Malware threats

The information in this document is only relevant if you have purchased the appropriate licenses to run malware checks in Security Manager. Contact your ManageSoft Corporation consultant for general advice on configuring your installation to perform malware checks.

Malware — a definition

The word *malware* is short for *malicious software*. Malware programs are those that, once installed, damage a computer or disrupt its operation. Common examples of malware programs are viruses and trojan horses.

Computers can be infected by malware programs in several ways: malware programs may be bundled with software such as file-sharing programs, or may be installed automatically when users visit some websites.

Regular identification of malware threats, and remedial action against malware infections, are of paramount importance in protecting your enterprise's computer assets.

This document provides instructions about monitoring and managing malware threats to your enterprise. This information applies only to managed devices running Windows.

In this document, you will:

- Learn what data is available about malware threats
- Read how to report on malware threats to your enterprise
- Understand how to report on malware infections on your managed devices
- Find out how to work with the details of malware threats.

About malware threats

Malware programs are malicious software that damage or disrupt the operation of computers. Regular identification and analysis of the threats posed by malware programs, and remedial action to fix any computers on which malware programs have been installed, form part of the task of protecting your organization's computers and data.

The `malwareupdate.cab` file contains the latest definitions of malware variants that Security Manager is able to detect, quarantine, and remove. This file is updated whenever new malware variants are added. When you refresh the list of available malware threats, the latest `malwareupdate.cab` file is downloaded from the ManageSoft Corporation website.

Security Manager helps automate the processes of regular scanning for, and removal of, malware programs. Using it, you can:

- View reports about your enterprise's exposure to each malware threat
- Specify the malware threats that you want to monitor
- Automatically clean managed devices infected by malware programs.

You perform these actions from the **Malware Threats** node, which is described more fully later.

Rolling out malware threat definitions

If you want to use Security Manager to monitor and manage malware threats, you need to roll out the package containing malware threat definitions. To do this:

1 Open the ManageSoft administration server, and browse to the **Software Library** node.

2 The **Malware definitions** package is located under **Software Library > Malware**.

3 Use the deployment policy editor to add the package to the **Enterprise** Group Policy Object to ensure it will be deployed to managed devices across your enterprise. (See the *ManageSoft Software Deployment Guide* for details.)

4 When policy is next synchronized and managed devices next update policy, the managed devices will be able to install this package.

To define scans for malware threats

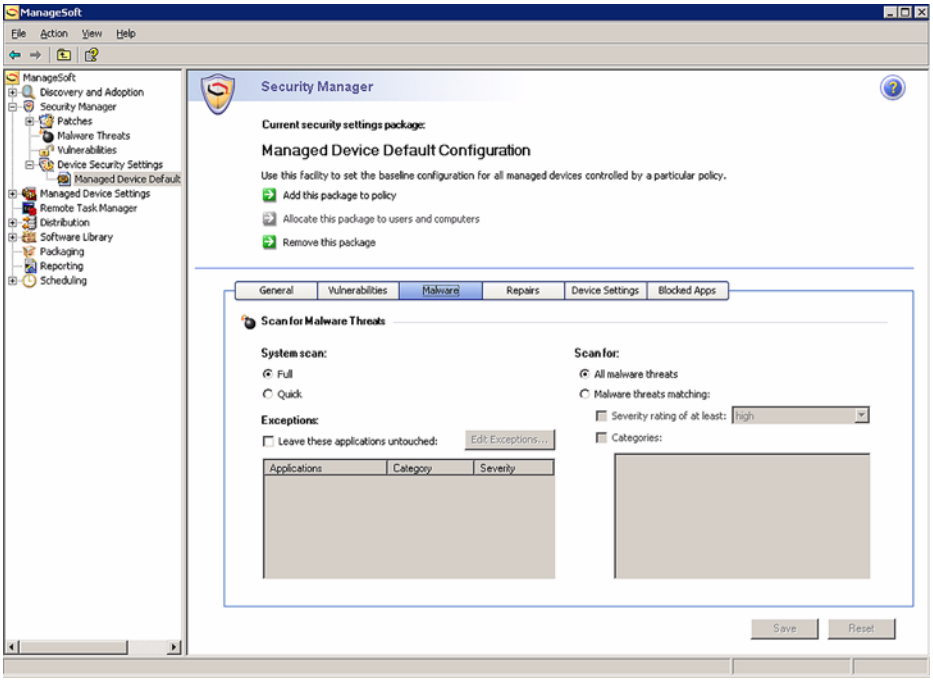
Security Manager allows you to define the scan options for malware threats on managed devices that use this security settings package. You can also specify malware programs that you want to ignore — for example, if 'Malware 711' only affects managed devices running Windows NT and you are not supporting Windows NT, it saves time to specify this malware program as an exception.

1 From the **Security Manager** node in the console tree, expand the **Device Security Settings** node and browse the folder structure to see the list of security settings packages.

If there are multiple versions of the security settings package, expand the node for that package to view the list of versions.

2 Select the package to display its details in the details pane.

3 Click the **Malware** tab.



Use this page to specify the scan options for malware threats on managed devices that use this security settings package.

4 By default, Security Manager scans the entire system for malware threats (**Full**). If you only want to scan the registry, cookies, memory, Windows folder, and Program Files folder, click **Quick**.

This information is stored in the **ScanType** registry key, which is described further on page 60.

5 By default, Security Manager scans for all types of malware threats. If this is what you want to do, ensure **All malware threats** is selected then go to step 7.

This information is stored in the **AllMalware** registry key, which is described further on page 34.

6 If you only want to scan for specific types of malware threats:

a. Click **Malware threats matching**.

b. To scan for malware threats according to their severity, select the **Severity rating of at least** check box, then click the down arrow and select the required severity rating (**none** being the least severe and **critical** being the most severe).

This information is stored in the **UseSeverityRating** registry key, which is described further on page 63.

c. To scan for malware threats according to category, select the **Categories** check box then select the check boxes to the left of the required categories.

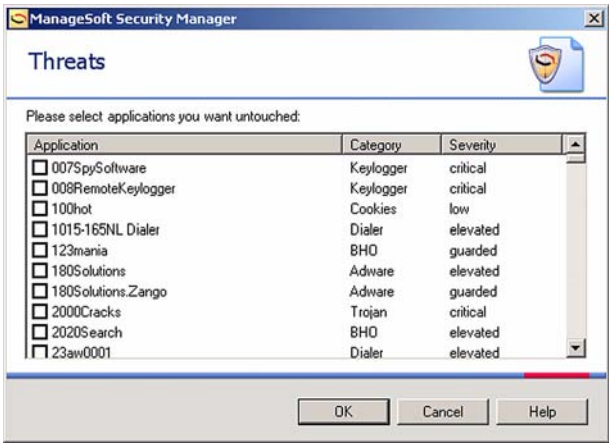
This information is stored in the **UseCategories** and **ScanSpecificCategories** registry keys, which are described further on page 62 and page 58 respectively.

