



CHAPTER 29

Symantec AntiVirus Configuration

To enable a Symantec AntiVirus agent as a reporting device in MARS, you must identify the Symantec System Center console as the reporting device. The Symantec System Center console receives alerts from the AV agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the AV agent that originally triggered the event, rather than the Symantec System Center console that forwarded it. Therefore, MARS requires host definitions for each of the AV agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the Symantec System Center console.

The MARS Appliance discovers AV agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the AV agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the Symantec System Center console as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the Symantec System Center console; however, you are not required to define each agent. The default topology presentation for discovered AV agents is within a cloud.



Note

The first SNMP notification from an unknown AV agent appears to originate from the Symantec System Center console. MARS parses this notification and defines a child agent of the Symantec System Center console using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the AV agent.

Prior to 4.2.1, you were required to manually add each agent or by using an exported agent list, as defined in [Export the AntiVirus Agent List, page 29-7](#). Beginning in release 4.2.1, the MARS Appliance discovers AV agents as they generate alerts.

Configuring the Symantec AntiVirus integration requires performing two tasks:

- [Configure the AV Server to Publish Events to MARS Appliance, page 29-2](#)
- [Add the Device to MARS, page 29-8](#)

In addition, you can perform the following task to expedite populating the Agent list in MARS:

- [Export the AntiVirus Agent List, page 29-7](#)

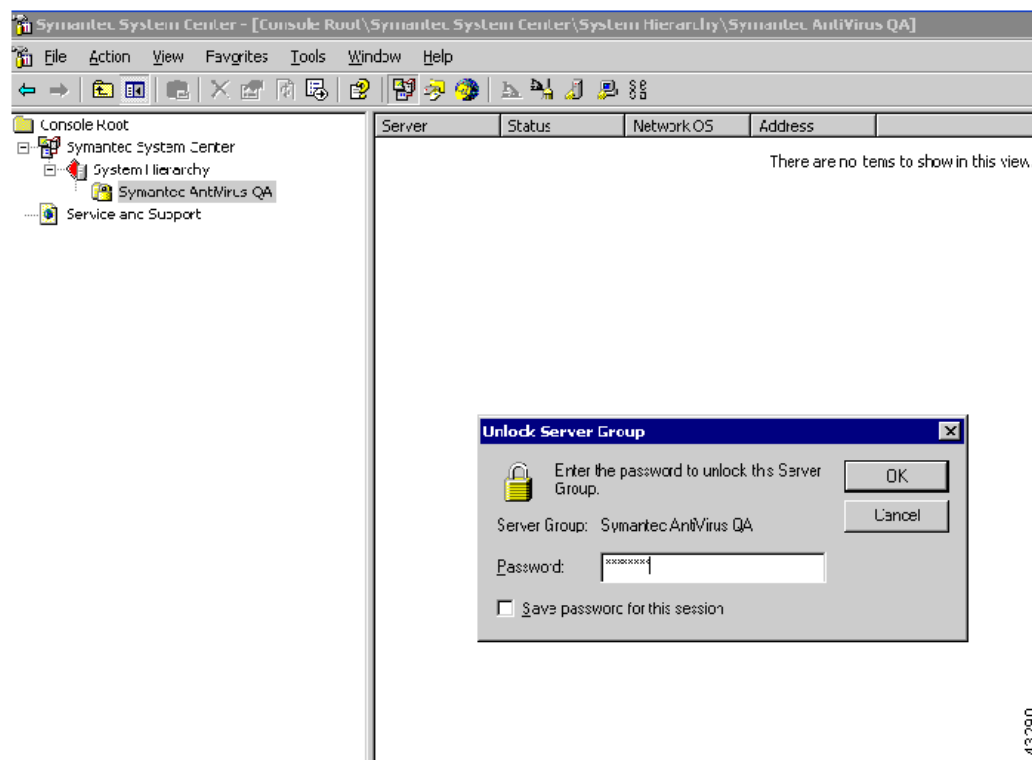
Configure the AV Server to Publish Events to MARS Appliance

To configure the AV server to publish events to MARS, follow these steps:

- Step 1** Log in to the Windows server running Symantec AV.
- Step 2** To identify the Local Controller as a valid SNMP trap destination, click **Administrative Tools > Services > SNMP Service > Traps > Trap destinations**.
- Step 3** Enter the IP address of the Local Controller in the Trap Destination page, and click **OK** to close all open windows.
- Step 4** Select **Start > All Programs > Symantec System Center Console**.
- Step 5** In the Symantec System Center window, click **System Hierarchy**.
- Step 6** Under System Hierarchy, right-click the appropriate server group name and unlock the server group by supplying the configured password.

