



Symantec™ Endpoint Protection for  
Microsoft® Windows Embedded Standard  
2009 (WES) and Windows® XP Embedded  
(XPe) User Guide

HP thin clients

© Copyright 2008–2009 Hewlett-Packard  
Development Company, L.P.

Microsoft and Windows are U.S. registered  
trademarks of Microsoft Corporation.  
Internet Explorer is either a registered  
trademark or trademark of Microsoft  
Corporation in the United States and/or other  
countries.

Intel and Pentium are trademarks of Intel  
Corporation in the U.S. and other countries.

The information contained herein is subject  
to change without notice.

The only warranties for HP products and  
services are set forth in the express warranty  
statements accompanying such products  
and services. Nothing herein should be  
construed as constituting an additional  
warranty. HP shall not be liable for technical  
or editorial errors or omissions contained  
herein.

**Symantec™ Endpoint Protection for  
Microsoft® Windows Embedded  
Standard 2009 (WES) and Windows® XP  
Embedded (XPe) User Guide**

HP thin clients

Second Edition (March 2009)

First Edition (August 2008)

506030-002

## About this book

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, <http://www.symantec.com>



---

# Table of contents

## 1 System requirements

Hardware requirements .....	1
Software requirements .....	1

## 2 Introducing the agent

About the Symantec Endpoint Protection for WES and XPe .....	2
About security policies .....	2
Key features of the agent .....	3

## 3 Agent basics

Opening the agent .....	4
Navigating the main window .....	4
Using the menus and the toolbar .....	5
Viewing traffic history .....	6
Displaying broadcast traffic .....	6
Viewing currently running applications and services .....	6
Displaying or hiding the message area .....	7
Viewing current security policy and communication status .....	7
About the notification area icon .....	8
About responding to the flashing icon .....	8
Displaying the shortcut menu .....	8
Disabling protection temporarily .....	9
Changing security levels .....	9
Enabling password protection .....	9
Testing your endpoint .....	10

## 4 Responding to messages and warnings

About message types .....	11
Application messages .....	11
Changed application messages .....	12
Responding to application messages .....	12
Responding to Trojan horse warnings .....	13
Responding to blocked traffic messages .....	14

Responding to permission status messages .....	14
<b>5 Monitoring and logging</b>	
About logs .....	15
About the Security log .....	16
About the Traffic log .....	17
About the Packet log .....	18
About the System log .....	19
Viewing logs .....	19
Back tracing logged events .....	20
Exporting logs .....	21
Filtering logged events .....	21
Stopping an active response .....	22
<b>6 Command Line Management</b>	
The command-line interface for the client service .....	23
Typing a parameter if the agent is password-protected .....	24
<b>Index .....</b>	<b>26</b>

---

# 1 System requirements

This chapter includes the following topics:

- [Hardware requirements on page 1](#)
- [Software requirements on page 1](#)

## Hardware requirements

The agent requires the following minimum hardware:

- Intel® Pentium® 133 MHz or equivalent
- 256 MB RAM
- 40 MB available hard disk space
- One Ethernet adapter (with TCP/IP installed)

## Software requirements

The agent requires the following software:

- Windows Embedded Standard 2009 (WES) operating system or
- Windows XP Embedded (XPe) operating system or
- Windows Embedded Point of Service operating system
- Windows Internet Explorer® 6.0
- TCP/IP Networking
- COM Base
- IP Security Services
- NDIS & NDSI User-mode I/O Driver
- OLE Dialog Interfaces
- User Interface Core

---

## 2 Introducing the agent

This chapter includes the following topics:

- [About the Symantec Endpoint Protection for WES and XPe on page 2](#)
- [About security policies on page 2](#)
- [Key features of the agent on page 3](#)

### About the Symantec Endpoint Protection for WES and XPe

The Symantec Endpoint Protection for WES and XPe (the agent) is security software that is installed on embedded endpoints, such as ATMs, Point of Service systems, and thin clients, that run the WES, XPe, or the XPe Point of Service operating system.

The agent provides a customizable firewall that protects the endpoint from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojan horses, port scans, and other common attacks. In response, it selectively allows or blocks traffic, or various networking services, applications, ports, and components.

### About security policies

The agent uses security policies, which include firewall rules, and security settings. These policies protect an individual endpoint from network traffic and the viruses that can cause harm. Firewall rules determine whether your endpoint allows or blocks an incoming or outgoing application or service from gaining access through your network connection. Firewall rules allow the agent to systematically allow or block incoming or outgoing applications and traffic from or to specific IP addresses and ports. Security settings detect and identify common attacks, send e-mail messages after an attack, display customizable messages, and accomplish other related security tasks. The configuration of firewall rules with other security and antivirus settings results in a security agent that protects your endpoint.