7 If there are malware threats that you do not want to scan for:

a. Select the **Leave these applications untouched** check box.

b. Click **Edit Exceptions...**

The **Threats** dialog is displayed.



Be aware: If you choose to ignore a malware program that has been quarantined, it will be restored on the managed device and ignored in the future.

c. Select the check box to the left of malware threats that are not to be scanned.

d. Click **OK**.

The dialog closes, and the malware threats are added to the list to be ignored.

This information is stored in the **ApplyExceptions** registry key, which is described further on page 36.

8 When you have finished making changes, do one of the following:

- Define the malware infection repair options — see *To define options for repairing malware infections* on page 7.
- Click **Save** if you have finished working with this security settings package.

  The **Security settings for managed device distribution wizard** is invoked. For step-by-step instructions, see the *ManageSoft Security Manager Guide*.

To define options for repairing malware infections

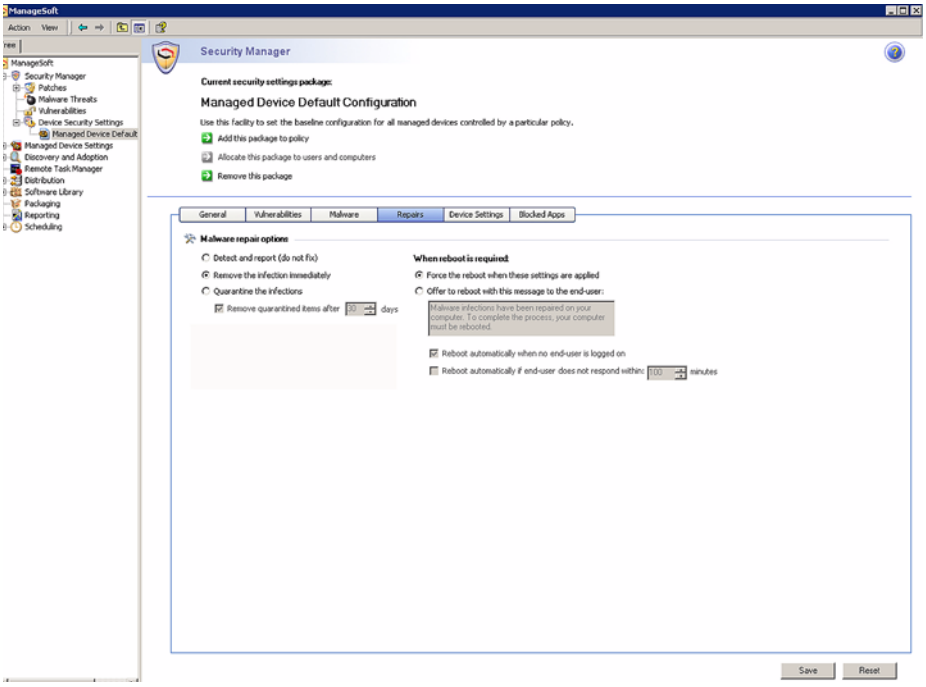
Security Manager allows you to define how to fix managed devices when malware programs are detected on managed devices that use this security settings package.

1 From the **Security Manager** node in the console tree, expand the **Device Security Settings** node and browse the folder structure to see the list of security settings packages.

If there are multiple versions of the security settings package, expand the node for that package to view the list of versions.

2 Select the package to display its details in the details pane.

3 Click the **Repairs** tab.



Use this page to specify the malware infection repair options on managed devices that use this security settings package.

4 Select one of the following actions for when malware infections are detected:

- **Detect and report (do not fix)**—If you click this button, you are not required to enter any further details on this page. Skip to step 10.

- **Remove the infection immediately**—Click this button if you want Security Manager to automatically remove any malware threats from the managed device.

  If you select this option, managed devices will report as compliant as soon as the infection is removed. Unless a threat cannot be removed, all managed devices will always report as compliant.

- **Quarantine the infections**—Click this button if you want Security Manager to quarantine any malware threats.

  If you want to monitor the level of infection occurring in your enterprise, this may be an appropriate option. It allows you to report on the level of infection, but offers you more protection than the **Detect and report** option. You can also automatically remove quarantined items after a specified number of days (see below).

5 If you clicked **Quarantine the infections** and you want to remove the quarantined items after a specified period:

- Ensure the **Remove quarantined items after** check box is selected
- Enter (or select) the number of days after which quarantined items are removed.

> **Be aware:** Make sure that you allow enough time for administrators to receive notification about quarantined malware threats that should be restored. To restore a quarantined malware threat on a managed device, mark it as an exception on the **Malware** tab page — see *To define scans for malware threats* on page 3.

This information is stored in the **RemoveInfectionAfterPeriod** registry key, which is described further on page 48.

When reboot is required

6 If managed devices must be rebooted, select one of the following:

- **Force the reboot when these settings are applied**

  If this check box is selected, Security Manager forces the managed device to immediately reboot if the package being installed requires it.

  This information is stored in the **MalwareForceReboot** registry key, which is described further on page 44.

- **Offer to reboot with this message to the end-user**

  If this check box is selected, Security Manager performs a *polite* reboot (prompting user interaction to close down other applications).

This information is stored in the **MalwareAutorebootMessage** registry key, which is described further on page 40.

7 If you selected to **Offer to reboot with this message to the end-user**, select:

- **Reboot automatically when no end-user is logged on**

  This information is stored in the **MalwareAutorebootNotLoggedIn** registry key, which is described further on page 41.

- **Reboot automatically if end-user does not respond within ... minutes**

  If this check box is selected, you can specify how long Security Manager should wait for end-users to respond before rebooting their computers.

  This information is stored in the **MalwareAutorebootWithNoWait** registry key, which is described further on page 43.

8 If you selected the **Reboot automatically if end-user does not respond within ... minutes** check box, enter the number of minutes before an automatic reboot takes place after displaying the reboot message.

This information is stored in the **MalwareAutoRebootPeriod** registry key, which is described further on page 42.

