



# CHAPTER 13

## Using Cisco Security Agent Analysis

---

### What is Analysis

Cisco Security Agent Analysis functionality works with CSA MC and the agent, serving as a data collection and behavior analysis tool for administrators who are deploying policies across systems and networks.

This section contains the following topics.

- [What is Analysis, page 13-1](#)
- [The Application Deployment Investigation Process, page 13-3](#)
- [Reporting Categories, page 13-3](#)
- [Turning Application Deployment Investigation On, page 13-4](#)
- [Configure Group Settings, page 13-4](#)
- [Configure Product Associations, page 13-7](#)
- [Associate Unknown Applications, page 13-12](#)
- [About Data Management, page 13-14](#)
- [Generating Application Deployment Reports, page 13-16](#)
- [AntiVirus Installations Report, page 13-17](#)
- [Installed Products Report, page 13-20](#)

- [Unprotected Hosts Report, page 13-23](#)
- [Unprotected Products Report, page 13-25](#)
- [Product Usage Report, page 13-27](#)
- [Network Data Flows Report, page 13-30](#)
- [Network Server Applications Report, page 13-34](#)
- [Viewing Reports, page 13-37](#)
- [Exporting Reports, page 13-38](#)
- [What is Application Behavior Investigation, page 13-38](#)
- [How Application Behavior Investigation Works, page 13-39](#)
- [The Application Behavior Investigation Process, page 13-39](#)
- [Behavior Analyses, page 13-40](#)
- [Creating, Saving, and Cancelling Analysis Data, page 13-40](#)
- [Configure a Behavior Analysis Investigation, page 13-43](#)
- [Start Behavior Analysis, page 13-48](#)
- [Importing the Rule Module, page 13-49](#)
- [Application Behavior Reports, page 13-51](#)
- [Report Components, page 13-52](#)
- [Working with Reports, page 13-56](#)
- [The Behavior Analysis Rule Module, page 13-57](#)
- [Behavior Analysis Methodology, page 13-57](#)
- [Reviewing the Rule Module, page 13-57](#)

The rules that comprise policies are aimed at protecting your enterprise resources, knowing exactly what those resources are and how they are used is essential to deploying effective policies.

With Application Deployment Investigation:

- You can see what applications are running on systems and determine what their usage patterns are.
- You can see what applications are installed but remain largely unused on systems.
- You can see what applications are accessing critical network resources.

- Use collected data to accurately deploy policies or to generate new policies for unprotected applications using the Cisco Security Agent.

## The Application Deployment Investigation Process

Deployment Investigation is a part of the Management Center for Cisco Security Agents and requires no separate installation process and very little configuration. As previously mentioned, the analysis data collection process is controlled on a per group basis. Application Deployment Investigation is either turned on or off for a group. The investigation process does not affect any policies that are attached to the group in question.

**Note**

---

All agent functionality, including enforced security policies, operate normally when tracking is taking place on an agent host.

---

## Reporting Categories

Application Deployment Investigation is mainly comprised of the reporting capabilities it provides once all the data is collected. You can organize the gathered data in various manners to provide information on how your enterprise operates, the resources that are accessed, resource and application usage time frames, and a great deal more. In turn, this data can inform the crafting of your policies while you create a more secure environment for all your users to operate within.

While you cannot configure what types of information you collect using deployment investigation (it gathers all usage information while it is enabled), you can organize the information that is gathered in various ways.

- You can generate reports to display the list of software products installed across your enterprise. Of those products, you can view which are being used and which are not. You can sort reports by application network usage. This could include usage time frames, client and/or server connections, and the applications that are accessing the network. Of the information types you gather, you can use reports to cross-reference this data to distill even more specific reports such as one which displays what applications are running unprotected (without a policy) on systems

# Turning Application Deployment Investigation On

**Note**

Application Deployment Investigation is only supported on Windows platforms.

**Note**

By default, Application Deployment Investigation is disabled for all Windows groups until you enable it.

## Configure Group Settings

Deployment Investigation is controlled on a per group basis and it is enabled or disabled using the **Analysis>Application Deployment Investigation>Group Settings** page.

**Caution**

If deployment investigation is enabled for the group, it begins on all hosts in the group in question after you generate rules and the hosts next poll in to CSA MC.

