



# Using Event Correlation

---

## Overview

Management Center for Cisco Security Agents provides rule modules and individual rules you can add to your policies that allow CSA MC to categorize processes and correlate events across multiple systems. When these rules are triggered by one or more system actions across a network, the MC registers this occurrence and automatically builds application classes and sends out new process categories to Cisco Security Agents. In some cases, the MC can prevent actions from executing on any additional systems. The Cisco Security Agent also uses heuristics to detect and terminate suspicious activities on systems, such as buffer overflows and password stealing attempts. These rule types differ from other action control rules in that multiple internal system events must trigger before these rules fire.

Use the rules and rule modules described in this chapter to protect systems just as you would other rules. For details on adding rules modules to policies and attaching policies to groups, refer back to [Chapter 5, “Rule Module Configuration”](#).

This section contains the following topics.

- [Event Correlation and Heuristics, page 7-2](#)
- [Email Worm Protection Rule Module, page 7-3](#)
- [Installation Applications Policy, page 7-4](#)
- [Global Events, page 7-5](#)
- [Correlation, page 7-6](#)

# Event Correlation and Heuristics

The Network shield rule which controls SYN flood protection and port scan detection and the System API control rule are some examples of preconfigured rules you can add to your modules in the same way you add other rules. These are basic system hardening, event correlation, and heuristic features that should be applied in most cases. Some are used in the General Applications Permissions module shown in [Figure 7-1](#).

**Figure 7-1** General Applications Permissions Module

The screenshot shows the Management Center for Cisco Security Agents V5.0 interface. The breadcrumb navigation is: Configuration > Rule Modules > Windows Rule Modules > General Application Permissions - all Security Levels [V5.0 r112] > Rules. The page title is "Management Center for Cisco Security Agents V5.0".

Below the navigation, there is a "View All rules" link and a status bar showing "Rules: 10 [10 enforce, 0 detect]". The main content is a table of rules:

ID	Type	Events (Last 24hr)	Status	Action	Log	Description
887	System API control		Enabled	?	☑	Network Applications, Access system functions from a buffer
884	System API control	5 (0)	Enabled	?	☑	All Applications, Write memory owned by other applications
885	System API control		Enabled	?	☑	All Applications, Trap keystrokes
886	System API control	10 (0)	Enabled	?	☑	All Applications, Downloading and invoking ActiveX Controls
888	System API control		Enabled	?	☑	All Applications, Monitor media devices
889	System API control	9 (0)	Enabled	?	☑	Applications processing untrusted content and Network Servers, Invoke unusual system calls
891	System API control		Enabled	?	☑	Applications processing untrusted content, Inject code into other applications
882	File access control		Enabled	?	☑	Applications processing untrusted content, read MS Script Runtime (providing scripts access to the file system)
883	File access control		Enabled	?	☑	NT Virtual DOS Machine, read executables on Removable Media
890	Application control	2 (0)	Enabled	?	☑	All applications, invoke executables on Removable Media

At the bottom of the table, there is an "Add rule" button and a "Copy" button. Below the table, there are "Delete", "Enable", and "Disable" buttons. A status bar at the bottom indicates "1 rule change pending" and "Generate rules". The user is logged in as "debbi".

148281

## Email Worm Protection Rule Module

Email worms are some of the most commonly spread and costly attacks affecting corporate networks today. Some well-known worms of the past include Mydoom, Anna Kournikova, and variations thereof. These worms easily infected systems, passing undetected through most security software until virus scanner vendors provided updates to detect these virus signatures. Even with this detection capability, if the worm is modified in any way, it is again undetectable by virus scanners.

When a worm of this type is received through email and executed by unsuspecting users, it generally attempts to send copies of itself to all entries in the email address book of the user. In doing this, the worm modifies registry keys, writes its own script files, and modifies existing files. This makes file recovery difficult and it can cause users to invoke the virus again when they attempt to open these infected files.

The Cisco Security Agent ships with a preconfigured email worm protection rule module. You must have this module deployed to take advantage of email worm network event correlation and quarantine capabilities.

The email worm protection module works through a combination of steps including dynamically building an application class through the detection of a suspicious action occurring on a system. If this suspicious action detection is seen by the MC as occurring on more than one system, a quarantine of the detected malicious process will also occur.