9 When you have finished making changes, do one of the following:

- Click another tab to continue working with the properties of this security settings package
- Click **Save** if you have finished working with this security settings package.

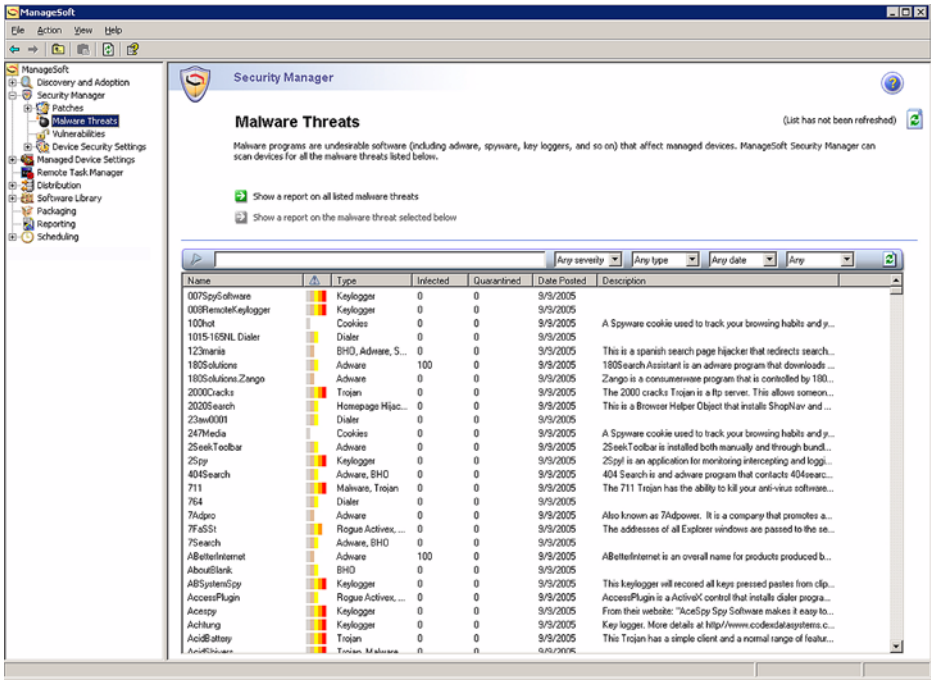
  The **Security settings for managed device distribution wizard** is invoked. For step-by-step instructions, see the *ManageSoft Security Manager Guide*.

Data about malware threats

Security Manager maintains a current list of malware threats. To view it:

1 In the console tree, under the **Security Manager** node, select **Malware Threats**.

The **Malware Threats** page is displayed, with a list of threats.



To retrieve the most up-to-date list of malware threats from the ManageSoft Corporation website, click the refresh icon: 

Threats are listed in alphabetical order by name. The information displayed about each threat includes:

- **Name**—the name of the threat.
- **Severity**—a graphical representation of the severity of this threat, where the red bar indicates the highest impact.
- **Type**—the category (such as keylogger, trojan horse, adware) of the threat.

- **Infected**—the number of managed devices in your organization with the malware program identified by this threat installed.
- **Quarantined**—the number of managed devices in your organization that had been infected, but the infection has been moved into a safe area. Quarantined items can be restored.
- **Date Posted**—the date at which details about this threat were added to this list.
- **Description**—details about the threat.

From this page, you can:

- Access reports about malware threats in your enterprise. See *Reporting on malware threats* on page 11.
- Use the filter bar to restrict the number of malware threats displayed in this list. See *Filtering the list of malware threats* on page 11.
- Double-click a threat to see its complete details. See *Viewing details about a malware threat* on page 12.

Reporting on malware threats

Security Manager provides some standard reports that help you to understand the exposure of your managed devices to known malware threats.

From the **Malware Threats** page, you can access two of these reports:

- Click **Show a report on all listed malware threats** to access the *Current managed device infections listed by malware program* report. See page 16 for details about this report.
- Select a malware threat from the list and click **Show a report on the malware threat selected below** to access the *Managed devices infected by this malware program* report. See page 20 for details about this report.

Filtering the list of malware threats

Use the filter bar to restrict the number of malware threats displayed in the list.

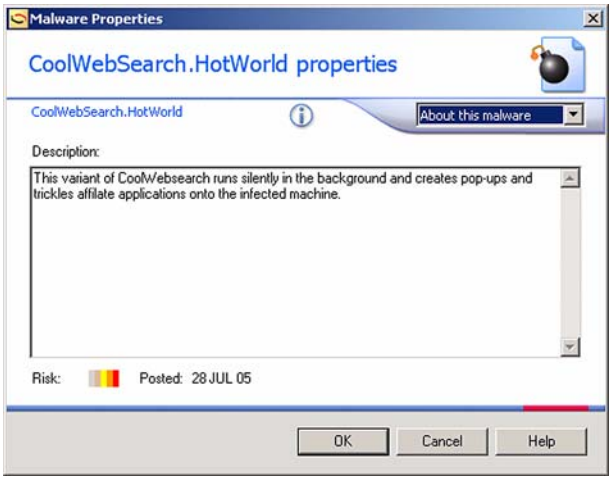
Do any of the following:

- In the text input field at the left of the filter bar, type one or more characters. Only malware threats whose names contain those characters will be displayed. For example, if you type **Keylogger**, only threats with **Keylogger** anywhere in their names will be displayed.
- From the **Any severity** pulldown list, select the severity of threats to display.
- From the **Any type** pulldown list, select the category of threats to display.
- From the **Any date** pulldown list, select a time period such as **< 1 week** or **< 1 month**. Only threats published in this time period will be displayed.
- From the **Any** pulldown list, choose whether to display only threats that have affected your enterprise (**Infected**), or only threats that have not affected your enterprise (**Not infected**).

The list of threats updates as you make your selections. Alternatively, click the refresh icon at the right hand side of the filter bar.

Viewing details about a malware threat

The **Malware Threat Properties** dialog shows a description of the selected malware threat.