## Key features of the agent

The agent can be used in the following networking environments:

- Directly connected to the local area network or wireless network
- Remotely connected using Virtual Private Network (VPN) or dial-up
- Completely disconnected from any network

The agent does not support location awareness or host integrity. Host integrity will be supported in a later release.

---

## 3 Agent basics

This chapter includes the following topics:

- [Opening the agent on page 4](#)
- [Navigating the main window on page 4](#)
- [Using the menus and the toolbar on page 5](#)
- [About the notification area icon on page 8](#)
- [Testing your endpoint on page 10](#)

### Opening the agent

The agent is designed to start automatically when you turn on your endpoint, protecting you immediately. To configure your agent or review logs of potential attacks on your agent, you open the agent first.

To open the agent

1. On the Windows taskbar, click **Start > Programs**.
2. Click **Symantec > Symantec Endpoint Protection for Windows XP Embedded agent**.

### Navigating the main window

Once you open the agent, you see the main screen. The main screen provides real-time network traffic updates, online status, links to logs, and access to various advanced rules, security settings, and antivirus settings.

The user interface changes depending on the different control modes of the agent, including user mode, admin mode, or mixed mode. In addition, some icons may not appear, depending on how your system administrator configured the agent.

The agent is resizable, so you can view it as a full-screen or part-screen image.

## Using the menus and the toolbar

The top of the screen displays a standard menu and toolbar. The toolbar icons can be used to quickly access logs, view the Help file, or test your system.

Some icons are either disabled or may not appear. This status depends on how the agent is configured or which control mode the agent is in.

The toolbar icons that are located below the menus provide shortcuts. These shortcuts can be used to do the following:

- Block all applications
- Change your security policy
- Access the logs
- Test the agent's effectiveness
- View the Help file

The File menu commands include Exit Symantec Endpoint Protection agent, which exits the agent and turns off security on your endpoint.

The Location menu displays the default Office location.

The Tools menu commands include the following:

<b>Applications</b>	<b>Opens the Applications List</b>
Options	Opens the Options dialog box, which contains many security options, including e-mail alerts, Network Neighborhood browsing rights, 802.1x authentication, AV/IPS signature update, and log file configurations.  This option appears in Power User mode only.
Advanced Rules	Opens the Advanced Rules dialog box, where you can set up firewall rules
Logs	Opens the logs
Automatically Start Service	Not enabled for the agent
Test Your System Security	Opens a Web site so that you can scan and test the effectiveness of the agent

The View menu gives users the option to change the display of software programs in the Running Applications field. The View menu commands include the following:

Large Icons	Displays 32x32 icons in the field. Each icon represents a software application or a system service
Small Icons	Displays 16x16 icons. Both the large and small icon displays provide the full name of the application
List	Provides small icon representations, with the icons displayed in a standard list
Applications Details	Provides a list of all running applications and their version numbers and paths
Connection Details	Provides further information on the type of connection that each application makes when accessing the network adapter and other details

Hide Windows Services	Toggles the display of Windows Services
Hide Broadcast Traffic	Toggles the display of broadcast traffic

## Viewing traffic history

You can view a real-time picture of the last two minutes of your traffic history in the main window. The graphs reload new information every second, providing instant data, as measured in bytes, about your incoming and outgoing network traffic.

The Traffic History graphs are broken down into three sections. The Incoming and Outgoing Traffic History graphs are on the left side of the graphs section. These provide a visual assessment of the current traffic that enters and leaves your endpoint through a network interface. This traffic includes the traffic that is allowed and the traffic that is blocked. The green lines and bars indicate the traffic that is allowed to pass through. The red coloring indicates the traffic that the agent has blocked traffic.

The Attack History graph on the right side of the screen provides information on attempted attacks against your computer.

## Displaying broadcast traffic

Broadcast traffic is the network traffic that is sent to every endpoint in a particular subnet. It is not directed specifically to your endpoint. If you do not want to see this traffic, you can remove it from this graphical view by checking Hide Broadcast Traffic. You then only see unicast traffic in this graph, which is the traffic that is directed specifically to your endpoint. To redisplay broadcast traffic, uncheck Hide Broadcast Traffic.

## Viewing currently running applications and services

The Running Applications field provides a list of all applications and system services that currently run on your system.

