authorize list, which means that sites appearing on both are blocked. Using this procedure ensures that users can access any site on the Authorize list, even if it also appears on a Prohibit list.

Adding a site to an Authorize list

Use this task to add one site at a time to an Authorize list.

For option definitions, click ? in the interface.
Task
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. For the policy you want to edit, click **Edit**.
4. On the **Manage Authorized Sites** tab, click **Add**.
5. Type a URL or partial URL (called a *site pattern*) that is at least three characters in length.
6. Type a comment or note to associate with the site (optional).
7. Click **OK**.

**Adding multiple sites to an Authorize list**
Use this task to add more than one site to an Authorize list simultaneously.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click **Edit**.
4. On the **Manage Authorized Sites** tab, click **Add Multiple**.
5. 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.
6. On a new line, repeat step 5 for each site you want to add to the Authorize list.
7. Click **OK**.

**Deleting sites from an Authorize list**
Use this task to remove sites from an Authorize list.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click **Edit**.
4. On the **Manage Authorized Sites** tab, select the checkbox next to each site you want to delete from the list.
5. Click **Delete**.
Editing information in an Authorize list
Use this task to change a URL, site pattern, or comment that appears on an Authorize list.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. On the Manage Authorized Sites tab, select the checkbox next to each site you want to edit, then click Edit.
5. 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.

6. Click OK.

Searching an Authorize list
Use this task to locate URLs or site patterns in an Authorize list. This feature is useful for finding sites in large lists.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. On the Manage Authorized Sites tab, 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.
5. To clear the search criteria and again display the contents of the list, click Clear.

Testing an Authorize list
When Authorize List is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy (see How multiple-instance policies work).
Use this task to test whether specific sites or site patterns are included in an Authorize list.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4 On the Test Site Patterns tab, type a URL or partial URL in the Match URL box, then click Go. SiteAdvisor Enterprise displays any site patterns that match your entry. If no site patterns are displayed, the Authorize list does ensure access to the URL you entered.

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

Blocking or warning 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.

Use this task to block users from downloading files that contain threats or to warn users about potential threats from downloads.

Use the Enforcement Messaging policy options to customize the message that is displayed to users for blocked and warned downloads (see Customize messages for users).

For option definitions, click ? in the interface.

Task
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 For the policy you want to edit, click Edit.
4 On the Advanced Options tab, select Track events and request information from the SiteAdvisor server.
5 For File downloads, select an action for yellow, red, and unrated files.
6 Click Save.

Blocking phishing pages on authorized sites
An authorized site can contain phishing pages. To protect users, use this task to block access to these pages.

Use the Enforcement Messaging policy options to customize the message that is displayed to users.

For option definitions, click ? in the interface.

Task
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 For the policy you want to edit, click Edit.
4 On the Advanced Options tab, select Track events and request information from the SiteAdvisor server.
5 For Phishing, select Block phishing pages.
6 Click Save.

Turning 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.

Use this task to turn off the tracking feature for sites in an Authorize list.
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.

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.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.
4. Click the **Advanced Options** tab.
5. 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.
6. Click **Save**.

**Setting list precedence**

By default, a Prohibit list has precedence over an Authorize list, which means that sites appearing on both are blocked. Using this procedure ensures that users can access any site on the Authorize list, even if it also appears on a Prohibit list.

Use this task to specify that users can access sites on the Authorize list, even if they also appear 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.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.
4. On the **Advanced Options** tab, select **Track events and request information from the SiteAdvisor server**.
5. Select **Give this Authorize list precedence over Prohibit lists**.
6. Click **Save**.

**Working with Prohibit lists**

Use Prohibit List policy options to create and manage the contents of a Prohibit list, which prevents managed systems from accessing sites considered to be inappropriate or noncompliant with company policy.
Tasks

- **Adding a site to a Prohibit list** on page 36
  A Prohibit list contains a list of URLs or site patterns that are blocked on all computers using the policy.

- **Adding multiple sites to a Prohibit list** on page 36
  Use this task to add more than one site to a Prohibit list simultaneously.

- **Deleting sites from a Prohibit list** on page 37
  Use this task to remove sites from a Prohibit list.

- **Editing information in a Prohibit list** on page 37
  Use this task to change a URL, site pattern, or comment that appears on a Prohibit list.