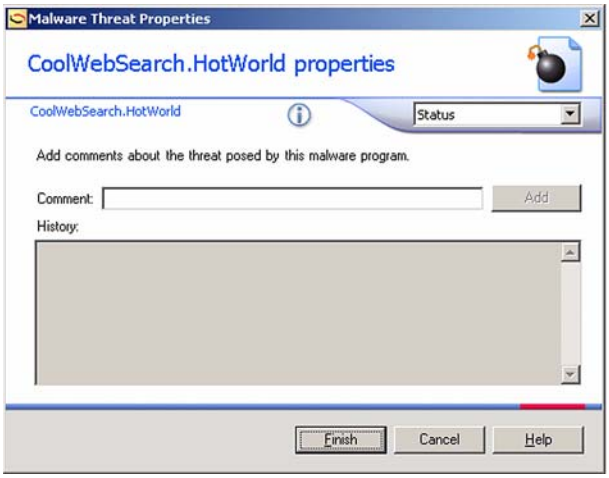
You cannot change any of the details on this dialog.

Do any of the following:

- For details about the status of this threat in your enterprise, click the **About this malware** drop-down arrow and select **Status**. See *Viewing the status of a malware threat* on page 13.
- Click **OK** to close the dialog.

Viewing the status of a malware threat

This dialog shows details about the status of the selected malware threat in your enterprise. You can add comments about the threat, and specify that the malware program that implements this threat should be automatically removed from managed devices in your enterprise when detected.



Do any of the following:

- In the **New comment** field, enter a comment and click **Add**.

  The comment is recorded against this malware threat, and automatically tagged with your username and the current date. This is added to the **History** box.
- To return to the description of this malware threat, click the **Status** drop-down arrow and select **About this threat**. See *Viewing details about a malware threat* on page 12.
- Click **Finish** to close the dialog.

Viewing reports about malware threats

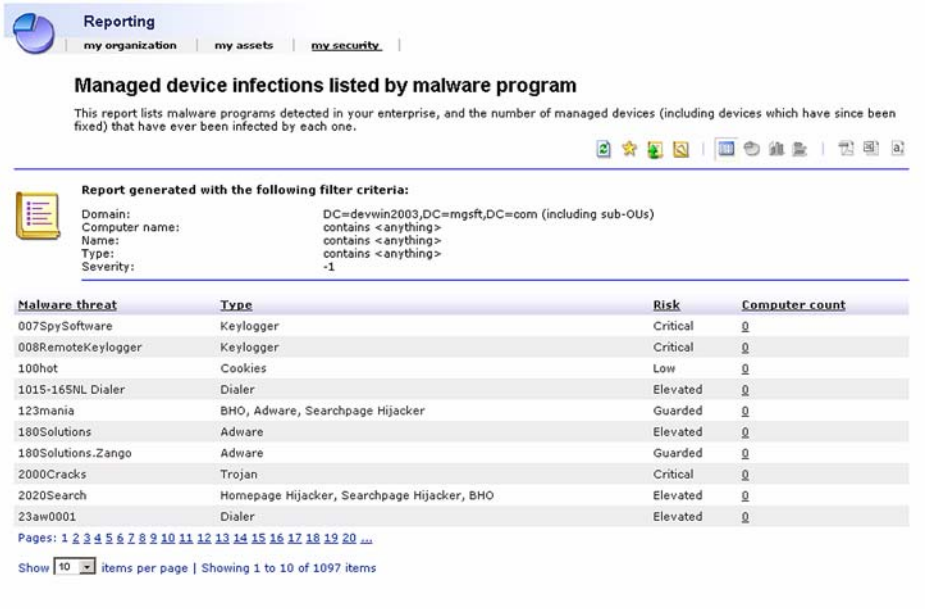
The following reports about malware threats in your enterprise are available:

Report	Description	For more details
Managed device infections listed by malware program	Lists all malware programs that have ever infected managed devices in your enterprise, and the number of managed devices that have been infected by each program. This total includes managed devices that have been infected, but subsequently fixed.	See page 15
Current managed device infections listed by malware program	Lists malware programs that are currently infecting managed devices in your enterprise, and the number of managed devices infected by each program.	See page 16
All managed devices showing current count of malware infections	Lists all managed devices and the number of current malware infections on each managed device. This does not include infections that have been fixed.	See page 17
Current malware infections listed by managed device name	Lists the number of malware programs that are currently infecting managed devices in your enterprise. This does not include infections that have been fixed.	See page 18
Malware scan details listed by managed device	Displays details about the last scan for malware infections on each managed device.	See page 19
Managed devices infected by this malware program	Lists managed devices currently infected by a selected malware program.	See page 20

To view the “Managed device infections listed by malware program” report

1 From the **my security** page, in the **Malware** panel, click the **All** link to the right of **Malware Threats**.

The report summary page is displayed. This page displays details about malware programs that have been detected in your enterprise, and how many managed devices were infected. Some of these managed devices may not be currently infected. (For a report listing only currently-infected devices, see *Viewing reports about malware threats* on page 14.)



2 To list the managed devices that have been infected by a malware program, click the **Computer count** column to the right of the required malware threat. The “Managed devices infected by this malware program” report is displayed. For further information, see *To view the “Managed devices infected by this malware program” report* on page 20.

To view the "Current managed device infections listed by malware program" report

1 To view this report, do one of the following:

- From the **my security** page, in the **Malware** panel, click the **Current infections** link to the right of **Malware Threats**.
- From the **Malware Threats** page (see Chapter 9 *Malware threats*), click **Show a report on all malware threats**, and complete the details on the following page to specify the scope of the report.

The report summary page is displayed. This page lists the malware programs that are currently infecting managed devices, and the number of managed devices infected by each malware program.

> **Be aware:** If you have configured your system to immediately remove infections, all managed devices should report with no infections.
>
> To monitor the level of infection occurring, you may find it useful to quarantine infections and remove them after a number of days, rather than removing them immediately. This configuration would allow you to report on current infections, while still offering some protection from the infections.
>
> See *To define options for repairing malware infections* on page 7 for details about changing the repair options for managed devices.