Permission status refers to the permissions that you allow an application. It shows whether it:

- Can access your Internet connection or network
- Is blocked from accessing the Internet or network altogether
- Asks your permission before it accesses that connection

You can change the status of applications from the Running Applications field by right-clicking an application's icon and selecting the desired status.

[Table 3-1 Running Applications field on page 6](#) displays how each application icon appears, depending on the permission status.

**Table 3-1 Running Applications field**

Status	Description
Allow	Icon appears normal, with no marks. The icon displays a small blue dot on the lower left corner if it receives traffic. It displays a small blue dot on the lower right corner if it sends traffic.
Ask	Icon appears with a small, yellow question mark.
Block	Icon appears with a red circle and cross-out mark.

There are a number of services running at any given time. Since they are often crucial to the operation of your endpoint, you may want to allow them. You can show or hide them from the message console.

To hide system services

- ▲ Click **Hide Windows Services**.

To change the display of applications

- ▲ Right-click the **Running Applications** field and select the desired view.

To stop an application or service from running

- ▲ In the **Running Applications** field, right-click the application and click **Terminate**.

## Displaying or hiding the message area

The message area is located at the bottom of the main screen. It provides a real-time update of the server-agent communication status. This update includes when the latest security policy is downloaded and the number of the policy serial numbers.

The message area is hidden by default.

To show or hide the message area

1. Below the **Running Applications** field, click **Show Message Console**. The message area appears.
2. To hide the message area from view, click **Hide Message Console**. The message area collapses and displays the **Show Message Console** icon.

## Viewing current security policy and communication status

This section explains how to view current security policy and communication status.

To view the current policy information

- ▲ On the bottom of the main screen, look for the status bar.

You can view a real-time update of the agent's communication with the server. If green, the light indicates that the agent is online and communicating with the management server. If gray, the agent is not connected to the management server.

To view the communication status

- ▲ In the right-hand corner of the status bar, look for the status icon.

## About the notification area icon

RED	The agent has blocked traffic.
GREEN	Traffic flows uninterrupted by the agent.
GRAY	No traffic flows in that direction. A green dot means that the agent is connected to the Symantec Policy Manager.

## About responding to the flashing icon

If you see a flashing icon, the endpoint may be responding to an attempted attack. When you rest your mouse over the flashing icon, a tool tip appears telling you that you are under an attack.

To make the icon stop flashing, double-click the icon. The Security log opens, displaying a new log entry. The icon stops flashing after one minute.

## Displaying the shortcut menu

The agent has a notification area icon that is located in the lower-right corner of your desktop. Right-click this icon to show frequently used commands.

[Table 3-2 Notification area icon shortcut menu on page 8](#) displays the following notification area icon shortcut menu and commands for the Server Control mode and Client Control mode. Commands on the shortcut menu for the Power User mode vary depending on what options are set on the server.

**Table 3-2 Notification area icon shortcut menu**

Menu command	Description	Server Control mode	Client Control mode
Symantec Protection Agent	Opens the agent's main screen	X	X
Normal	Allows network traffic to flow as normal		X
Block All	Blocks all network traffic		X
Applications	Opens the Applications list	X	X
Logs	Opens the agent logs	X	X
Options	Opens the Options dialog box, where you can configure the settings for the agent		X
Advanced Rules	Opens the Advanced Rules dialog box, where you can write specific rules for allowing or blocking network access		X
Help Topics	Opens the online Help system	X	X

**Table 3-2 Notification area icon shortcut menu (continued)**

Menu command	Description	Server Control mode	Client Control mode
About	Opens the About dialog box, providing information on your version of the agent	X	X
Exit Symantec Protection Agent	Stops the agent from running. You need to restart the agent to protect your system	X	X

**NOTE:** This option may appear dimmed or not at all.

## Disabling protection temporarily

You may need to disable security on the agent so that the agent does not block outbound traffic. You disable security from the management server. You cannot do it from the agent. If you must disable security from the agent, exit the agent.

To temporarily disable blocking

- ▲ Exit the agent.

## Changing security levels

The agent supports two security levels: Normal and Block All.

To change your security level

1. Click **Security**.
2. Click **Block All** or **Normal**.

## Enabling password protection

You can set your agent to require a password before you make any security changes or before you exit the agent.

To enable password protection

1. Click the **Tools > Options > General** tab.
2. Click **Set Password**.
3. In the **Password** dialog box, type your new password in the **New Password** and **Confirm New Password** fields. You can disable password protection by leaving both fields blank.
4. Click **OK**.
5. To have the agent prompt you for a password before you exit the agent, on the **General** tab, click **Ask password while exiting**.