- **Searching a Prohibit list** on page 37
  Use this task to locate URLs or site patterns in a Prohibit list. This feature is useful for finding sites in large lists.

- **Testing a Prohibit list** on page 38
  When Prohibit List is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy (see *How multiple-instance policies work*).

**Adding a site to a Prohibit list**

A Prohibit list contains a list of URLs or site patterns that are blocked on all computers using the policy.

Use this task to add one site at a time to a Prohibit list.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.
4. On the **Manage Prohibited Sites** tab, click **Add**.
5. Type a URL or partial URL (called a **site pattern**) that is at least three characters in length.
6. Type a comment or note to associate with the site (optional).
7. Click **OK**.

**Adding multiple sites to a Prohibit list**

Use this task to add more than one site to a Prohibit list simultaneously.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.
4. On the **Manage Prohibited Sites** tab, click **Add Multiple**.
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.

On a new line, repeat step 5 for each site you want to add to the Prohibit list.

Click OK.

Deleting sites from a Prohibit list
Use this task to remove sites from a Prohibit list.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. On the Manage Prohibited Sites tab, select the checkbox next to each site you want to delete from the list.
5. Click Delete.

Editing information in a Prohibit list
Use this task to change a URL, site pattern, or comment that appears on a Prohibit list.
For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. On the Manage Prohibited Sites tab, select the checkbox next to each site you want to edit, then click Edit.
5. Modify the site patterns or comments as needed.

Comments are optional. Spaces are allowed within a comment. Each URL or site pattern must appear at the beginning of a new line.

Click OK.

Searching a Prohibit list
Use this task to locate URLs or site patterns in a Prohibit list. This feature is useful for finding sites in large lists.
For option definitions, click ? in the interface.

Task
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.
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. For the policy you want to edit, click **Edit**.

4. Click the **Manage Prohibited Sites** tab.

5. 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.

6. To clear the search criteria and again display the contents of the list, click **Clear**.

### Testing a Prohibit list

When Prohibit List is implemented as a multiple-instance policy, this is useful for testing the resulting effective policy (see *How multiple-instance policies work*).

Use this task to test whether specific sites or site patterns are included in a Prohibit list.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.

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

5. Type a URL or partial URL in the **Match URL** box, then click **Go**. SiteAdvisor Enterprise displays any site patterns that match your entry. If no site patterns are displayed, the Prohibit list does not block access to the URL you entered.

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

### Customize messages for users

Use the Enforcement Messaging policy to customize messages that users see.

<table>
<thead>
<tr>
<th>Type of message</th>
<th>Location of message</th>
</tr>
</thead>
</table>
| Short message to display when users attempt to access a site rated red, yellow, or green. | • Safety balloons  
• Warn or block pages |
| Short message to display when users attempt to download files or access blocked phishing pages. | • Safety balloons  
• Warn or block pages |
| Short message to display when users attempt to access a site on the Authorize list or Prohibit list. | • Safety balloons  
• Block pages |
| Explanatory message to display when users attempt to access a site on the Prohibit list. | • Block pages |

### Creating a message for rated sites

Use this task to customize the message that is displayed when users attempt to access a site where you have associated an action with the site’s rating.

This message appears on:
• Safety balloons
• Warn or block pages

See Block and warn sites by ratings for information on using Rating Actions policy options.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click Edit.
4. Click the Site tab.
5. Select a language.
6. Type a message of up to 50 characters for these circumstances:

<table>
<thead>
<tr>
<th>This type of message...</th>
<th>Appears when users attempt to access...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn message</td>
<td>A site you have configured as Warn.</td>
</tr>
<tr>
<td>Block message</td>
<td>A site you have configured as Block.</td>
</tr>
<tr>
<td>Allow message</td>
<td>A site you have configured as Allow.</td>
</tr>
</tbody>
</table>

7. Click Save.

**Creating a message for phishing pages**

Use this task to customize the message that is displayed when users attempt to access a blocked phishing page.

This message appears on:
• Safety balloons
• Block pages

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click Edit.
4. Click the Site Resources tab.
5. Select a language.
6. Type a Block message of up to 50 characters for phishing pages.
7. Click Save.

**Creating a message for downloads**

Use this task to customize the message that is displayed when users attempt to access a download file that you have configured to block or warn users.

This message appears on:
• Safety balloons
• Warn or block pages

For option definitions, click ? in the interface.