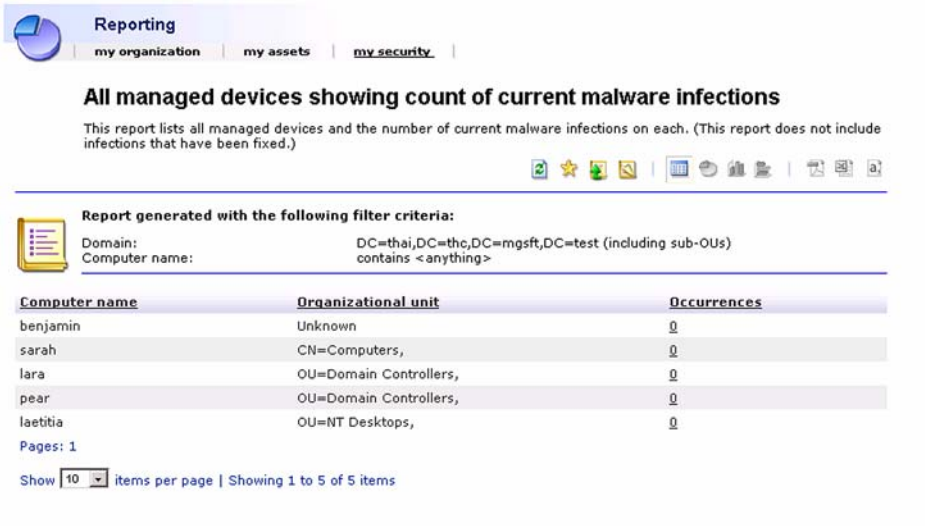
2 To list the managed devices that have been infected by a malware program, click the **Computer count** column to the right of the required malware threat. The “Managed

devices infected by this malware program” report is displayed. For further information, see *To view the “Managed devices infected by this malware program” report* on page 20.

To view the “All managed devices showing count of current malware infections” report

1 From the **my security** page, in the **Malware** panel, click the **All** link to the right of **Managed Devices**.

The report summary page is displayed. This page lists all managed devices and the number of malware programs currently installed on each managed device.



2 To view a list of the malware programs that have been detected on a specific managed device, click the **Occurrences** column to the right of the required managed device. The “Malware programs detected on this managed device” report is displayed.

To view the “Current malware infections listed by managed device name” report

1 From the **my security** page, in the **Malware** panel, click the **Current infections** link to the right of **Managed Devices**.

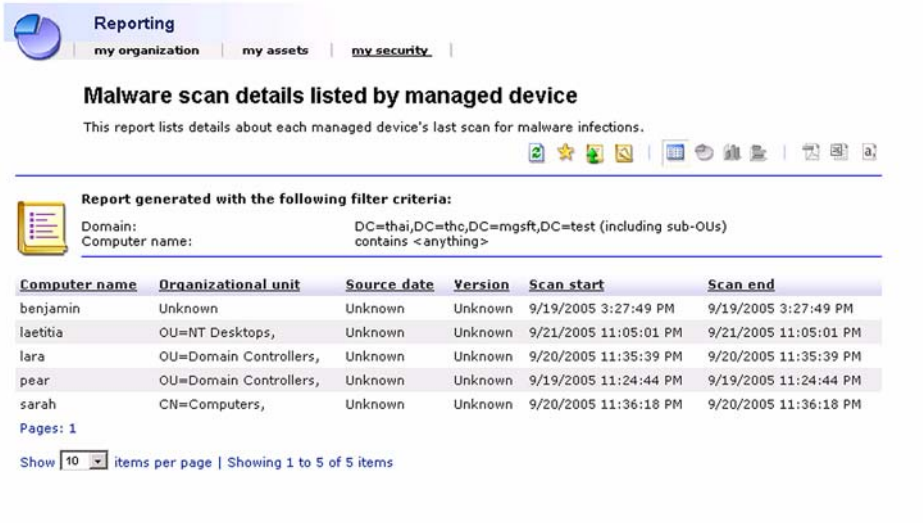
The report summary page is displayed. This page shows the number of malware programs currently installed on each managed device.

2 To view a list of the malware programs that have been detected on a specific managed device, click the **Occurrences** column to the right of the required managed device. The “Malware programs detected on this managed device” report is displayed.

To view the “Malware scan details listed by managed device” report

From the **my security** page, in the **Malware** panel, click the **Scan Status** link to the right of **Managed Devices**.

The report summary page is displayed. This page displays details about the last scan for malware programs on each managed device.



To view the “Managed devices infected by this malware program” report

To view this report, do one of the following:

- From the **Malware Threats** page (see Chapter 9 *Malware threats*), select the malware threat on which you want to report, and click **Show a report on the malware threat selected below**.
- Click the **Computer count** column from the “Managed device infections listed by malware” report (see page 15) or the “Current managed device infections listed by malware program” report (see page 16).

The report summary page is displayed. This page lists all managed devices that are currently infected by the selected malware program.

To temporarily stop malware or vulnerability scans

Malware scans occur on managed devices according to the events defined in the schedules defined in Deployment Manager. These schedules are distributed to managed devices, and are run as scheduled tasks by ManageSoft Task Scheduler (or Microsoft Task Scheduler) on the managed device.

Two events contain settings associated with malware scans and vulnerability scans:

- **Generate a ManageSoft Security Analysis** event
- **Apply a ManageSoft Security Policy** event.

To stop malware or vulnerability scans from occurring, you can remove the relevant triggers from your schedules and re-distribute the schedules to managed devices. (To initiate scans again, simply re-apply the triggers and distribute the updated schedule again.)

> **Be aware:** These events also contain options to initiate security patch deployment tasks. If you modify fields not described in the following instructions, you may stop these security patch deployment tasks.

To remove the triggers:

1. From the ManageSoft console, navigate to the **Scheduling** node.
2. In the console tree, click the schedule that you want to change.

   > **Be aware:** Security management events are only applicable for machine schedules, not user schedules.

   The details pane lists all events associated with the schedule.
3. Right-click the **Generate Security Analysis** event, and select **Properties** from the context menu.

   The **Generate Security Analysis Properties** dialog is displayed.
4. Do any of the following:
   - To stop generating compliance data about vulnerabilities on managed devices, clear the **Vulnerabilities** check box.
   - To stop generating malware compliance data, clear the **Malware** check box.

5 Click **OK**.

The properties dialog is closed.

6 Right-click the **Apply Security Policy** event, and select **Properties** from the context menu.

The **Apply Security Policy Properties** dialog is displayed.

7 To stop malware compliance scans, clear the **Malware** check box.

8 Click **OK**.

The properties dialog is closed.

9 Distribute the modified schedule to managed devices. For details about distributing schedules, see the *Scheduling* chapter of the *ManageSoft Software Deployment Guide*.

Malware and vulnerability troubleshooting

This section provides the following troubleshooting tips:

- *Malware and vulnerability management files and locations* on page 23
- *Malware scanning won't turn on/off* on page 25
- *Malware reports show devices of unknown status* on page 27.

Malware and vulnerability management files and locations

This section lists some of the key files and locations used by Security Manager. You may need to reference some of these during troubleshooting operations.

Administration server signature files

Malware signature files contain information required by Security Manager to identify installed malware.