**Note**

If you want to enable Application Deployment Investigation for only one host, you must create a new group with Application Deployment Investigation enabled and add the host to that group. If a host belongs to multiple groups, having Application Deployment Investigation enabled, if present in any group for which the host is a member, takes precedence over not having it enabled. Once Application Deployment Investigation is enabled for a group, it continues to collect data until you disable it and generate rules.

To configure group settings for Application Deployment Investigation, do the following.

- Step 1** Move the mouse over **Analysis>Application Deployment Investigation** in the menu bar and select **Group Settings** from the drop-down list that appears.
- Step 2** Click the **New** button to create a new group setting. See [Figure 13-2](#).
- Step 3** In the available group setting fields, enter the following information:

- **Name**—This is a unique name for this group setting. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, hyphens -, and underscores \_ .
- **Description**—This is a useful line of text that is displayed in the list view and helps you to identify this particular group setting.

**Step 4** Configuration Analysis Application Deployment Investigation enable options. Click the **Enable Application Deployment Investigation** checkbox and select one of the following radio button options:

- Product data collection - which would apply to the following reports:  
AntiVirus Installations, Installed Products, Unprotected Products, Product Usage
- Product and network data collection - which would apply to the following additional report:  
Network Server Applications
- Product and verbose network data collection - which would apply to the following additional reports:  
Unprotected Hosts, Network Data Flows

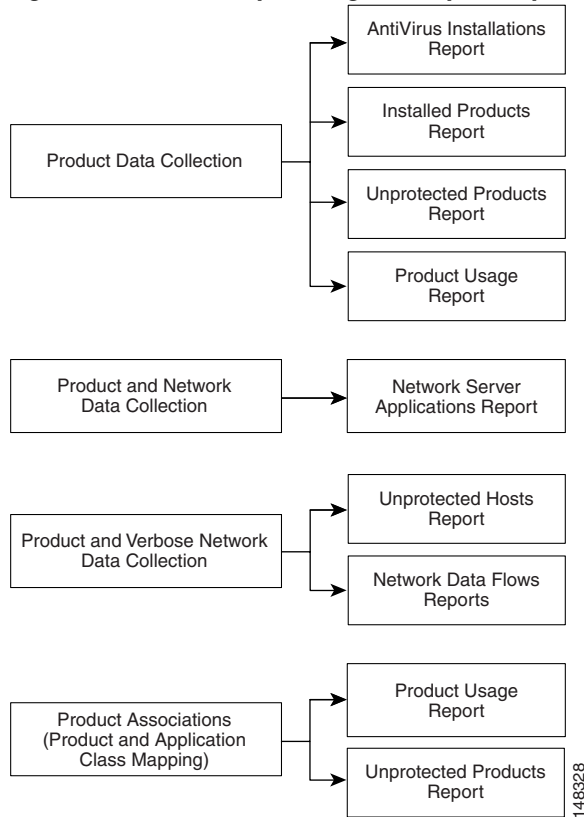
**Caution**

---

For Deployment Investigation to function properly, you must not exceed the following limits: The total number of agents with Application Deployment Investigation enabled should not exceed 100,000; The total number of agents with Application Deployment Investigation enabled in non-verbose network mode should not exceed 10,000; The total number of agents with Application Deployment Investigation enabled in verbose network mode should not exceed 1,000.

---

The following diagram illustrates which radio buttons must be selected for which report types:

**Figure 13-1 Group Setting and Report Dependencies**

It is recommended that you choose lowest verbosity level available in reports whenever possible to keep the volume of network data collection manageable.

Also, enter an **Upload Interval** time for agent to send collected data to the MC. The default and minimum interval is 24 hours.