# Testing your endpoint

You can test the vulnerability of your system to outside threats by scanning your system. Assessing your vulnerability to an attack is one of the most important steps that you can take. With what you learn from the tests, you can more effectively set the various options on your agent to protect your endpoint from attack.

To test your endpoint

1. Do one of the following:

- On the toolbar, click **Security Test**.
- On the **Tools** menu, click **Test Your System Security**.

The Symantec Security Check scans your endpoint and tries to determine your IP address, operating system, Web browser, and other information about your system.

2. Choose one of the following scans:

- Security Scan
- Virus Detection

3. Click **Start**.



---

# 4 Responding to messages and warnings

This chapter includes the following topics:

- [About message types on page 11](#)
- [Responding to application messages on page 12](#)
- [Responding to Trojan horse warnings on page 13](#)
- [Responding to blocked traffic messages on page 14](#)
- [Responding to permission status messages on page 14](#)

## About message types

You may see several different types of messages on the endpoint. These messages usually describe a situation and indicate how the agent tries to resolve the issue.

You may see the following types of messages:

- Application messages
- Changed application messages
- Fast user switch messages

## Application messages

An application-related message occurs for one of the following reasons:

- An application that the agent has never seen before, or that has been assigned the status of Ask, tries to access your network connection.
- An application that normally accesses your network connection has changed, possibly because of a product upgrade.
- Your agent software is being updated.
- Your agent has detected a Trojan horse on your endpoint.

For example, you may see the following type of message when an application or service tries to access your endpoint, the port, and other information.

Internet Explorer (IEXPLORE.EXE) is trying to connect to www.symantec.com using remote port 80 (HTTP - World Wide Web). Do you want to allow this program to access the network?

This message appears because the application has been opened, either directly or indirectly by you, or by another application.

If you didn't open any program or click any link and an application tries to access your network connection, there may be a number of different reasons. However, if you cannot see any reason that application should try to access your network connection, it is always safest to click **No**. This message might indicate the presence of a Trojan horse on your endpoint, something that needs to be checked immediately.

## Changed application messages

Occasionally, you might see a message that indicates an application has changed.

- Telnet Program has changed since the last time you opened it, this could be because you have updated it recently. Do you want to allow it to access the network?

The application that is listed on the message is trying to access your network connection. Although the agent recognizes the name of the application, something about the application has changed since the last time the agent encountered it.

This change could be because you have upgraded the product recently. The agent uses an MD5 checksum to determine the legitimacy of an application. An upgraded version might not pass the checksum test because it may have a different checksum value.

If you have not recently upgraded the application, your network may be under attack by a Trojan horse.

## Responding to application messages

You can change the status of the application at any time, either in the Running Applications field or in the Applications List.

To respond to application messages

1. Click **Detail** to view more information about the application, including the file name, version number, and path name. The Detail section also displays whether the application tries to connect locally to your endpoint or remotely to an outside destination. It shows the local and remote port numbers and IP addresses.
2. If you want the agent to remember your choice for the next time this application tries to access your network connection, click **Remember my answer, and do not ask me again for this application**.
3. Do one of the following actions: Depending on whether you select or don't select the **Remember my answer, and do not ask me again for this application** option and click the **Yes** or **No** icons, the application is assigned the following permission statuses.
  - To allow the application to access the network connection, click **Yes**.
  - To block the application from accessing the network connection, click **No**.

## Responding to Trojan horse warnings

If the agent detects a known Trojan horse on your endpoint, it blocks the Trojan horse from accessing your system and displays a message such as the following:

- "C:\WINNT\System32\UMGR32.EXE, a Trojan horse application has been detected on your computer. It has been blocked by the Symantec Protection Agent."

This message means that a Trojan horse is present on your system and has been activated. Either you tried to open the program that was identified as a Trojan horse, or it has been triggered by another program on your endpoint. It is possible that the Trojan horse was on your endpoint when you installed the agent. It is also possible that you have recently downloaded it through a legitimate application, such as a Web browser. The Trojan horse tried to access your network connection, and has been blocked by the agent.

To respond to a Trojan horse warning

1. Click **OK**.
2. Immediately notify your IT department. The agent blocks the Trojan horse from sending any information out of or into your endpoint. However, it is still important to remove it from your system as soon as possible. The agent terminates the Trojan horse process automatically, but removal requires the assistance of your IT department.