When you download the latest malware signature files from ManageSoft Corporation, these files are downloaded to the following location on the administration core server:

```
C:\ManageSoft\Repository\SecurityPatch\errata\malware
```

These are automatically packaged into a `Malware definitions` package for deployment.

Managed device signature files

When the malware definitions files are deployed to managed devices, they are stored in the following location:

```
C:\Program Files\ManageSoft\Security Agent\data\malware
\Definition files
```

Managed device quarantined files

When malware is found on a managed device, quarantined files are moved to the following location:

```
C:\Program Files\ManageSoft\Security Agent\data\malware
\Quarantine files
```

Managed device vulnerability scan files

MBSA is used on managed devices to scan for vulnerabilities.

This product is installed in one of the following locations:

MBSA version 1:

```
C:\Program Files\Microsoft Baseline Security Analyzer
```

MBSA version 2:

```
C:\Program Files\Microsoft Baseline Security Analyzer 2
```

Managed device log files

To assist with troubleshooting malware and vulnerability functions on managed devices, you can review a log of security agent activities. This log file is located in:

```
C:\Temp\SecurityAgent.log
```

Malware scanning won't turn on/off

Problem

The behavior of managed devices does not match my malware scan settings in one of the following ways:

- I have turned malware scans off, but they continue to run
- I have turned malware scans on, but they do not run.

Resolution

Malware scans can be turned on or off in a number of ways.

If malware operations on a managed device are not as expected, one or more of the following settings may not be set appropriately. Check and modify the settings as necessary to achieve the correct result.

In schedules

- The **Generate a ManageSoft Security Analysis** event contains settings that determine whether malware scans are run on the managed device.
- The **Apply a ManageSoft Security Policy** event contains settings that determine whether malware compliance data is generated on the managed device.
- By default, security compliance data (including malware data) is also generated on the managed device by the **Generate a ManageSoft Inventory** event. However, security compliance data will not be generated if the command-line contains the option `-o Security=False`. This setting stops security compliance generation only for this event, not for the **Apply a ManageSoft Security Policy** event.

If you make a change to a schedule, you must re-distribute the schedule before the new settings take effect.

In the Registry

- The **Security** registry key (documented in *ManageSoft Reference: Preferences for Managed Devices*) applies the same setting as the `-o Security` command-line option described above. However, if this registry key is set on the managed device, it overrides the behavior specified by the command-line option.
- Managed device settings packages can be used to modify registry keys on managed devices. The **Security** registry key can be defined in a managed device settings package (using the view available from the **Managed Device Settings** node on the ManageSoft console).

If you make a change to a managed device settings package, you must re-distribute the package before the new settings take effect.

Malware reports show devices of unknown status

Problem

Some Security Manager compliance reports are displaying accurate data, but malware and vulnerability reports do not contain any data.

Instead, all managed devices are listed as devices of unknown status.

Resolution

This symptom occurs if you do not have a license for the malware and vulnerability components of Security Manager.

Contact your ManageSoft Corporation consultant to arrange purchase of the required license.

Stored procedures

During installation on administration servers, Security Manager installs a number of stored procedures, used for compliance reports.

If you choose to customize these reports, or create your own compliance reports, you can use these stored procedures:

Stored procedure name	Description
AllComputerByMalware	Provides a summary of all managed devices that are infected by a particular malware program.
AllComputersHavingVulnerability	Provides a summary of all managed devices exposed to a particular vulnerability.
AllMalwareByComputer	Lists malware programs currently infecting a particular managed device.
AllVulnerabilitiesByComputer	Lists vulnerabilities currently detected on a particular managed device.
ComplianceBulletinAndComputerDetails	Provides details about patches, including the status of each patch for a particular bulletin applied on a particular managed device.
ComplianceByBulletinComputerList	Lists managed devices that have applied a particular bulletin.
ComplianceByBulletinSummaryList	Provides a summary of bulletins, with a count of managed devices that have downloaded the bulletin. The totals are put into columns for each category of compliance and non-compliance.
ComplianceByComputerBulletinList	Lists bulletins that have been applied on a particular managed device.

Stored procedure name	Description
ComplianceByComputerSummaryList	Provides a summary of managed devices, with a total of bulletins that have been tested on that device. The count is put into columns for each category of compliance and non-compliance.
ComplianceComputerAndBulletinList	Populates temporary tables with all the data for each bulletin against each managed device. Other stored procedures then extract data from the temporary tables and make further joins. No report uses this stored procedure directly.
ComputerCountByMalware	Counts the number of managed devices infected by each malware program (includes malware programs that are not infecting any managed devices).
ComputerCountByUnresolvedMalware	Counts the number of managed devices infected by each malware program where at least one infected managed device is known.
ComputerCountByUnresolvedVulnerability	Counts the number of managed devices exposed to each vulnerability where at least one managed device is known to be exposed to the vulnerability.
ComputerCountByVulnerability	Counts the number of managed devices exposed to each vulnerability (includes vulnerabilities to which no managed devices are exposed).
MalwareCountByComputer	Counts the number of malware infections for each managed device.

Stored procedure name	Description
MalwareGetAllSummaryCount	Counts the malware compliance of all managed devices, grouped into compliant, non-compliant, and unknown states.
MalwareGetManagedSummaryCount	Counts the malware compliance of all managed devices, grouped into compliant, non-compliant, and unknown states.
MalwareUnresolvedCountByComputer	Counts the number of malware infections for each managed device, filtered to only show managed devices with current infections.
VulnerabilityUnresolvedCountByComputer	Counts the number of malware infections for each managed device (filtered to only show managed devices with current infections).

Malware security agent preferences

The following malware preferences can be used to control the behavior of Security Manager. Most of these can be used on the security agent command line:

- **Action** — action required when a malware infection is detected.
- **AllMalware** — whether to scan for all malware threats (`True`) or only for malware threats that match specific criteria.
- **ApplicationsToIgnore** — lists malware programs to be ignored (not fixed or quarantined) if detected on managed devices. This preference is ignored unless **ApplyExceptions** is `True`.
- **ApplyExceptions** — whether to apply exceptions when scanning for malware threats.
- **ApplyMalwarePolicy** — if **ApplySecurityPolicy** is `True`, this specifies whether to scan for malware threats and remove or quarantine infections (`True`) or not (`False`).
- **Confirm** — whether confirmation is required before stopping suspicious activities.
- **DatFilePath** — the path to where the malware definition files are located. This preference cannot be used on the security agent command line.
- **MalwareAutoRebootMessage** — message displayed to the end-user before the managed device is automatically rebooted.
- **MalwareAutorebootNotLoggedIn** — whether to reboot automatically if **MalwareAutoRebootMessage** is set and no end-user is logged on.
- **MalwareAutoRebootPeriod** — number of minutes before a reboot takes place if **MalwareForceReboot** is not set and the user does not respond.
- **MalwareAutorebootWithNoWait** — whether to reboot automatically if **ForceReboot** is not set and no user is logged on.
- **MalwareForceReboot** — determines whether ManageSoft performs a forced reboot if the desktop is not locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- **MalwareScan** — if **ApplySecurityPolicy** is `False`, this specifies whether or not to scan for malware threats.
- **MalwareUpdateURL** — the URL used by Security Manager to retrieve malware information.
- **QuarantinePeriod** — number of days after which quarantined items are to be removed.