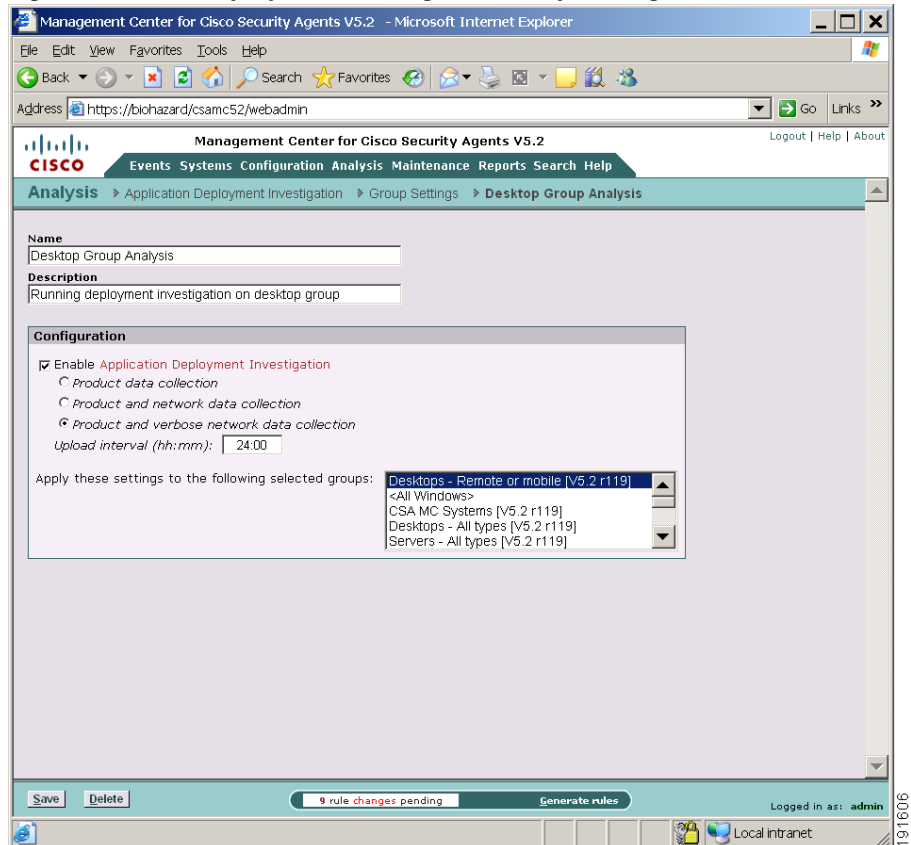
**Note**

The uploading of data occurs at the end of the interval in question. Therefore, it may take more than one interval receive collected data. It depends upon when the hosts polls into the MC.

**Step 5** In the **Apply these settings to the following selected groups** list box, select one or more groups for data collection.

- Step 6** Click the **Save** button when your group setting configuration is finished. Deployment investigation begins on all hosts in the group in question after you generate rules and the hosts next poll in to CSA MC.

**Figure 13-2** Deployment Investigation Group Settings



## Configure Product Associations

You can use Application Deployment Investigation to generate reports that use installed software products as part of the report criteria. In order to do this, there is some prerequisite configuration. This is necessary because the deployment

investigation process, in part, gathers data on systems according to the application name it finds. That is the application executable itself and not the product with which the application is associated. Application Deployment Investigation does gather information on the products that are installed on systems, but it does not then map the applications back to the installed products. For example, Application Deployment Investigation may find that excel.exe is running on a system. It may also find that Microsoft Office is installed on that same system. But it will not know that excel.exe is part of Microsoft Office. You must tell it so.

Therefore, in order to generate certain reports types using installed product information, you must first associate the installed products found by Application Deployment Investigation with the application(s) that comprise the product. (This could entail creating new application classes for this purpose.)

You must make this application class/product association to use product criteria to generate the following report type:

- Product Usage




---

**Caution**

Pre-configured application classes that ship with CSA MC are not available to Application Deployment Investigation functionality. It is recommended that you configure application classes that are separate and solely for the purpose of Analysis reports and investigation. This way, you are not compromising existing application classes that are used in CSA MC security policies.

---

To create application class/product associations, after Application Deployment Investigation has collected data, do the following.

---

**Step 1** Move the mouse over **Analysis** in the menu bar of CSA MC and select **Application Deployment Investigation>Product Associations**.