## Responding to blocked traffic messages

Security messages display a message box when applications are blocked:

---

Blocked application message

An application that has been launched from your computer has been blocked in accordance with rules set by your system administrator. For example, you may see the following text:

```
Application Internet Explorer has been
blocked, file name is IEXPLORE.EXE.
```

These messages indicate that your agent has blocked traffic that you have specified as not trusted. If the agent is operating under Block All mode, these messages appear quite often. If you are operating in Allow All mode, these messages do not appear.

---

If you or the system administrator configures the agent to display a message when either the agent blocks the endpoint from accessing an application or when an attack is launched, a message appears above the notification area.

To respond to security messages

- ▲ In the message box, click **Do not show this window again**.

## Responding to permission status messages

If you or your system administrator have set an applications' permission status to Ask or Block, a message appears when an incoming application accesses your endpoint.

[Table 4-1 Application permission status messages on page 14](#) displays how you can respond to an application or permission status message.

**Table 4-1 Application permission status messages**

If you check Remember my answer box?	If you click	Your agent
Yes	Yes	Allows the application and won't ask again.
No	Yes	Allows the application and ask you every time.
Yes	No	Blocks the application and ask you every time.
No	No	Blocks the application and won't ask you again.

---

You can change an application's permission status from the Applications List.

---

# 5 Monitoring and logging

This chapter includes the following topics:

- [About logs on page 15](#)
- [Viewing logs on page 19](#)
- [Back tracing logged events on page 20](#)
- [Exporting logs on page 21](#)
- [Filtering logged events on page 21](#)
- [Stopping an active response on page 22](#)

## About logs

The agent's logs are an important method for tracking your endpoint's activity and its interaction with other endpoints and networks. The logs record information about the agent's status and about the traffic that tries to enter or exit your endpoint through your network connection.

The agent's logs perform the following tasks:

- Record information about the agent's status and about the traffic that tries to enter or exit your endpoint through your network connection.
- Track your endpoint's activity and interaction with other endpoints and networks.
- Detect potentially threatening activity, such as port scanning.
- Help you troubleshoot connectivity problems or possible network attacks.
- Record the results of the management policies that are applied to your endpoint.

The agent includes the following types of logs:

---

Security	Records potentially threatening activity that is directed towards your endpoint, denial-of-service attacks, port scans, executable file alterations, and Trojan horse attacks.
Traffic	Records every connection your endpoint makes through the network.
Packet	Captures every packet of data that enters or leaves a port on your endpoint.
System	Records all operational changes for the agent, such as starting and stopping services, detecting network applications, and configuring software.

---

## About the Security log

The Security log records potentially threatening activity that is directed towards your endpoint, such as port scanning, virus attacks, or denial-of-service attacks. The Security log is probably the most important log in the agent.

The Security log records attacks in the following categories:



Critical attack



Major attack



Minor attack



Information

---

The Security log records the following information about each activity:






Time	The exact date and time that the event was logged
Security Type	Type of security alert, such as a DoS attack, executable file, Ping of Death, or virus attack
Severity	The severity of the attack (either Critical, Major, Minor, or Information)
Direction	Direction that the traffic was traveling in (incoming, outgoing, or unknown)—Most attacks are incoming, that is, they originate in another endpoint. Other attacks, like Trojan horses, are programs that have been downloaded to your endpoint and therefore are already present; they are considered outgoing. Still other attacks are unknown in direction; they include Active Response or application executable changed.
Protocol	Type of protocol—UDP, TCP, and ICMP
Remote Host	IP address of the remote endpoint (only appears in Local View - this is the default)
Remote MAC	MAC address of the remote endpoint. If outside the subnet, it is the MAC address of the router. (only appears in Local View - this is the default)
Local Host	IP address of the local endpoint (only appears in Local View - this is the default)
Local MAC	MAC address of the local endpoint (only appears in Local View - this is the default)
Application Name	Name of the application associated with the attack
User Name	User or endpoint that sent or received the traffic
Domain	Domain of the user
Occurrences	Number of occurrences of the attack method
Begin Time	Time the attack began
End Time	Time the attack ended

## About the Traffic log

Whenever your endpoint makes a connection through the network, this transaction is recorded in the Traffic log. The Traffic log includes information about incoming and outgoing traffic.