More specifically, it is through two sets of rule types that the detection and tagging of a virus or email worm occurs. In fact, these rules can be used more widely to identify and stop any type of virus, not only email. Although, this does require some different parameters to be set in the first group of rules.

The email worm protection rule module works this way:

- The first set of rules are written to deny or terminate processes or to query the user when a set of actions are attempted. Those actions are something along the lines of “a process that downloaded content over the network is now attempting to access an email COM component, such as the address book.” This action is suspicious. It is either denied or terminated or the user is queried about it.
- If the action is denied or terminated (automatically or by the user), the second set of rules tags the offending process and adds the process to the dynamically built “Suspected Virus Applications” class. Once a process is in this class,

other rules prevent all processes that are dynamically added to this class from accessing any resources on a system. If these processes are seen on more than one system, it also quarantines the processes in question. See [Global Events, page 7-5](#) for quarantine details.

The methodology used in the email protection module can be applied to any virus type you're protecting against. By altering the parameters of the first rule set (in this example, downloaded content accessing the COM component for the email application address book) you can configure parameters to categorize any process as suspicious and subsequently stop any type of errant action.

## Email Worm Event Correlation

If you select one of the options to add dynamically quarantined files to the list in the Global Event Correlation page (see [Correlation, page 7-6](#)), when a worm is detected, other agents will be notified to prevent the spread of this virus. Under these circumstances, the agent(s) report the file name the worm was written into. If at least two agents report worms writing to the same file name within an hour, the file is added to a dynamic list (@dynamic) of quarantined files. If you have a rule configured to stop dynamically quarantined files in a deployed policy, no further agents can open the contaminated file during the quarantine time frame. See also, [page 6-23](#) for information on using @dynamic in File access control rules.

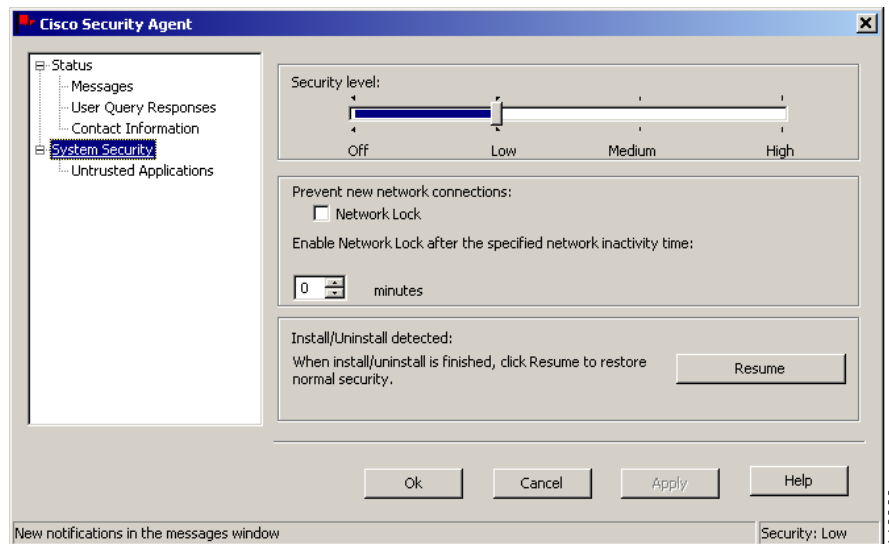
## Installation Applications Policy

There is a preconfigured policy that you can apply to systems to detect when a software installation occurs and to add the install process or processes to a dynamically built application class. If dynamic tagging occurs, another set of rules would apply to the install processes added to this dynamic class. You may need to use this installation detection rule module in order to enforce a less strict set of rules to the system while an approved software installation is occurring. Under normal conditions, other rules on the system may prevent the install from occurring.

The built-in dynamic application class in question is called "Installation Applications." The rule module may build this application class under the following circumstances: A set of rules determines that setup.exe is detected on a system and it is added to the dynamic built-in Installation Applications class. As a result, a System State installation condition is triggered (see [System State Sets](#),

page 5-13) and a new policy is applied to the system. The system should automatically return to its original policy when the install exits. If this does not occur, the user can manually indicate when the installation is complete (a Resume button, see Figure 7-2, is made available if the end user has an agent UI) and return the system to the initial stricter policy. The installation state may also time out and the system then automatically returns to its initial policy.