**Task**
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. For the policy you want to edit, click Edit.
4. Click the Site Resources tab.
5. Select a language.
6. Type a message of up to 50 characters for downloads:

<table>
<thead>
<tr>
<th>This type of message...</th>
<th>Appears when users attempt to access...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn message</td>
<td>Download files that have a warning associated with their rating. You can explain why users should be cautious.</td>
</tr>
<tr>
<td>Block message</td>
<td>Blocked download files. You can explain why the file is blocked.</td>
</tr>
</tbody>
</table>
7. Click Save.

**Creating a message for sites on Authorize or Prohibit lists**
Use this task to customize the message that is displayed when users attempt to access sites you have added to an Authorize list or Prohibit list.

For option definitions, click ? in the interface.

**Task**
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. For the policy you want to edit, click Edit.
4. Click the Authorize and Prohibit Lists tab.
5. Select a language.
6. Type the text you want to display for sites on an Authorize list and sites on a Prohibit list.
7. Click Save.

**Adding a logo in a message**
Use this task to add your company logo or a custom image to the warn or block pages.

**Task**
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. For the policy you want to edit, click Edit.
Enable or disable the software
Administrators can configure two options for enabling or disabling the SiteAdvisor Enterprise client software on managed systems:
- Enable or disable the software on all systems managed by the McAfee ePO server. The default setting is to have SiteAdvisor Enterprise enabled.
- Allow users to disable and then enable the software again from the SiteAdvisor Enterprise menu in the browser or to do so only with a password. The default setting is to block disabling.

In general, McAfee does not recommend disabling the client software. However, it might be useful when performing tests or troubleshooting network connection problems. Be sure to enable the software as soon as it is practical to do so.

Tasks
- **Enabling or disabling from the ePO server on page 41**
  Use this task to enable or disable the SiteAdvisor Enterprise client software on all systems managed by the ePO server with this policy.
- **Enabling and disabling from the browser on page 42**
  Use this task to allow the SiteAdvisor Enterprise client software to be disabled on an individual managed system from the SiteAdvisor menu. When disabled, policy settings are not enforced, the site report cannot be displayed, and the SiteAdvisor menu button is gray.

Enabling or disabling from the ePO server
Use this task to enable or disable the SiteAdvisor Enterprise client software on all systems managed by the ePO server with this policy.

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.

For option definitions, click ? in the interface.

Task 1
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. For the policy you want to edit, click Edit.
4. For SiteAdvisor policy enforcement, select Enable.
5. Click Save.
6. To disable the SiteAdvisor on all managed system, deselect the option, click Save, and apply the policy.
Enabling and disabling from the browser

Use this task to allow the SiteAdvisor Enterprise client software to be disabled on an individual managed system from the SiteAdvisor menu. When disabled, policy settings are not enforced, the site report cannot be displayed, and the SiteAdvisor menu button is gray.

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.

For option definitions, click ? in the interface.

Task
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. For the policy you want to edit, click Edit.
4. For SiteAdvisor menu option, select Enable.
5. Select Only allow with password if a password is required. If you select this option, type and confirm the password.
6. Click Save. Run an agent wake-up call to apply the setting immediately, or wait for the next automatic agent-server communication.
7. From the SiteAdvisor menu in the browser, select Disable SiteAdvisor. To enable the software again, select Enable SiteAdvisor from the SiteAdvisor menu. If a password is required to perform this action, type the one specified in the policy setting.

Track events for reports

Use the Event Tracking policy to indicate which events to track for reports.

To track visits by a user to website domains either globally or locally in an intranet, select the Domains option to track visits. The option in effect turns on or off the other tracking options in the policy. The domain is the recognizable name of the Internet or local intranet network resource that a server at a particular IP address serves up. A server or single IP address can have several domains; for example,

- example.com
- www.example.com
- example.net
- www.example.org
- example.org

The URL used to reach a particular domain site and the domain’s domain name are tracked. For example, if user A goes to www.google.com to search for fishing in Alaska, and user B goes to maps.google.com to search for Vermont, the following are reported:

<table>
<thead>
<tr>
<th>Time</th>
<th>Domain</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;time&gt;</td>
<td><a href="http://www.google.com">www.google.com</a></td>
<td><a href="http://www.google.com/search(keyword?alaska%20sfishing">www.google.com/search(keyword?alaska%20sfishing</a></td>
</tr>
<tr>
<td>&lt;time&gt;</td>
<td>maps.google.com</td>
<td>maps.google.com/search/gps?vermont</td>
</tr>
</tbody>
</table>

Because the domain for both visits is the same, two visits to a single domain (google.com) are reported.