The Traffic log categorize different types of traffic as:

---

	Incoming traffic; passed through the agent
	Incoming traffic; blocked by the agent
	Outgoing traffic; passed through the agent
	Outgoing traffic; blocked by the agent
	Traffic direction unknown; passed through the agent
	Traffic direction unknown; blocked by the agent

---

The Traffic log records the following information about each activity:

---

Time	The exact date and time that the event was logged
Severity	The severity of the traffic
Direction	Direction that the traffic travels (incoming or outgoing)
Protocol	Type of protocol - UDP, TCP, and ICMP
Remote Host	IP address of the remote endpoint (only appears in Local View - this is the default)
Remote MAC	MAC address of the remote endpoint. If outside the subnet, it is the MAC address of the router. (only appears in Local View - this is the default)
Remote Port	Port on the remote endpoint (only appears in Local View - this is the default)
Local Host	IP address of the local endpoint (only appears in Local View - this is the default)
Local MAC	MAC address of the local endpoint (only appears in Local View - this is the default)
Local Port	Port used on the endpoint (only appears in Local View - this is the default)
Application Name	Name of the application that is associated with the attack
User	User's log on name

---

Domain	User's domain name
Location	The Location (Normal or Block All) that was in effect at the time of the attack
Occurrences	Number of packets each piece of traffic sends between the beginning and ending time
Begin Time	Time traffic starts matching the rule
End Time	Time traffic stops matching the rule
Rule Name	The rule that determined the passing or blockage of this traffic

## About the Packet log

The Packet log captures every packet of data that enters or leaves a port on your endpoint. The Packet log is disabled by default in the agent because of its potentially large size. You must enable the Packet log before you can use it.

The Packet log uses the following icons to categorize data packets:



Full data packet captured

The Packet log records the following information about each data packet:

Time	The exact date and time that the packet was logged
Remote Host	Name of the remote endpoint (only appears in Local View - this is the default)
Remote Port	Port on the remote host that sent/received the traffic (only appears in Local View - this is the default)
Local Host	IP Address of the local endpoint (only appears in Local View - this is the default)
Local Port	Port used on the endpoint for this packet (only appears in Local View - this is the default)
Source Host	Name of the source endpoint (only appears in Source View)
Source Port	Port on the source host that sent/received the traffic (only appears in Source View)
Destination Host	IP Address of the destination endpoint (only appears in Source View)
Destination Port	Port used on the destination endpoint for this packet (only appears in Source View)
Direction	Direction that the traffic was traveling in (incoming or outgoing)
Action	Action taken by the agent: Blocked or Allowed
Application Name	Name of the application that is associated with the packet

Below the Log Viewer are two additional data fields that provide further detail regarding the selected event. The left field provides data on the type of packet logged. The right field displays the actual data packet.



## About the System log

The System log records all operational changes, such as the starting and stopping of services, detection of network applications, software configuration modifications, and software execution errors. It also logs communication with the Symantec Policy Manager, including connection and downloads. All information that is provided in the System log also appears in real time in the message area. The System log is especially useful for troubleshooting the agent.

The System log records the following information about each system error:

Time	The date and time that the event was logged
Type	Type of event can be an error, warning, or information regarding the Symantec Policy Manager. An error indicates a problem with the source; a warning indicates a potential problem; and an information point provides information about an event involving the agent.
ID	ID assigned to the event by the agent
Summary	Description of the event

## Viewing logs

The following procedure explains how to view logs.

To view logs

1. Do one of the following:
  - Click **Tools > Logs**.
  - On the toolbar, click the drop-down arrow next to the **Logs** icon.
2. Click one of the log types. Each log opens the **Log Viewer** dialog box. The **Log Viewer** is a table where each row represents a logged event and each column displays information regarding the event.
3. In the **Log Viewer** dialog box, click the **View** menu and then click either **Local View** or **Source View**. The fields in the log change depending on whether you choose the local view or source view.
4. To view a description of each event, select an event row
5. Click **Refresh**, or press **F5** to update the log that you are viewing.
6. Click **File > Exit**.

## Back tracing logged events

Back tracing enables you to pinpoint the source of data from a logged event. Back tracing shows the exact steps, or hops, that incoming traffic has made before reaching your endpoint. A hop is a transition point, usually a router, which a packet of information travels through on a public network. Back tracing follows a data packet backwards; discovering which routers the data took to reach your endpoint.

[Figure 5-1 Back tracing a packet on page 20](#) shows how the agent back traces a packet.

**Figure 5-1** Back tracing a packet



For each log entry, you can trace a data packet that was used in an attack attempt. Each router that a data packet passes through has an IP address. You can view the IP address and other details. The information that appears does not guarantee that you have discovered who the hacker is. The final hop's IP address lists the owner of the router that the hackers connected through, and not necessarily the hackers themselves.