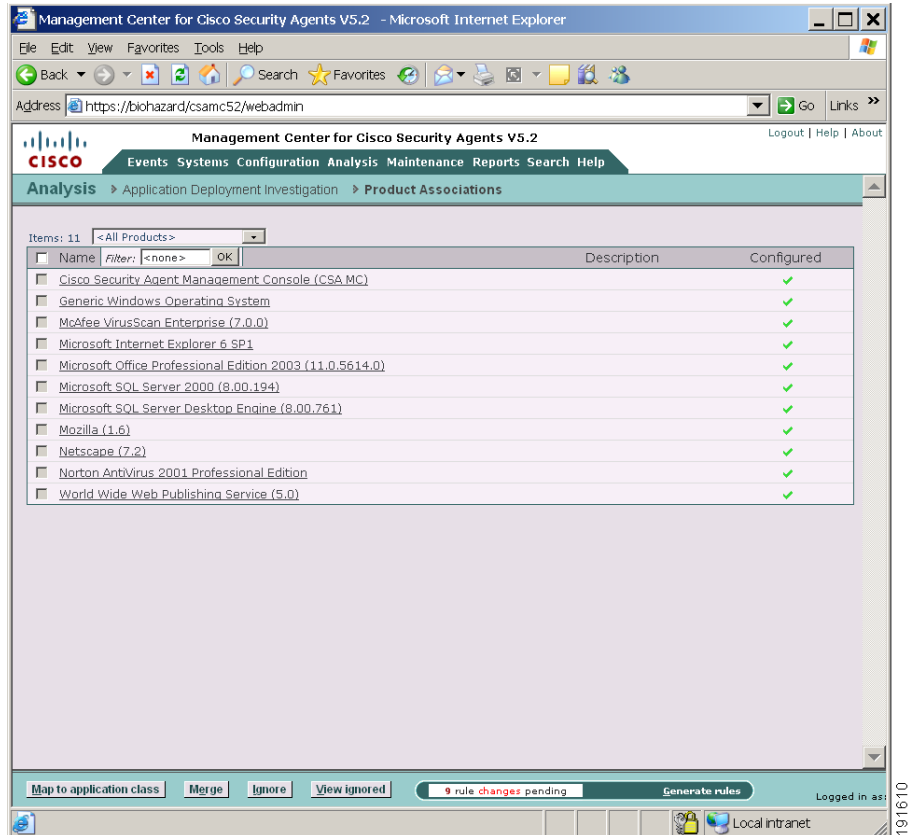
The deployment investigation Products page contains a list of all the installed products (not applications) found on systems that were investigated. See [Figure 13-3](#). These are the products names that would be viewable through the Microsoft Add/Remove Programs window.

**Step 2** To associate a product with an application, click the product in the Product Associations window. This takes you to a window which allows you to select an application class or classes that will define the product.

You can also associate a product with an application by selecting the checkbox beside the product name link and clicking the **Map to application class** button. This opens a new window which allows you to select an application class that will define the product. You can map the product to an existing or new application class.

- Step 3** Click **Save** once you selected an application class(es).
- Step 4** Optionally, select a product and use the **Ignore** button to have that product be “ignored” and not appear in reports. You can undo an ignore setting by clicking the **View ignored** button to launch a new window which allows you to “restore” the product in question.