By default, visits to private domains on your local intranet are not tracked. These internal intranet sites are likely accessed often, and are thus excluded to save processing time and to avoid wasting log file space. The following IP ranges and URLs are always treated as private domains:
You have the option to force tracking of all private domains at all times, or to force tracking if the client is disconnected from the corporate network. Tracking visits to private domains can greatly increase the size of log files and the ePO server database, where this information is stored.

If you installed the Web Filtering for Endpoint extension, additional options appear in this policy. See the Web Filtering for Endpoint and Web Reporter Appendix for details.

The Authorize List policy also has a tracking option, which takes precedence over the tracking options in this policy. See Turning off tracking for visits to authorized sites for details.

### Tracking visits to domains and downloads

Information on the domains visited and the files downloaded from the domains are sent to the ePO database for queries and reports. By default, no visits to private domains are tracked.

Use this task to enable the tracking of visits to domains and domain resources such as downloads.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.
4. For **Domain and downloads**, select **Track**.
5. 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**.
6. Click **Save**.

### Tracking domain page views and downloads

Information on the domain’s pages that are visited and the files downloaded are sent to the Web Reporter database for queries and reports. By default, no visits to pages accessed on private domains are tracked.

Use this task to enable the tracking of page views accessed from a single domain. You must also indicate the location of Web Reporter, whose database stores this information.

**Before you begin**

This option is available only if you have installed the Web Filtering for Endpoint extension and Web Reporter. For details, see the Web Filtering for Endpoint extension and Web Reporter Appendix.

For option definitions, click ? in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.

4. For **Page views and downloads**, select **Track**.

5. 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**.

6. Enter Web Reporter access information if you use Web Reporter:
   a. Type the path to the location of Web Reporter.
   b. Type the password to access Web Reporter, and confirm the password.
   c. Type the number of days to store the information.

7. Click **Save**.

### Capturing user name in events

Events on the client systems can be tracked using the ePO server at every agent-sever communication interval. You can also capture the user name while tracking events on the client system.

Use this task to capture the logged-on user name in the events sent to the ePO server.

**Task**

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. For the policy you want to edit, click **Edit**.

4. Select **Capture logged-on user name in events**.

5. Click **Save**.

### Tracking green site content categories

Use this task to track content categories for all green sites. When a green site is on a Prohibit list or has a rating or content action assigned to it, it is tracked; otherwise, green sites are not tracked individually and are simply rolled up in reports. To track content categories of all green sites, use this option.

**Before you begin**

This option is available only if you have installed the Web Filtering for Endpoint extension and selected to track visits to domains. For details, see the *Web Filtering for Endpoint and Web Reporter Appendix*. For option definitions, click **?** in the interface.

**Task**

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. For the policy you want to edit, click **Edit**.

4. For **Domains and downloads**, select **Track content categories for all green sites**.

5. Click **Save**.
To monitor browser protection and security, use the ePolicy Orchestrator dashboard, monitor, and query features. SiteAdvisor Enterprise provides a number of predefined queries and monitors that create reports on the sites and download files which users access or attempt to access.

After running queries and reports over an extended period of time, it is good practice to purge the ePO database of SiteAdvisor Enterprise data to ensure proper generation of queries and reports. This occasional database maintenance is done by running an ePO purge server task.

**Contents**
- Use queries to create reports
- Use dashboards and monitors

### Use queries to create reports

Use SiteAdvisor Enterprise queries to obtain reports about browsing activity on managed systems. Choose from a variety of predefined McAfee queries, or create your own by using the ePO Query Builder. You can use a predefined query as the basis for a customized query or create a brand new query. See *Querying the Database* in the *ePolicy Orchestrator Product Guide* for more information.

Access queries by going to the **Queries** pane under **Reporting**. All predefined SiteAdvisor Enterprise queries begin with **SAE+**, followed by a descriptive name.