You can back trace a logged event in the Security, Traffic, and System logs

To back trace a logged event

1. Open the log file and click an event so that the entire row is selected.  
The agent begins back tracing the event.
2. Do one of the following:
  - Right-click and click **BackTrace**.
  - Click **Action > BackTrace**.
3. In the **Back Trace Information** dialog box, click **Whois** to view detailed information on each hop. A drop panel displays detailed information about the owner of the IP address from which the traffic event originated. You can cut and paste the information in the Detail information panel. Press **Ctrl +C** to copy the information into the **Clipboard**. Then press (**Ctrl+V**) to paste it into an e-mail message to your system administrator.
4. Click **Whois** again to hide the information.
5. Click **OK**.
6. Click **OK**.

## Exporting logs

You can save and export the contents of the logs to different locations. You may want to export logs to save space or to perform a security review.

To export a log file

1. Open the log in the **Log Viewer**.
2. Click **File > Export**.
3. In the **Save As** dialog box, select the location and format type for the log file.
4. Click **OK**.

## Filtering logged events

You can view the recorded events in the Log Viewer by the severity level of the attack and by a previous period of time.

To filter log events by severity

1. In the Log Viewer dialog box, click the **Filter** menu.
2. Click **File > Export > Severity**.
3. Click **Severity**.
4. In the **Save As** dialog box, select the location and format type for the log file.

You can view more than one type of event at one time. The **Log Viewer** is automatically reloaded.

5. Click the severity level(s) so that a check mark appears to the left of the severity level name. You have the following options:
  - **Critical** (Security log only)
  - **Major**
  - **Minor**
  - **Error** (System log only)
  - **Warning** (System log only)
  - **Information**

To filter log events by time period

1. In the **Log Viewer** dialog box, click the **Filter** menu.
2. Select the time period for which you want to view log events. For example, 2 Week Logs displays the events that were recorded over the past 14 days.

## Stopping an active response

If the agent detects an attack, it triggers an active response. The active response automatically blocks the IP address of a known intruder for a specific amount of time (from 1 to 2,147,483,647 seconds). The default amount of time is 10 minutes. If you don't want to wait the default amount of time to unblock the IP address, you can stop the active response immediately.

An active response can also be triggered by IPS signatures that are updated weekly and by denial of service signatures that can be updated with new builds, port scans, and MAC spoofing. However, a Trojan horse is not considered an attack because it is a program that runs on the same endpoint where it was detected. It is considered a security alert rather than an attack.

You can stop active responses in the Security log only.

To stop an active response

1. Click **Tools > Logs > Security**.
2. Select the row for the application or service you want to unblock. Blocked traffic is specified as **Blocked** in the **Action** column.
3. On the **Action** menu, click **Stop Active Response** to block the selected application, or click **Stop All Active Response** if you want to unblock all blocked traffic.
4. When the **Active Response** dialog box appears, click **OK**.

---

# 6 Command Line Management

This chapter includes the following topics:

- The command-line interface for the client service
- Typing a parameter if the agent is password-protected

## The command-line interface for the client service

You can manipulate the agent directly from the command line on the agent computer by using the `smc` command for the client service. You may want to use this command in a script that runs the parameters remotely. For example, if you need to stop the agent to install an application on multiple agents, you can stop and restart each client service.

With the exception of `smc -start`, the client service must run to use the command-line parameters. The command-line parameters are not case sensitive.

**Table 6-1 Parameters that administrators can use**

Parameter	Description
<code>smc -importadvrule</code>	<p>Replaces the imported firewall rules to the agent's list of existing firewall rules.</p> <p>These rules overwrite the existing rules. The client service must run to import the profile file's contents.</p> <p>To import firewall rules, you import a <code>.sar</code> file. For example, you can type the following command:</p> <p>To import firewall rules, you import a <code>.sar</code> file. For example, you can type the following command:</p> <pre>smc -importadvrule C:\config\AllowExplorerRule.sar</pre> <p>An entry is added to the System log after you import the rules.</p>
<code>smc -appendadvrule</code>	<p>Adds the imported rules to the bottom of an existing advanced rules list. This command does not overwrite existing Advanced rules.</p> <p>To append firewall rules, you import a <code>.sar</code> file. For example, you can type the following command:</p> <pre>smc -appendadvrule C:\config\AllowExplorerRule.sar</pre> <p>An entry is added to the System log after you append the rules.</p>