Unlocking the server enables you to configure it.

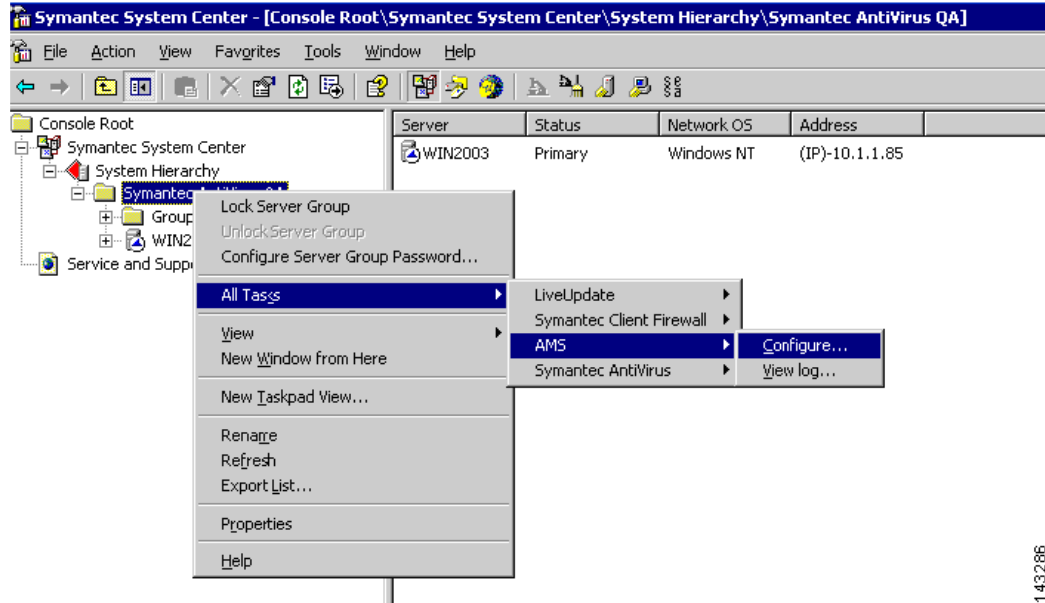
Figure 29-1 Symantec Unlock Server



143290

- Step 7** Configure Symantec server (AMS-Alert Management System) to send SNMP traps to MARS. Right click the unlocked server group name, then select **All Tasks > AMS > Configure**.