**Figure 7-2 Agent UI Resume Button**



148283

## Global Events

The Management Center for Cisco Security Agents lets you enable correlation functions for particular types of events. In each case, you must have a corresponding rule enabled in a policy for the global event correlation to take place. If you do not enable global event correlation, individual events are logged by system agents but similar events across multiple agents are not correlated by the central CSA MC.

# Correlation

The **Event Correlation** page, accessible from the menu bar as follows **Configuration>Global Event Correlation** (see [Figure 7-3](#)), provides the following capabilities:

- Correlate network scans

With this checkbox enabled, correlated port scans and ping scans across multiple agent systems are logged separately as a correlated event in addition to the individual port scan and ping scan events that continue to be logged.

Note that you must have a Network shield rule with Port scan detection and Ping scan enabled in a policy deployed to the agent(s) in question for these event types to be detected and logged.

The threshold and time frame for correlating network scans are values you can configure.

- Correlate events received from operating system event logs and generate a summary event
  - Log individual events in addition to summary event

With this checkbox enabled, events from multiple systems are correlated based on the NT event code, NT event severity, NT event source, and NT event log type. If 2 systems log the same NT event type within 30 minutes, a correlated summary event is logged.

Note that you must have an NT event log rule in a policy deployed to the agent(s) in question for these events to be uploaded to the CSA MC log.

If you do not enable this checkbox, NT event correlation does not take place, but individual NT events are logged in accordance with the NT event log rule you have configured.



---

**Note**

In this case, there is an additional checkbox (Log individual events in addition to summary events) to control whether the individual events are logged in addition to the summary event. If you do not enable this checkbox, but you do enable the Correlate events checkbox, only correlated summary events will log, NOT individual events. This can be useful if NT event log messages are filling up your CSA MC logfile.

---

- Correlate suspected virus application events and add contaminated files to list of dynamically quarantined files

With this checkbox enabled, when processes are added to the dynamic <Suspected Virus Applications> application class (see [Built-in Configurable Application Classes, page 8-7](#)) and this event is logged across multiple agent systems, these events are correlated and the contaminated file that triggered the event is added to a dynamic list of quarantined files that CSA MC maintains. If you have a rule configured to stop dynamically quarantined files in a deployed policy, no further agents can access the contaminated file. See [page 6-23](#) for information on using @dynamic in File access control rules.

If you do not enable this checkbox, suspected virus correlation does not take place, but individual virus events are logged.

Note that you must have a corresponding policy deployed to the agent(s) in question for these event types to be detected and logged.

- Correlate events received from virus scanners and add contaminated files to list of dynamically quarantined files

With this checkbox enabled, events logged by virus scanners running on agent systems are received and correlated by CSA MC. Contaminated files detected by virus scanners are added to the list of quarantined files. If you have a rule configured to stop access to dynamically quarantined files in a deployed policy, no further agents can receive the contaminated file. See [page 6-23](#) for information on using @dynamic in File access control rules.

**Note**

---

This feature works with Norton, McAfee, and Trend AntiVirus. To receive these virus events, you must have an NT event log rule in a policy deployed to the agent(s) in question for these events to be uploaded to the CSA MC logfile. In the NT event log rule, you must enter the name of the antivirus software in the Event Source field. See [NT Event Log, page 6-58](#) for details.

---

The threshold and time frame for correlating events received from virus scanners are values you can configure.

**Note**


---

To view the files that are added to the dynamically quarantined files list, click the numbered link beside **dynamically quarantined files**. It takes you to the pertinent event log messages. Read the messages there to locate the names of quarantined files. You can also click the **Manage dynamically quarantined files** link at the bottom of the page.

---

- Correlate communications with untrusted hosts and add peer addresses to list of dynamically quarantined IP addresses.