**Table 6-1 Parameters that administrators can use (continued)**

Parameter	Description
smc -exportadvrule	<p>Exports the agent's firewall rules to a .sar file.</p> <p>Agent rules are only exported from the agent when in Server Control mode.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -exportadvrule C:\config\AllowExplorerRule.sar</pre>
smc -importallconfig	<p>Imports the server and client profiles to the agent. The source folder must contain both serdef.xml and cltdef.xml.</p> <p>This command replaces the current profile file's contents. Therefore, you can deploy the most current profile file without having to remove out-of-date firewall rules, antivirus scans, security settings, and user interface settings.</p> <p>You must specify the path name and file name and extension. Any name or extension is acceptable. For example, you can type the following command:</p> <pre>smc -importallconfig C:\profile\source_folder\OfficeRules.xml</pre>
smc -exportallconfig	<p>Exports the server and client profiles to file and folder of your choice.</p> <p>Exports the server and client profiles to file and folder of your choice.</p> <p>You must specify the path name and file name and extension. Any name or extension is acceptable. For example, you can type the following command:</p> <pre>C:\profile\dest_folder\OfficeRules.xml</pre>
smc -start	Starts the client service.
smc -stop	Stops the client service.


When you import profile files and firewall rules, note that the following rules apply:

- You cannot import profile files or firewall rule files directly from a mapped network drive.
- The agent does not support UNC (universal naming convention) paths.

## Typing a parameter if the agent is password-protected

You can password-protect the agent computer for the following parameters:

-stop	The agent asks for a password before you or the user stops the agent.
-importconfig	The agent asks for a password before you can import the profile file.
-exportconfig	The agent asks for a password before you can export the profile file.

 **NOTE:** The password is limited to 15 characters or less.

To type a parameter if the agent is password-protected, perform the following steps:

1. On the agent computer, on the taskbar, click **Start > Run**.
2. In the Run dialog box, type `cmd`.
3. In the Windows MS-DOS prompt, type either one of the following:

```
smc -parameter -p password
```

```
smc -p password -parameter
```

Where:

parameter is `-stop`, `-importconfig`, or `-exportconfig`.

password is the password you specified in the console.

For example, you can type either:

```
smc -exportallconfig c:\profile.xml -p password or
```

```
smc -p password -exportallconfig c:\profile.xml
```

4. Close the command prompt.

---

# Index

- A**
  - active response, stopping 15
  - agent
    - about 2
    - basics 4
    - commands 23
    - features 2
    - opening 4
    - password-protected 24
  - application messages 11
  - application messages, changed 12
  - applications, viewing running 6
- B**
  - back tracing logged events 15
  - broadcast traffic 6
- C**
  - changed application messages 12
  - changing security levels 9
  - client service, command-line interface for 23
  - CMD 23
  - command line management 23
  - command-line interface 23
  - communication status, viewing 7
- D**
  - disabling protection 9
- E**
  - endpoint, testing 4
  - events, filtering logged 15
- F**
  - File menu 5
  - filtering logged events 15
  - flashing icon 8
- H**
  - hardware requirements 1
  - history, traffic 6
- I**
  - icon
    - flashing 8
    - notification area 4
- L**
  - Location menu 5
  - log
    - Packet 18
    - Security 16
    - System 19
    - Traffic 17
  - logged events
    - back tracing 15
    - filtering 15
  - logging 15
  - logs
    - about 15
    - exporting 15
    - viewing 15
- M**
  - menu
    - File 5
    - Location 5
    - shortcut 8
    - Tools 5
    - View 5
  - menus, using 4
  - message area
    - displaying 7
    - hiding 7
  - messages
    - application 11
    - blocked traffic 11
    - changed application 12
    - permission status 11
    - responding to 11
    - responding to application 11
    - types 11
  - monitoring 15
- N**
  - navigating main window 4
  - notification area icon 4
- O**
  - opening agent 4
- P**
  - Packet log, about 18
  - parameter, typing 24
  - password protection 9
  - password-protected agent 24
  - policies, security 2
  - protection, disabling 9
- R**
  - requirements
    - hardware 1
    - software 1
    - system 1
  - responding to
    - application messages 11
    - blocked traffic messages 11
    - flashing icon 8
    - messages 11
    - permission status messages 11
    - Trojan horse warnings 11
    - warnings 11
  - response, stopping active 15
- S**
  - security
    - changing levels 9



- disabling protection 9
- enabling password protection 9
- policies 2
- viewing policy 7
- Security log, about 16
- shortcut menu 8
- software requirements 1
- stopping active response 15
- System log, about 19
- system requirements 1

## T

- testing endpoint 4
- toolbar, using 4
- Tools menu 5
- traffic
  - blocked messages 11
  - broadcast 6
  - history 6
- Traffic log, about 17
- Trojan horse warnings 11
- typing parameter 24

## V

- View menu 5
- viewing
  - communication status 7
  - logs 15
  - running applications 6
  - security policy 7

## W

- warnings, responding to 11