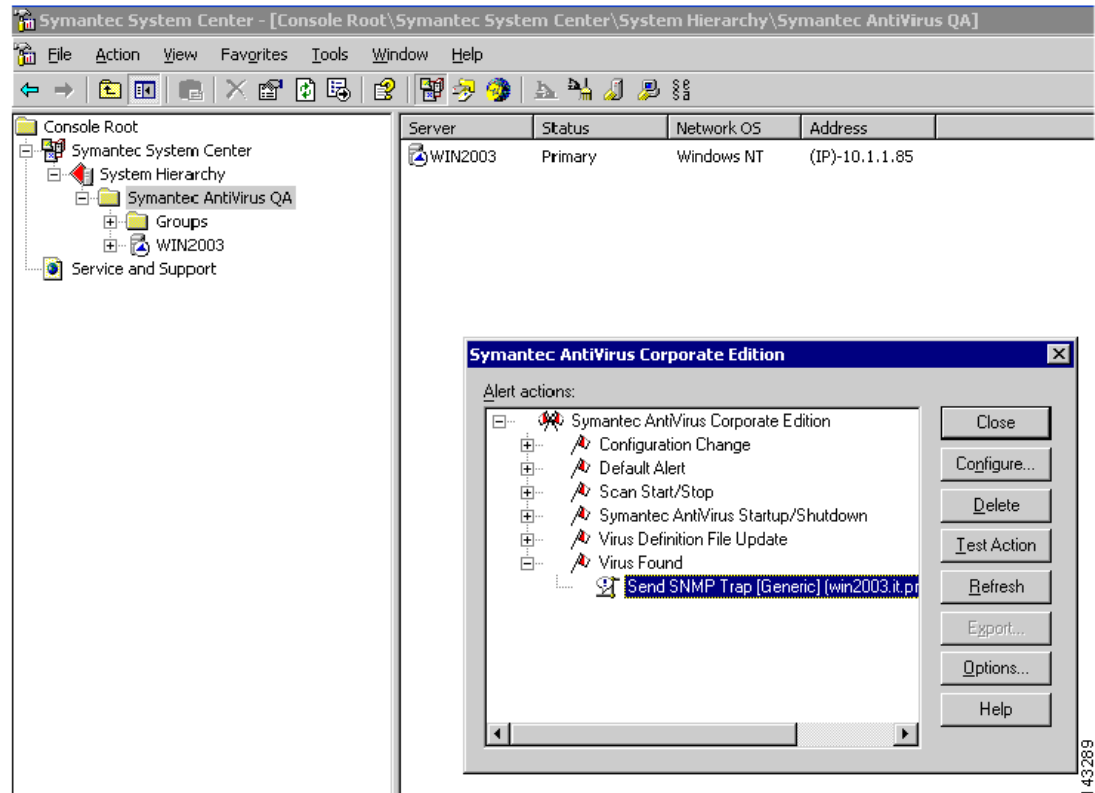
Figure 29-2 Symantec AV AMS



143286

Step 8 Select **Send SNMP Trap** under each Alert Action, then click **Configure**.

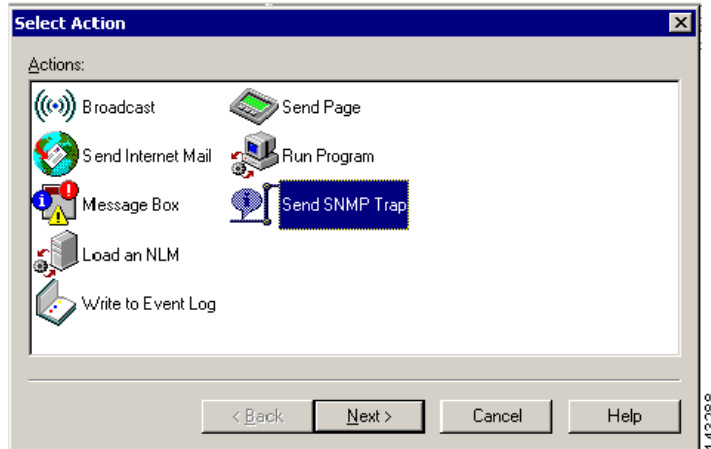
Figure 29-3 Symantec AV Trap



143289

Step 9 Click **Send SNMP trap**, and then click **Next**.