Figure 13-3 Product Association List Window

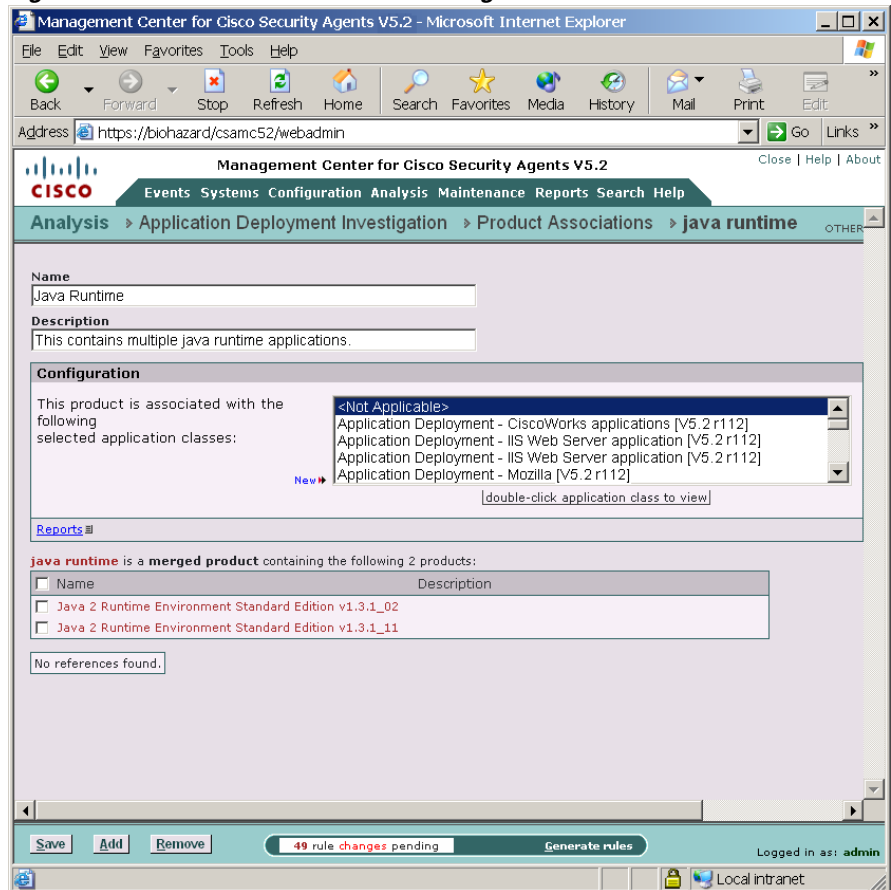


**Step 5** Optionally, you can use the **Merge** button to combine multiple unmapped products into one merged product. For example, you may have several “hotfix” items in your product list. You can put them all into one “Microsoft Hot Fixes” product category using the merge feature.

To merge products, select the checkboxes of the products you want to combine and click the **Merge** button. This takes you to a window which allows you to create a new name for the merged products. See [Figure 13-4](#).

Once you merge products, they will no longer appear as separate items in your product list.

Figure 13-4 Product Association Merge Window



The Product Associations merge window allows you to enter a name for the new merged products. You can also use the **Add** and **Remove** buttons on this page to add more products to the merge or to remove one or more products from the merge.



#### Note

You can also use the shortcut **Reports** link on the merge page to view the Installed Products and Product Usage reports for the product named on the page you're on.

## Associate Unknown Applications

This window displays a list of applications (processes) that have run on systems but have no product associated with them. (This is the inverse of the Application Deployment Investigation Product Associations page.)

You can use Application Deployment Investigation to generate reports that use installed software products as part of the report criteria. In order to do this, there is some prerequisite configuration.

This is necessary because the investigation process, in part, gathers data on systems according to the application name it finds. That is the application executable itself and not the product with which the application is associated. Application Deployment Investigation does gather information on the products that are installed on systems, but it does not then map the applications back to the installed products. For example, it may find that excel.exe is running on a system. It may also find that Microsoft Office is installed on that same system. But the analysis process will not know that excel.exe is part of Microsoft Office. You must tell it so.

Therefore, in order to generate certain reports types using installed product information, you must first associate the installed products found by the investigation process with the application(s) that comprise the product. (You can also associate a product with an existing application class from the Product Associations page.)

You must make this application/product association to use product criteria to generate the following reports type:

- Product Usage

To create application/product associations, after the data has been collected, do the following.

- 
- Step 1** Move the mouse over **Analysis** in the menu bar of and select **Application Deployment Investigation>Unknown Applications**.
- Step 2** The Unknown Applications window contains a list of all the processes found on systems that were tracked which have no association with an installed product. See [Figure 13-5](#). To associate an application with a process, select the checkbox beside the process name link and click the **Map to product** button. This opens a new window which allows you to select a product that will define the application

process. You can also map the application to an existing or new application class. (Note that you can only map and/or ignore products that have not yet been mapped.)

**Step 3** Click **Save** once you selected a product. The process will then disappear from the Unknown Applications list as it is no longer unknown.

Optionally, select a process and use the **Ignore** button to have that process be “ignored” and not appear in reports. You can undo an ignore setting by clicking the **View ignored** button to launch a new window which allows you to “un-ignore” the process in question.