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

The predefined SiteAdvisor Enterprise queries are:

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Log</td>
<td>Detailed event log listing all downloads over the last 30 days.</td>
</tr>
<tr>
<td>Downloads by Action</td>
<td>Bar chart depicting the number of downloads over the last 30 days, grouped by policy-based action.</td>
</tr>
<tr>
<td>Downloads by Rating</td>
<td>Pie chart depicting the number of downloads over the last 30 days, grouped by file rating.</td>
</tr>
<tr>
<td>Functional Compliance</td>
<td>Pie chart depicting the number of managed systems where the SiteAdvisor Enterprise client software is installed and able to function correctly.</td>
</tr>
<tr>
<td>Top 100 Blocked Red Sites</td>
<td>List of 100 blocked red sites that users attempted to visit most frequently.</td>
</tr>
<tr>
<td>Top 100 Blocked Sites</td>
<td>List of 100 blocked sites that users attempted to visit most frequently.</td>
</tr>
<tr>
<td>Top 100 Red Downloads</td>
<td>List of 100 most frequently downloaded files rated red over the last 30 days.</td>
</tr>
<tr>
<td>Top 100 Red Sites</td>
<td>List of 100 red sites visited most frequently in the last 30 days.</td>
</tr>
</tbody>
</table>
### Query Name | Description
---|---
**Top 100 Red Sites on Authorize List** | List of 100 red sites included on an Authorize list that users visited most frequently over the last 30 days.

*Top 100 Sites on Authorize List* | List of 100 sites included on an Authorize list that users visited most frequently over the last 30 days.

*Top 100 Sites on Prohibit List* | List of 100 sites users attempted to visit most frequently that were blocked.

*Top 100 Unrated Downloads* | List of 100 unrated files that users downloaded most frequently over the last 30 days.

*Top 100 Unrated Sites* | List of 100 unrated sites that users visited over the last 30 days.

*Top 100 Warned-Cancelled Sites* | List of 100 most frequently visited sites over the last 30 days where users received a warning, then cancelled their visit.

*Top 100 Warned-Continued Sites* | List of 100 most frequently visited sites over the last 30 days where users received a warning, then proceeded with their visit.

*Top 100 Yellow Downloads* | List of 100 yellow files that users downloaded most frequently over the last 30 days.

*Top 100 Yellow Sites* | List of 100 yellow sites visited most frequently in the last 30 days.

*Visit Log* | Detailed event log listing all site navigation activity over the last 30 days.

*Visits by Action* | Bar chart depicting the number of visits over the last 30 days, grouped by policy-based action.

*Visits by Rating* | Pie chart depicting the number of visits over the last 30 days, grouped by site rating.

---

### Creating reports

Use this task to run a query. SiteAdvisor Enterprise is packaged with several default queries, and you can create new queries by using the ePolicy Orchestrator Query Builder.

See *Querying the Database* in the *ePolicy Orchestrator Product Guide* for information about creating new queries and editing existing queries.

For option definitions, click ? in the interface.

**Task**

1. From ePolicy Orchestrator, click **Menu** | **Reporting** | **Queries**.

2. From the Queries column, select the query to run. All SiteAdvisor Enterprise queries begin with `SAE` followed by the query name.

3. Click **Run**. The query results page shows you the details.

4. Click **Close** when finished viewing the query results.

---

### Running a purge task

Use this task to create and run an ePO purge server task to run periodic clean up of maintenance on the ePO database of SiteAdvisor Enterprise events.

For option definitions, click ? in the interface.

**Task**

1. From ePolicy Orchestrator, click **Menu** | **Automation** | **Server Tasks**.

2. Click **New Task**.
3 Name the task and click Next.

4 From the Actions list select Purge SiteAdvisor Enterprise Events, and for Purge visits older than, indicate a number of days, weeks, months, or years.

5 Click Next.

6 Schedule the task, click Next, then click Save.

Use dashboards and monitors

Use the ePolicy Orchestrator dashboard and monitor features to monitor browser activity on managed systems. For details about these features, see the ePolicy Orchestrator documentation.

Dashboards consist of monitors, and monitors are based on queries. To monitor browser activity on your network, use one or more predefined SiteAdvisor Enterprise monitors or create new monitors by using the predefined SiteAdvisor Enterprise queries or your own custom queries.