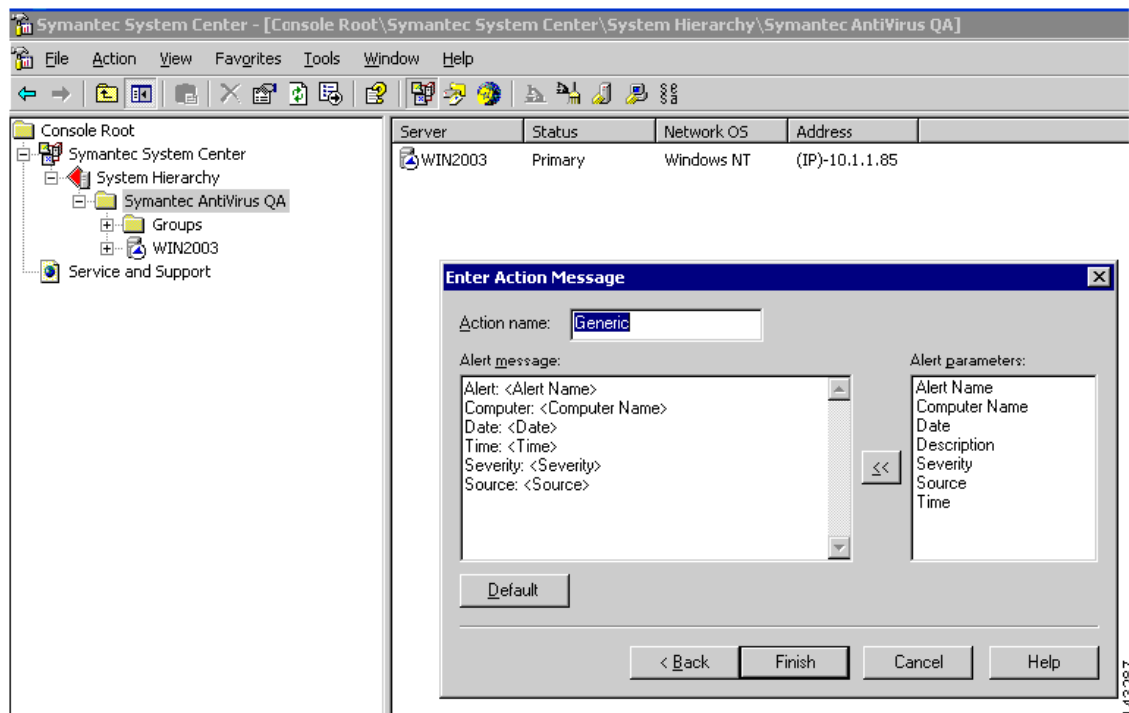
Figure 29-4 Symantec AV Send SNMP Trap



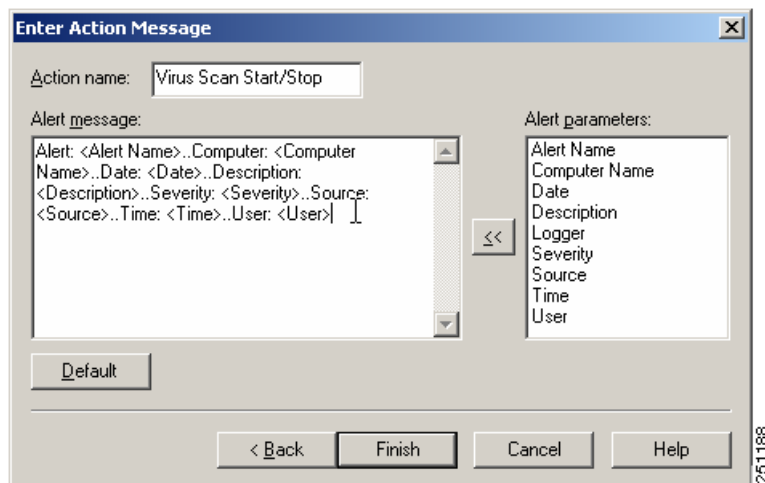
Step 10 Select the Local Controller to send the SNMP trap to as defined in [Step 3](#), and then click **Next** to view the Action Message window.

Step 11 Add alert parameters to the Alert message list according to the following information:

Figure 29-5 Symantec AV Action Msg



The following mandatory fields are required for MARS to parse AV traps. If these fields are among those possible, you must define these fields in order before defining any of the optional fields.



Note For MARS Appliance models 25, 55, 110, 210, and GC2, do not include a CR/LF (Enter key) in the action message.

- Alert: *<Alert Name >*
- Computer: *<Computer Name >*
- Date: *<Date >*
- Time: *<Time >*
- Action: *<Actual Action >*
- Description: *<Description >*



Note This ordering is required is because some optional fields can be so long as to prevent Mars from correctly parsing the mandatory fields if they do not appear first in the list of attributes.

The following optional fields can be defined after all mandatory fields are defined:

- User: *<User >*
- Virus Name: *<Virus Name >*
- File Path: *<File Path >*
- Severity: *<Severity >*
- Source: *<Source >*

The following list identifies the trap type and the full list of possible fields:

Alert: Virus Found

- Alert: *<Alert Name >*
- Computer: *<Computer Name >*
- Date: *<Date >*
- Time: *<Time >*
- Action: *<Actual Action >*

- Severity: <Severity >
- Source: <Source >
- File Path: <File Path >
- Logger: <Logger >
- Requested Action: < Requested Action >
- User: <User >
- Virus Name: <Virus Name >

Alert: Virus Definition File Update

- Alert: <Alert Name >
- Computer: <Computer Name >
- Date: <Date >
- Time: <Time >
- Description: <Description >
- Severity: <Severity >
- Source: <Source >

Alert: Symantec AntiVirus Startup/Shutdown

- Alert: <Alert Name >
- Computer: <Computer Name >
- Date: <Date >
- Time: <Time >
- Description: <Description >
- Severity: <Severity >
- Source: <Source >

Alert: Scan Start/Stop

- Alert: <Alert Name >
- Computer: <Computer Name >
- Date: <Date >
- Time: <Time >
- Severity: <Severity >
- Source: <Source >
- Source: <Source >
- Logger: <Logger >
- User: <User >

Alert: Scan Start/Stop

- Alert: <Alert Name >
- Computer: <Computer Name >
- Date: <Date >
- Time: <Time >

- Description: *<Description >*
- Severity: *<Severity >*
- Source: *<Source >*
- Logger: *<Logger >*