- **RemoveInfectionAfterPeriod** — whether a malware infection should be removed after a specified period.
- **ScanCDROMDrive** — whether to enable scanning of CD-ROM drives.
- **ScanCookies** — whether to enable scanning of cookies.
- **ScanFileSystem** — whether to enable scanning of file systems.
- **ScanFixedDrive** — whether to enable scanning of fixed drives.
- **ScanMemory** — whether to enable scanning of memory.
- **ScanNetworkDrive** — whether to enable scanning of network drives.
- **ScanRAMDiskDrive** — whether to enable scanning of RAM disk drives.
- **ScanRegistry** — whether to enable scanning of the Windows registry.
- **ScanRemovableDrive** — whether to enable scanning of removable drives.
- **ScanSpecificCategories** — semi-colon (;) separated list of categories for malware threat scanning. Managed devices will only be scanned for malware threats in these categories.
- **ScanSpecificFolders** — folders to scan for malware threats.
- **ScanType** — whether to perform a `Full` scan or a `Quick` scan for malware threats.
- **SeverityRatingMinimum** — the minimum severity rating of malware threats to scan for.
- **UseCategories** — whether the scan should be restricted to particular categories of malware threats (`True`). Works in conjunction with **ScanSpecificCategories**.
- **UseSeverityRating** — whether the scan should be restricted to malware threats of particular severity. Works in conjunction with **SeverityRatingMinimum**.

Action

Command line | **Registry**

Security Manager provides malware repair options on the **Repairs** tab of the **Device Security Settings** node.

This preference specifies the action performed by Security Manager when a malware infection is detected.

Also see *RemoveInfectionAfterPeriod* on page 48 and *QuarantinePeriod* on page 47.

Values / range	`Report, Remove, Quarantine`
Default value	`Remove`

Command line

Tool:	Security agent
Example:	`-o Action=Remove`

Registry

Installed by:	ManageSoft internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

AllMalware

Command line | **Registry**

Security Manager provides the facility to scan for all malware or malware that matches specific criteria (selected on the **Malware** tab of the **Device Security Settings** node).

When this preference is set to `True`, Security Manager scans for all malware.

When set to `False`, Security Manager only scans for malware that matches a specific severity and/or categories. Severity ratings are set on the **UseSeverityRating** preference (see page 63); categories are set on the **UseCategories** preference (see page 62).

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o AllMalware=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ApplicationsToIgnore

Command line | Registry

If the **ApplyExceptions** preference is set to `True`, this preferences specifies the malware programs that can be ignored on managed devices. They will be reported as present, but they will not be fixed or quarantined.

Application names must be separated by semi-colons (;).

Values / range	String
Default value	None
Example value	`winmine.exe;hugovirus.exe`

Command line

Tool:	Security agent
Example:	`-o ApplicationsToIgnore=winmine.exe`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ApplyExceptions

Command line | **Registry**

Security Manager provides the facility to ignore applications that are not to be scanned for malware (selected on the **Malware** tab of the **Device Security Settings** node).

When this preference is set to `True`, Security Manager does not scan applications that have been specified as exceptions. Exceptions are set on the **ApplicationsToIgnore** preference.

When set to `False`, all applications are to be scanned without exception.

For information on **ApplicationsToIgnore**, see page 35.

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o ApplyExceptions=False`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ApplyMalwarePolicy

Command line | **Registry**

WARNING

Internal use only: do not edit.

This preference only applies if **ApplySecurityPolicy** is set to `True`.

This preference specifies whether (`True`) or not (`False`) the Security Manager security agent will scan for malware threats, and remove or quarantine malware infections.

For information on **ApplySecurityPolicy**, see *ManageSoft Reference: Preferences for Managed Devices*.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ApplyMalwarePolicy=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

Confirm

Command line | **Registry**

Security Manager provides malware repair options on the **Repairs** tab of the **Device Security Settings** node.

When this preference is set to `True`, Security Manager asks the end-user for confirmation to stop suspicious activities.

When set to `False`, suspicious activities are stopped immediately without notifying the end-user.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o Confirm=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

DatFilePath

Registry

WARNING

Internal use only: do not edit.

The path to where the malware definition files are located.

The malware definition files are installed by the Security Manager malware definition package, which is created automatically whenever Security Manager is refreshed.

Values / range	String
Default value	`$(ProgramPath)\\..\\SecurityAgent\\data\\malware\\Definition Files`

Registry

Installed by:	Predefined within Security Manager malware definition package.
User preference:	Not available

MalwareAutoRebootMessage

Command line | Registry

If managed devices require a reboot after applying security setting packages, this preference is used to record the message that is displayed to the end-user before the managed device is automatically rebooted.

Also see *MalwareAutorebootWithNoWait* on page 43 and *MalwareAutoRebootPeriod* on page 42.

Values / range	String
Default value	`Malware infections have been repaired on your computer. To complete the process, your computer must be rebooted.`

Command line

Tool:	Security agent
Example:	`-o MalwareAutoRebootMessage="We've updated your computer, and it now needs to reboot. Sorry for the inconvenience."`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareAutorebootNotLoggedIn

Command line | Registry

If the **MalwareForceReboot** preference is set to `False` and no user is logged on, this preference specifies whether reboot takes place automatically (`True`) or not (`False`).

If set to `False`, Security Manager waits for the specified period before rebooting the managed device. The wait period is determined by the **MalwareAutoRebootPeriod** preference (see page 42).

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o MalwareAutorebootNotLoggedIn=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareAutoRebootPeriod

Registry

If the **MalwareForceReboot** preference is set to `False` and the end-user does not respond, this preference specifies the number of minutes before a reboot takes place.