The predefined SiteAdvisor Enterprise monitors are:

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Shows results for these queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>• Top 100 Red Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Yellow Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Unrated Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Red Downloads</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Yellow Downloads</td>
</tr>
<tr>
<td>Authorize/Prohibit Lists</td>
<td>• Top 100 Green Sites on Authorize List</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Red Sites on Authorize List</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Green Sites on Prohibit List</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Red Sites on Prohibit List</td>
</tr>
<tr>
<td>Summary</td>
<td>• Top 100 Visits by Rating</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Visits by Action</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Downloads by Rating</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Downloads by Action</td>
</tr>
<tr>
<td>Warned/Blocked</td>
<td>• Top 100 Blocked Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Blocked Red Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Warned-Cancelled Sites</td>
</tr>
<tr>
<td></td>
<td>• Top 100 Warned-Continued Sites</td>
</tr>
</tbody>
</table>

Creating monitors

Use this task to create a monitor that reports browser activity on managed systems. Monitors appear in tabs on the Dashboards page.

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

1. From ePolicy Orchestrator, click **Menu | Reporting | Dashboards**.
2. Select **Options**, then **New Dashboard**.
3. In the **Name** field, type a descriptive name.
4. From the **Size** list, select a dashboard layout.
5. For each dashboard panel, click **New Monitor**.
6. For the **Category** option, select **Queries**.
7. For the **Monitor** option, select a query from the drop-down list. All SiteAdvisor Enterprise queries begin with **SAE+**.
8. Click **OK**.
9. Repeat steps 5-8 to add monitors, then click **Save**.
10. In the **Make Active** dialog box, click **Yes**. You can add only active dashboards to the Dashboard page.
11. In the **Manage Dashboards** page, click **Close**.
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 Using Dashboards, Monitors, and Reports 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 Enable/Disable 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.

**Why is the SiteAdvisor button orange?**

Several causes are possible:

- The managed system is not communicating with the Internet. Check the Internet connection.

- The managed system is not communicating with the SiteAdvisor server. A communication error icon appears instead of a question mark on the button.

- The administrator has configured options in the General policy to use the proxy settings in Internet Explorer, but no proxy settings are defined in Internet Explorer. As a result, SiteAdvisor Enterprise cannot connect to the Internet. To resolve this problem, configure your proxy settings in Internet Explorer or reconfigure the policy settings in SiteAdvisor Enterprise.

**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

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.
With the additional purchase of the Web Filtering for Endpoint extension and the 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
- Policy additions with web content filtering
- Report and dashboard additions with web content filtering
- How Web Reporter works
- Sending Web Reporter logs
- Applying the Content Actions policy
- Working with the Web Reporter

How web content filtering works

The Web Filtering for Endpoint extension provides extra filtering ability. When installed, a Content Actions policy becomes available. When this policy is applied to client systems, content classification ratings for a site are returned in addition to SiteAdvisor’s usual security ratings, and the settings in the Content Actions policy to block, warn, or allow the site based on content type are applied 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 with all content filtering options
- These options in the Event Tracking policy:
  - Track website pages viewed and files downloaded (for public or private domains)
  - Track allowed green site content categories
  - Enter Web Reporter access information

For details on applying the Content Actions policy, see Applying the Content Actions policy. For details on applying the Event Tracking options, see Track events for reports under Configuring Policies.
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 Using Dashboards, Monitors, and Reports 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:

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Sites Grouped by Content</td>
<td>Top sites grouped by content over the last 30 days.</td>
</tr>
<tr>
<td>Visits by Content</td>
<td>Pie chart depicting the number of visits over the last 30 days grouped by site content.</td>
</tr>
<tr>
<td>Visits by Action Grouped by Content</td>
<td>Bar chart depicting the number of visits to each content category over the last 30 days, grouped by policy-based actions.</td>
</tr>
</tbody>
</table>

How Web Reporter works

Web Reporter provides reports showing Web usage and trends in your organization. Used in connection with the Web Filtering for Endpoint extension, 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 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 ePO server on all managed systems.

There are three groups of people involved in the Web Reporter environment:

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

The reporting users log on to the Web Reporter server with a web-based interface to view reports. A reporting administrator uses the same Web-based interface to manage how 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.
Web Reporter environment

The Web Reporter environment comprises these areas:

- **Web Reporter** — This is the server-based software with a web-based user interface and configuration settings that create detailed reports.

- **Log sources** — These 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. 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 Web Reporter report server, an FTP Server, or NetCache.

- **Database** — The 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.

Sending Web Reporter logs

The 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 Web Reporter server, you must run an ePO server client task. Use this task to set up the client task to run on managed systems.