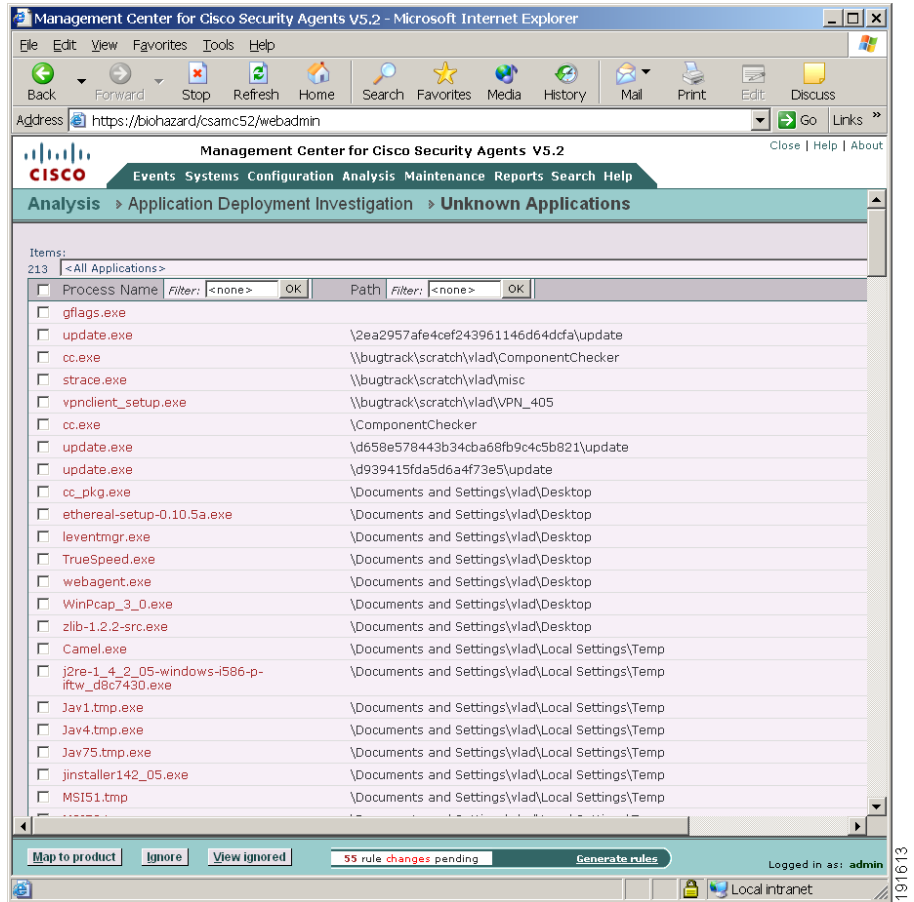
**Note**

---

You can enter text strings into the Filtering fields in this Window to search for particular items. You can also use the pulldown field at the top of the page to find particular paths for applications.

---

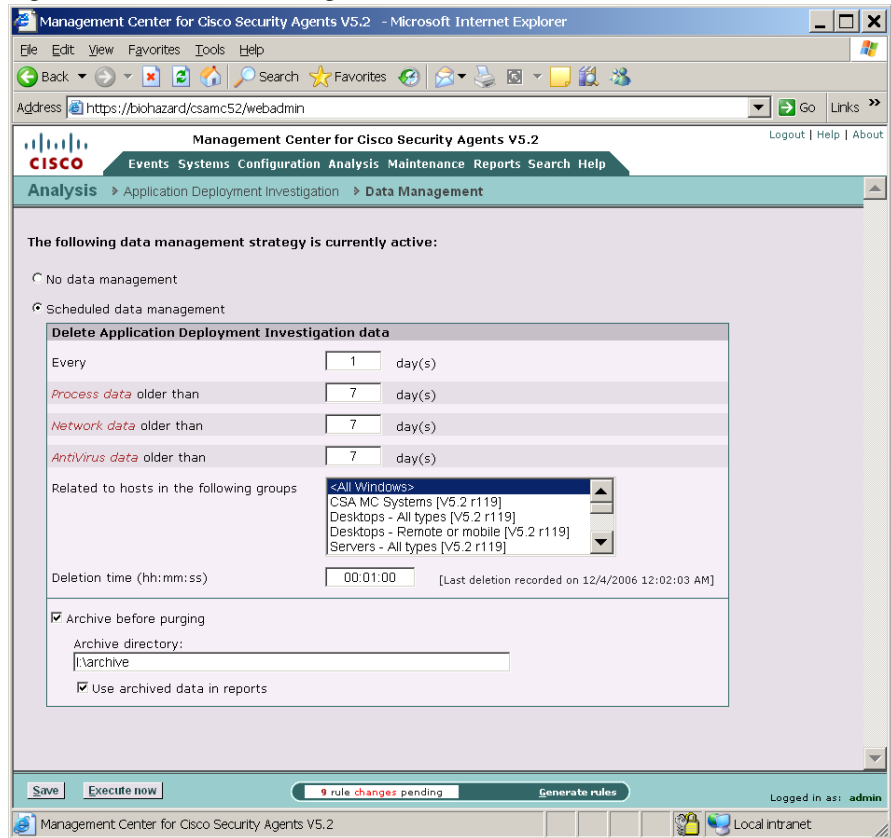
Figure 13-5 Unknown Applications List Window



## About Data Management

Accessible from the **Analysis>Application Deployment Investigation>Data Management** menu, the Data Management window allows you to archive and purge the data collected by the deployment investigation. See [Figure 13-6](#).