The minimum number of minutes is `5`, and the maximum is `60000`.

Also see **MalwareForceReboot** on page 44.

Values / range	Integer between `5` and `60000`.
Default value	`100`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareAutorebootWithNoWait

Registry

If the **MalwareForceReboot** preference is set to `False` and this preference is set to `True`, Security Manager waits for the specified period before rebooting the managed device.

The period to wait before a reboot is determined by the **MalwareAutoRebootPeriod** preference (see page 42).

Values / range	Boolean (true or false)
Default value	`True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareForceReboot

Registry

If managed devices require a reboot after applying security setting packages, this preference specifies whether to force the reboot (`True`) or prompt the end-user to reboot (`False`).

Values / range	Boolean (true or false)
Default value	`True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareScan

Command line | **Registry**

WARNING

Internal use only: do not edit.

This preference only applies if **ApplySecurityPolicy** is set to `False`.

This preference specifies whether (`True`) or not (`False`) scanning is to be performed for malware threats.

For information on **ApplySecurityPolicy**, see *ManageSoft Reference: Preferences for Managed Devices*.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o MalwareScan=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

MalwareUpdateURL

Registry

The URL used by Security Manager to retrieve malware information.

This registry key can also be set using the ManageSoft Configuration Tool. See *Reviewing Security Manager configuration* on page 48 for details.

Values / range	String
Default value	`http://www.managesoft.com/support/SecurityManagement/malwareupdate.cab`
Example value	`http://www.mySite.com/support/malwareupdate.cab`

Registry

Installed by:	Installation of Deployment Manager on core servers
User preference:	N/A
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft\SecurityPatch\CurrentVersion

QuarantinePeriod

Command line | **Registry**

If the **RemoveInfectionAfterPeriod** preference is set to `True`, this preference specifies the number of days after which quarantined malware infections are to be removed.

The minimum number of days is `1`, and the maximum is `30`.

For information on **RemoveInfectionAfterPeriod**, see page 48.

Values / range	Integer between `1` and `30`.
Default value	`30`

Command line

Tool:	Security agent
Example:	`-o QuarantinePeriod=20`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

RemoveInfectionAfterPeriod

Command line | Registry

If malware infections are quarantined, this preference determines whether a malware infection should be removed after a specified period (`True`) or not removed (`False`).

Also see *Action* on page 33 and *QuarantinePeriod* on page 47.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o RemoveInfectionAfterPeriod=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanCDROMDrive

Command line | Registry

When this preference is set to `True`, Security Manager scans file CD-ROM drives for malware.

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o ScanCDROMDrive=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanCookies

Command line | Registry

When this preference is set to `True`, Security Manager scans cookies for malware.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ScanCookies=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanFileSystem

Command line | Registry

When this preference is set to `True`, Security Manager scans file systems for malware.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ScanFileSystem=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanFixedDrive

Command line | Registry

When this preference is set to `True`, Security Manager scans fixed drives for malware.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ScanFixedDrive=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanMemory

Command line | Registry

When this preference is set to `True`, Security Manager scans memory for malware.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ScanMemory=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanNetworkDrive

Command line | Registry

When this preference is set to `True`, Security Manager scans network drives for malware.

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o ScanNetworkDrive=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanRAMDiskDrive

Command line | Registry

When this preference is set to `True`, Security Manager scans RAM disk drives for malware.

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o ScanRAMDiskDrive=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanRegistry

Command line | Registry

When this preference is set to `True`, Security Manager scans the Windows registry for malware.

Values / range	Boolean (true or false)
Default value	`True`

Command line

Tool:	Security agent
Example:	`-o ScanRegistry=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanRemovableDrive

Command line | Registry

When this preference is set to `True`, Security Manager scans removable drives for malware.

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o ScanRemovableDrive=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanSpecificCategories

Command line | Registry

Specify the categories of malware threats for which Security Manager scans managed devices. Categories must be separated by semi-colons (;).

Values / range	Semi-colon (;) separated string containing any of the categories listed on the **Malware** tab of the page on which you define device security settings. Refer to the Device security settings chapter of the *ManageSoft Security Manager Guide* for details.
Default value	`{empty}`

Command line

Tool:	Security agent
Example:	`-o ScanSpecificCategories=Adware;Cookies`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

ScanSpecificFolders

Command line | **Registry**

Specify the folders that Security Manager scans for malware. This preference can accept multiple folders; delimited by (|).

Values / range	String
Default value	`{empty}`

Command line

Tool:	Security agent
Example:	`-o ScanSpecificFolders="C:\Program Files|C:\Windows"`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft\Security Agent\CurrentVersion

ScanType

Command line | **Registry**

Security Manager provides the facility to perform a `Full` system scan or a `Quick` scan for malware on managed devices (selected on the **Malware** tab of the **Device Security Settings** node).

A `Full` scan searches the entire managed device for malware; whereas a `Quick` scan searches only the registries, cookies, memory, Windows folder, and Program Files folder.

Values / range	`Full` or `Quick`
Default value	`Full`

Command line

Tool:	Security agent
Example:	`-o ScanType="Quick"`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

SeverityRatingMinimum

Command line | Registry

If the **UseSeverityRating** preference is set to `True`, this preference specifies the minimum severity rating to use when scanning for malware.

For information on **UseSeverityRating**, see page 63.

Values / range	`Critical, Elevated, Guarded, High, Low, None, Not applicable, Unknown`
Default value	`High`

Command line

Tool:	Security agent
Example:	`-o SeverityRatingMinimum=High`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

UseCategories

Command line | **Registry**

If the **AllMalware** preference is set to `False`, this preference specifies if the malware scan should be filtered based on categories (`True`) or not (`False`).

The malware categories are set in the **ScanSpecificFolders** preference (see page 58).

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o UseCategories=False`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion

UseSeverityRating

Command line | **Registry**

If the **AllMalware** preference is set to `False`, this preference specifies if the malware severity rating should be used (`True`) or not (`False`). For further information on **AllMalware**, see page 34.

The minimum malware severity rating is set on the **SeverityRatingMinimum** preference (see page 61).

Values / range	Boolean (true or false)
Default value	`False`

Command line

Tool:	Security agent
Example:	`-o UseSeverityRating=True`

Registry

Installed by:	Security Manager internals, or manual configuration
User preference:	HKEY_CURRENT_USER\Software\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion
Computer preference:	HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ ManageSoft\Security Agent\CurrentVersion