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

Before you begin

The client task to send 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 Web Reporter server must be in place.

For option definitions, click ? in the interface.

**Task**

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**.
Applying the Content Actions policy

Use this task to find and set the action for any site content category. You can sort by functional group, risk group, or action; or filter by a specific item. By default, all content categories are set to Allow.

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

For option definitions, click ? in the interface.

Task
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.

Working with the Web Reporter

Refer to the Web Reporter Installation and Configuration Guide and the Web Reporter Product Guide for detailed information on how to configure and use the tool to generate reports. Topics include:

- Entering license information
- Managing login accounts
- Connecting to the database
- Configuring options
- Defining directories
- Optimizing performance
- Configuring log sources
- Maintenance
- Customizing a log format
- Running reports
- Setting up email delivery
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 allow you to customize how you enforce your network traffic.

Contents

- How web gateway enforcement works
- Policy options with web gateway enforcement

How web gateway enforcement works

Web gateways can be configured to protect users from threats they encounter while searching or browsing the web and downloading files. You can configure SiteAdvisor Enterprise policies in ePolicy Orchestrator such that it can be forced to an inactive state when a web gateway is detected 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

SiteAdvisor Enterprise provides these 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 Enabling web gateway enforcement.
Index

A
about this guide 5
Authorize List
  adding sites to 31, 32
  allowing access to sites 14
  blocking activity 34
  controlling access to sites 29
  creating and managing 31
  creating messages for sites on 40
  deleting sites from 32
  editing 33
  events and SiteAdvisor 15
  list precedence 35
  multiple-instance policies 31
  searching for URLs or site patterns 33
  site patterns 29
  SiteAdvisor Enterprise policies 11
  specifying user access 35
  testing 33
  tracking feature, turning off 34

B
balloons, safety information in SiteAdvisor 8
browsing of websites
  creating a security strategy 13
  creating monitors 47
  protection for 9
  safety ratings 8
  using dashboards and monitors 47

C
client settings, SiteAdvisor Enterprise 49
communication error, SiteAdvisor Enterprise
  troubleshooting 9
configuration, SiteAdvisor Enterprise
  authorize lists 31
  block phishing pages 28
  client settings for SiteAdvisor Enterprise 49
  content actions 56
  control panel option for 23
  customizing policies 11
  disabling from browser 42
  disabling from ePO server 41
  configuration, SiteAdvisor Enterprise (continued)
    file downloads based on ratings 28
    observe mode 23
    policies for 17
    prohibit lists 35
    proxy settings for 22
    site access based on ratings 27
    track allowed green sites 44
    track domain page views 43
    track visits to domains 43
consumer version, SiteAdvisor (See SiteAdvisor Enterprise) 49
control panel option
  configuring SiteAdvisor Enterprise 23
conventions and icons used in this guide 5

D
dashboards
  monitoring browser activity 47
  SiteAdvisor Enterprise queries for 45
  SiteAdvisor Enterprise queries for web filtering 54
deployment
  SiteAdvisor Enterprise policies 17
documentation
  audience for this guide 5
  ePolicy Orchestrator 47, 50
  product-specific, finding 6
  SiteAdvisor Enterprise 50
typographical conventions and icons 5

E
enable
  web gateway enforcement 24
events, SiteAdvisor Enterprise
  information for queries 15