With this checkbox enabled, when the "Set" action is used in a rule to mark a host address as Untrusted (globally) (see [Using the Set Action, page 5-44](#)) and this event is logged across multiple agent systems, these events are correlated and the untrusted peer address that triggered the event is added to a dynamic list of quarantined IP addresses that CSA MC maintains. If you have a rule configured to stop dynamically quarantined IP addresses in a deployed policy, no further agents can communicate with this peer address. See [page 6-28](#) for information on using @dynamic in Network access control rules.

If you do not enable this checkbox, untrusted host correlation does not take place, but individual untrusted host events are logged.

**Note**


---

You must have a corresponding policy deployed to the agent(s) in question for these event types to be detected and logged.

---

**Note**


---

To view the IP addresses that are added to the dynamically quarantined addresses list, click the numbered link beside **dynamically quarantined IP Addresses**. It takes you to the pertinent event log messages. Read the messages there to locate the quarantined IP addresses. You can also click the **Manage dynamically quarantined IP addresses** link at the bottom of the page.

---

## Manage Dynamically Quarantined Files and IP Addresses

You can use the @dynamic token in the File set text field and in the Network address set text field where they are available in rules to control access to files and addresses that have been quarantined by CSA MC. Files are quarantined as a

result of suspected virus application events, correlated virus scanner log messages, or files that were added manually. This list updates automatically (dynamically) as logged quarantined files are received. Addresses are quarantined as a result of communication with a suspected untrusted host (this updates dynamically) or by being added manually.

To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the **Manage dynamically quarantined files** link on the Global Event Correlation page. See [Figure 7-4](#). Add and Remove files from this list using the provided buttons on the bottom of the window that appears.

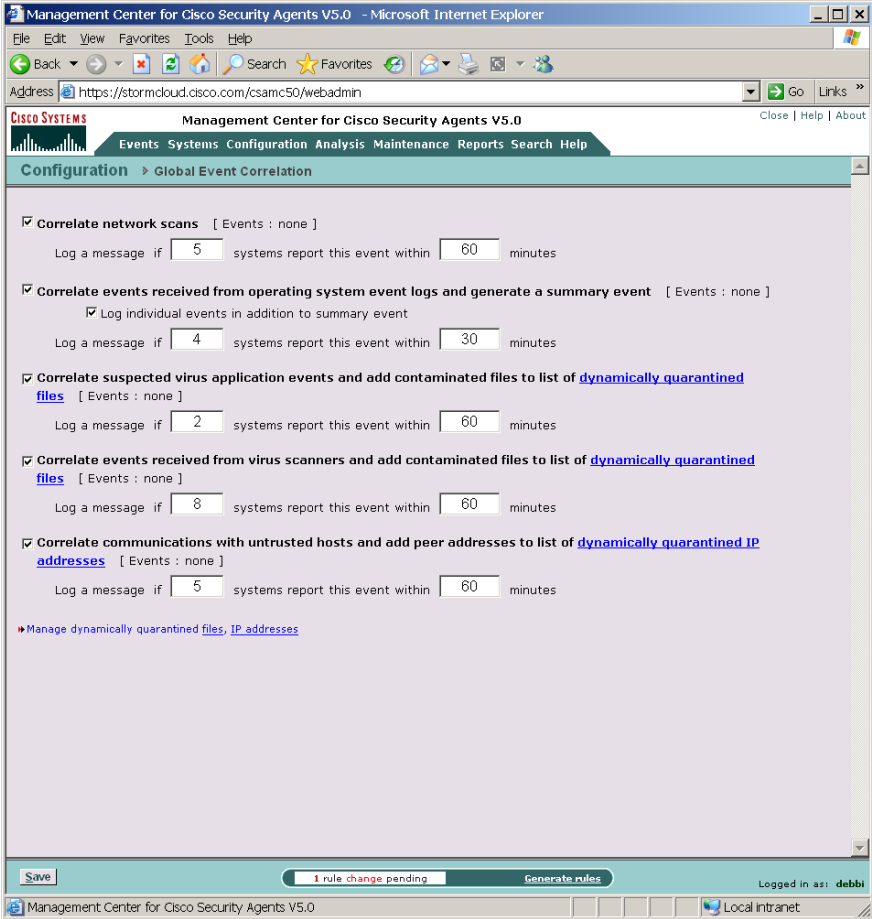
To view the addresses that are added to the dynamically quarantined IP addresses list and to manually add addresses to be quarantined, click the **Manage dynamically quarantined IP addresses** link on the Global Event Correlation page. Add and Remove IP addresses from this list using the provided buttons on the bottom of the window that appears. See [Figure 7-5](#). The “Source” column in this window describes how the address was added to the list (manually by the administrator or through a correlation event).