Figure 13-6 Data Management Window



Use the Data Management page to purge deployment investigation data at scheduled intervals and to optionally archive the data you are deleting from the active database.

This page gives you the option having no scheduled data management (**No data management** radio button) or setting parameters for a scheduled purging of data (**Scheduled data management** radio button).

You can configure your data management to purge certain types of data at different time intervals as you choose. Process data, Network data, and AntiVirus data can be purged according to the day and time interval you set. Note that AntiVirus data has been added as a separate category due to the large volume of this data type that can accumulate.

If you click the **Execute Now** button, you can trigger data management to occur immediately based on the current configuration, regardless of the data management type you have configured using the available radio buttons.

### Archive before purging



#### Note

---

The Archive feature is only available if the database is local to the CSA MC system.

---

Select the Archive before purging checkbox and enter a directory to store archived data in if you do not want to lose the report data you are purging. You can continue to use this archived data in your reports.



#### Note

---

If you change the Archive directory after you've already archived data, that data is automatically moved to the new directory and new archived data will be stored in the newly specified directory as well.

---



#### Note

---

You can click the **Archive history** link at the top of this page to view an informational list of data purges that have taken place on the system.

---

## Generating Application Deployment Reports

You can generate several different Application Deployment Report types using the data gathered during the tracking process. The following sections describe each of these reports.

You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report. The report opens in a new browser window.

To generate an Application Deployment Report, do the following.

- 
- Step 1** Move the mouse over **Analysis>Application Deployment Reports** in the menu bar.
  - Step 2** A drop-down list and a cascading menu of report types appears. Select a report type from the cascading menu to enter parameters and generate that report.

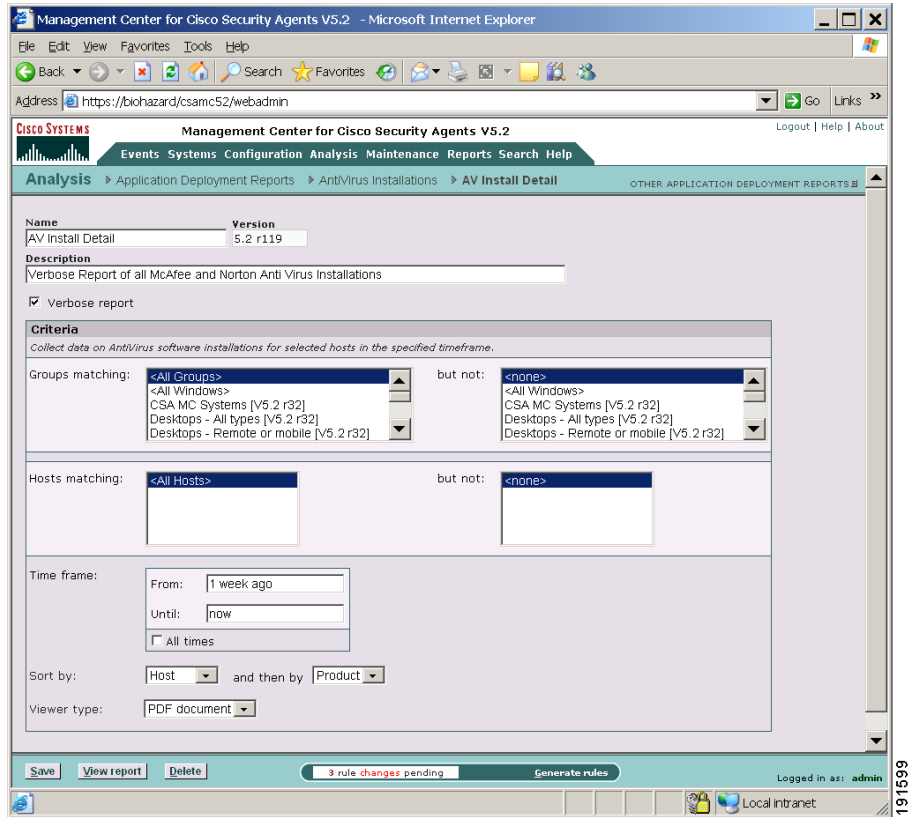
The follow section continues these instructions and describes each type of report.