F
FAQs, SiteAdvisor Enterprise 49
file downloads
  blocking or warning by ratings 28
  using Authorize lists to block activity 34
forums, online for SiteAdvisor Enterprise 50
icons, safety 8
Internet Explorer
  SiteAdvisor Enterprise and 7
  supported browsers on SiteAdvisor Enterprise 7
Internet usage, tracking 15, 49
managed systems
  disabling SiteAdvisor on 42
  running SiteAdvisor Enterprise 7
  SiteAdvisor Enterprise policies 11
McAfee Default policy
  SiteAdvisor Enterprise 17
McAfee ServicePortal, accessing 6
messages, SiteAdvisor Enterprise
  customizing 38
  downloads 39
  phishing pages 39
Mozilla Firefox
  SiteAdvisor Enterprise and 7
  supported browsers on SiteAdvisor Enterprise 7
multiple-instance policies
  SiteAdvisor Enterprise 11, 31
Observe mode, SiteAdvisor Enterprise
  creating a strategy 13
  effect of policy settings 14
  enabling 23
online forums, SiteAdvisor Enterprise 50
page views, SiteAdvisor Enterprise
  creating reports with Web Reporter 54–56
phishing
  blocking page access by ratings 28
  blocking pages on authorized sites 34
  customized messages for pages 39
  scams and SiteAdvisor Enterprise 8
policies, SiteAdvisor Enterprise
  about 17
  Authorize List 29
  Content Actions 53, 54, 56
  controlling access by ratings 27
  creating and editing 20
  customizing 11
  default settings 19
  duplicates 17
  Enable/Disable 41
  Enforcement Messaging 38
  Event Tracking 42
  McAfee Default policy 17
  multiple-instance 11, 31
  Observe mode (continued)
  Rating Actions 27
  selecting options and features 14
  types of 18
  user-based 17
  web filtering extension 53
popups
  browsers and safety ratings 8
Prohibit List
  adding sites to 36
  blocking sites 14
  creating and managing 35
  creating messages for sites on 40
  deleting sites from 37
  editing 37
  events and SiteAdvisor 15
  list precedence 35
  multiple-instance policies 31
  searching for URLs or site patterns 37
  site patterns 29
  SiteAdvisor Enterprise policies 11
  specifying user access 35
  testing 38
  threat protection 29
proxy settings
  configuring SiteAdvisor Enterprise 22, 49
purge task, SiteAdvisor Enterprise
  running 46
queries, SiteAdvisor Enterprise
  creating reports 45
  creating reports for web filtering 54
  information sent for 15
reports, SiteAdvisor Enterprise
  creating 46
  creating a strategy for web-based threats 13
  data sent to ePO server 15
  data sent to SiteAdvisor website 15, 49
  purge tasks 46
  queries for 45
  queries for web filtering 54
  safety 7, 10
  viewing 11
  Web Reporter 54–56
  website safety 10
safety balloons and icons 8, 9
safety ratings
  Authorize List 27
  controlling access to sites 27
  controlling file downloads 28
  dispute resolution for site owners 49
  how website ratings are derived 8
  phishing pages, blocking 28
  SiteAdvisor Enterprise and 7
safety reports (See reports, SiteAdvisor Enterprise) 8, 10
search engines and SiteAdvisor safety icons 8
ServicePortal, finding product documentation 6
settings, SiteAdvisor Enterprise
  client settings 49
  menu buttons 9
site patterns in SiteAdvisor Enterprise
  controlling access 29
  searching Authorize lists 33
  searching Prohibit lists 37
  testing Authorize lists 33
  testing Prohibit lists 38
SiteAdvisor
  safety reports 10
  viewing site reports 11
SiteAdvisor Enterprise
  about 7
  benefits of 7
  button, gray 49
  customizing messages 38
  customizing policy settings 11
  differences with consumer version 49
  disabling 41, 42
  enabling 41
  finding more information about 50
  frequently asked questions 49
  messages for downloads 39
  monitors for browser activity 47
  resolving a rating dispute 49
  tracking Internet usage 15, 49
  troubleshooting communication error 9
website 50
SiteAdvisor menu
  description of 9
  disabled 41
  displaying options 10
support, SiteAdvisor 50
support, SiteAdvisor Enterprise
  McAfee ServicePortal website 50
support, SiteAdvisor Enterprise (continued)
  online forums 50
  website 50

T
  Technical Support, finding product information 6
threats
  browsers and safety ratings 8
  protection with Prohibit lists 29
  web-based 13
tracking feature
  allowed green sites, applying 44
  Authorize lists, turning off 34
  domains and downloads, applying 43
  page views and downloads, applying 43
  troubleshooting
    communication error 9

V
  vulnerabilities (See threats) 8

W
  web filtering, SiteAdvisor Enterprise
    additional policy options 53
    explanation 53
  website access
    controlling by safety ratings 27
    creating messages for sites 40
    file downloads, blocking on authorized sites 34
    phishing pages, blocking on authorized sites 34
    specifying users for 35
    tracking feature, turning off 34
    using ratings to block or warn 27
websites
  browsing protection 9
  McAfee ServicePortal 50
  rated, customized messages for 38
  search protection 8
  SiteAdvisor Enterprise support 50
  SiteAdvisor support 50
  testing for safety 8
  viewing SiteAdvisor site reports 11