Changes made to the quarantined file and IP address lists are not received by agents until they next poll in to the management center. You can send a hint message to hosts to poll in sooner than the set interval. See [Configuring Groups, page 3-4](#) for poll hint details.

### Fidelity Ratings

When you click the Manage dynamically quarantined files and IP addresses links, items that are not added manually by the administrator, but are added automatically through event correlation will have a “high” or a “low” fidelity rating. This rating indicates the “danger” likelihood of the item that has been quarantined. This rating is based on the detected file type and the network protocol involved.

Figure 7-3 Global Event Correlation Page



148286

Figure 7-4 Quarantine Files Window

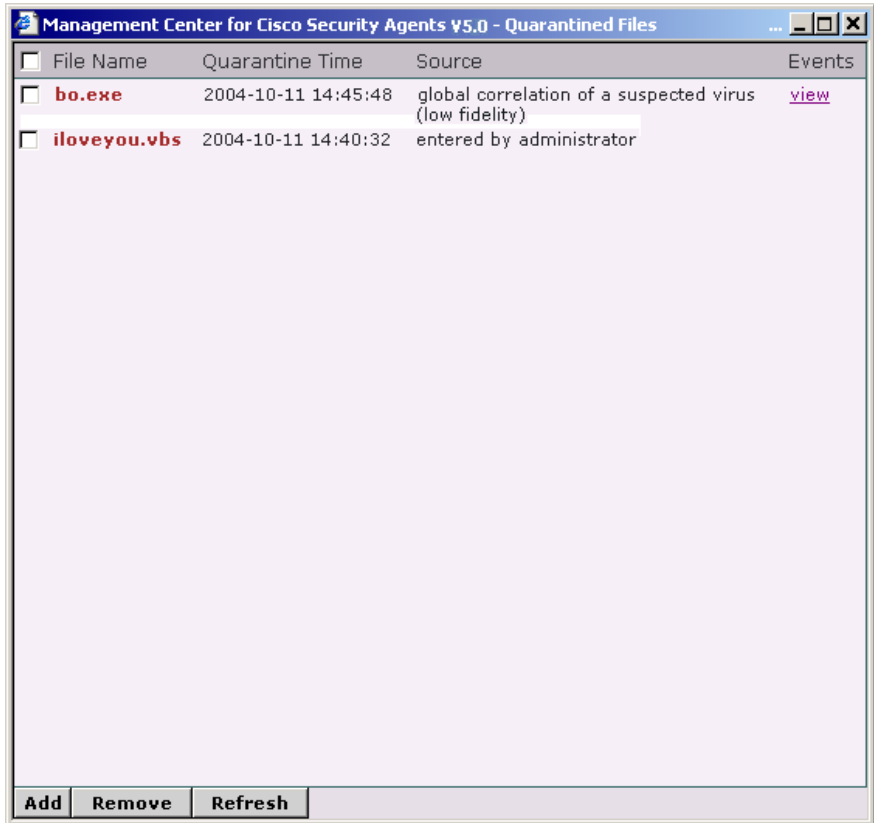


Figure 7-5 Quarantine IP Addresses Window

IP Address	Quarantine Time	Source	Events
<a href="#">144.254.230.132</a>	2005-09-22 18:17:02	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">161.44.122.35</a>	2005-09-22 18:17:02	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">161.44.181.20</a>	2005-09-22 17:24:01	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">206.24.222.126</a>	2005-09-22 17:23:56	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">207.68.172.234</a>	2005-09-22 17:23:56	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">207.68.177.126</a>	2005-09-22 17:23:56	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>
<a href="#">65.54.195.188</a>	2005-09-22 17:23:56	global correlation of an untrusted address (low fidelity)	<a href="#">view</a>

At the bottom of the window, there are buttons for **Add**, **Remove**, and **Refresh**.

148285