Alert: Default Alert

- Alert: *<Alert Name >*
- Computer: *<Computer Name >*
- Date: *<Date >*
- Time: *<Time >*
- Severity: *<Severity >*
- Source: *<Source >*
- Failed Alert: *<Failed Alert >*

Alert: Configuration Change

- Alert: *<Alert Name >*
- Computer: *<Computer Name >*
- Date: *<Date >*
- Time: *<Time >*
- Severity: *<Severity >*
- Source: *<Source >*
- Failed Alert: *<Failed Alert >*

Alert: Configuration Change

- Alert: *<Alert Name >*
- Computer: *<Computer Name >*
- Date: *<Date >*
- Time: *<Time >*
- Description: *<Description >*
- Severity: *<Severity >*
- Source: *<Source >*

Step 12 Repeat [Step 8](#) through [Step 11](#) for each alert event.

Export the AntiVirus Agent List

While MARS discovers the list of antivirus agents that report to the Symantec System Center console automatically, you can export the list of Symantec AntiVirus Clients and Agents as a CSV file (*.csv), which enables you to use the CSV file to manually load the agents into MARS. For more information on adding agents from the file, [Add Agents from a CSV File, page 29-9](#). This approach is much faster than if you had to identify the agents manually.

To generate the CSV file, follow these steps:

-
- Step 1** Select **View > Default Console View** to ensure the generated CSV file will be based on the Console Default View.
- Step 2** Right-click the name of the server that you want to export, choose **Export List**, and save it as Text (Comma Delimited) (*.csv) file.
- Step 3** Copy the file to an FTP server that the MARS Appliance can access.
- You will use this file when you add the AntiVirus agents within the web interface.
-

Add the Device to MARS

Before you can identify the agents, you must add the Symantec System Center console to MARS. All AntiVirus agents forward notifications to the Symantec System Center console, and the Symantec System Center console forwards SNMP notifications to MARS. Once you define the Symantec System Center console and activate the device, MARS can discover the agents that are managed by that Symantec System Center console. However, you can also choose to manually add the agents.



Tip

For Symantec AntiVirus, the Symantec agent hostname (AV client computer name) appears in the "Reported User" column of the event data. Therefore, you can define a query, report or rule related to this agent based on the "Reported User" value.

To add the host and application configuration information, follow these steps:

-
- Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.
- Step 3** To add a new host, enter the device name and IP addresses.
- Step 4** Click **Apply**.
- Step 5** Click the **Reporting Applications** tab.
- Step 6** From the Select Application list, select one of the following values:
- **Symantec AntiVirus 9.x**
 - **Symantec AntiVirus 10.x**
- Step 7** Click **Add**, then add the agents.
- Step 8** Done one of the following:
- To save your changes and allow the AntiVirus agents to be discovered automatically, click **Submit**, and then click **Done**.
 - To add agents using an exported seed file, continue with [Add Agents from a CSV File, page 29-9](#).
 - To add a single agent manually, continue with [Add Agent Manually, page 29-9](#).
-

Add Agent Manually

MARS can automatically discover agents or you can manually add them one at a time or in bulk using a CSV file (see [Add Agents from a CSV File, page 29-9](#).) This topic explains how to manually add a single agent. The value of defining an agent is that it accelerates the discover process; however, it is not required.

To add an agent manually, follow these steps:

-
- Step 1** Click **Add Agent**.
- Step 2** Select the existing device or click **Add New**.
- Step 3** Enter the following information for new device.
- **Device Name**—The DNS entry for this device.
 - **Reporting IP**—The IP address that the agent uses to send logs to the console.
- Step 4** Under the Interfaces list, specify the IP address and netmask values associated with each interface installed in the host on which the agent is running.
- MARS uses interface information to calculate attack paths.
- Step 5** Click **Submit**.
-

Add Agents from a CSV File

You can generate a CSV file that contains the list of agents managed by the Symantec AV server as defined in [Export the AntiVirus Agent List, page 29-7](#). Once the file is generated, you can use the file to import the list of agents into the MARS web interface as child modules of the Symantec AV server.



Note Other population options exist: MARS can automatically discover agents (default) or you can manually add them one at a time (see [Add Agent Manually, page 29-9](#).)

To import the list of AV agents into MARS, follow these steps:

-
- Step 1** Click **Load From CSV**.
- Step 2** Enter the FTP server information and location of the CSV (comma-separated values) file.
- Step 3** Click **Submit**.
-

■ Add the Device to MARS