## AntiVirus Installations Report

Use this report type to view software version and signature version information for detected Norton and McAfee AntiVirus installations. (Note that for McAfee AntiVirus software, you will also see the engine version in the report.) From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **AntiVirus Installations** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-7](#).

Figure 13-7 AntiVirus Installations Report Page



**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information (number of overall installation copies found) for installed antivirus products. If you enable Verbose, you will see a much longer report containing details for installed antivirus products on each host by host name.

AntiVirus Installations non-verbose reports contain the following data:

- AntiVirus product name, Product version, Engine and signature version, the number of Hosts running this combination.

AntiVirus Installations verbose reports contain the following data:

- Host name, Product version, Engine version, Signature version, Time this information was obtained.

**Step 4** From the **Groups matching** field, you can select a specific group for which to generate antivirus installation information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate antivirus installation information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.



---

**Note**

Individual hosts do not appear in the Hosts report field until they have uploaded data at least once.

---

**Step 6** Enter a **Time Frame** by which to view the collected data. This time indicates the last or most recent time the antivirus product was used on the system(s) in question.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second.

**Step 7** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

**Step 8** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer. Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

## Installed Products Report

Use this report type to view a list of products that are installed or not installed on various selected host machines. The Products listed alphabetically in the report page are the software programs found to be installed (or not installed) on the systems that were analyzed. These are software programs that are visible in the Add/Remove Programs window.

**Note**

---

This report provides only the latest reported installed product information. It does not provide any historic data on installed products. Therefore, there is no time range available in this report.

---

You can choose to generate a report that provides the following information:

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Installed Products** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-8](#).

Figure 13-8 Installed Products Report Page

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin

Address: https://biohazard/csamc52/webadmin

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Analysis > Application Deployment Reports > Installed Products > Non Microsoft Web Browsers

Warning: The report generation could take a while, depending on the report selections.

Name: Non Microsoft Web Browsers Version: 5.2 r119

Description: Summary report of some common Web Browsers other than Microsoft Internet Explorer

Verbose report

Criteria

List hosts with/without the selected products installed.

With products: Mozilla (1.6), Netscape (7.2), <All Products>, Cisco Security Agent Management Console (CSA MC), Generic Windows Operating System

Groups matching: <All Groups>, <All Windows>, CSA MC Systems [V5.2 r119], Desktops - All types [V5.2 r119], Desktops - Remote or mobile [V5.2 r119] but not: <none>, <All Windows>, CSA MC Systems [V5.2 r119], Desktops - All types [V5.2 r119], Desktops - Remote or mobile [V5.2 r119]

Hosts matching: <All Hosts> but not: <none>

Sort by: Host and then by Product

Viewer type: PDF document

Save View report Delete 9 rule changes pending Generate rules Logged in as: admin

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information (number of overall installation copies found) for installed products. If you enable Verbose, you will see a much longer report containing details for installed products on each host by host name.

Installed products non-verbose reports contain the following data:

- Distinct product name and the overall number of Hosts that have this product installed.

Installed products verbose reports contain the following data:

- Distinct product name and the individual Hosts that have this product installed.

**Step 4** If you are creating a report of products not installed on the system(s) in question, select “Count hosts **without** the selected product installed.” If this is a report on products installed on selected hosts, leave the default choice of **with** in the pulldown view.

**Step 5** From the **Products** list field, you can select one or more products and view which hosts and or groups have that product installed (or not installed) on their system (verbose). You can also select <All Products> depending on the type of report you wish to generate.




---

**Note** You do not have to associate products with application classes to run this report type.

---

**Step 6** From the **Groups matching** field, you can select a specific group for which to generate product installation information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 7** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate product installation information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 8** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

**Step 9** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer. Click the **Save** button to save the parameters you’ve just configured for generating this report.

**Step 10** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

## Unprotected Hosts Report

Use this report type to view hosts which are being used in network connections, but are not protected by Cisco Security Agents.

**Note**

This report type uses Network address sets and Network services for filtering criteria. It is recommended that you restrict the network address set to systems under your control. Otherwise, the report may describe external sites as not having the Cisco Security Agent installed. Likely, this is not the intention of the report.

**Note**

Network data collection must be enabled to gather data relevant to this report.

From the **Analysis>Application Deployment Reports** option, select a report type. In this case, click on **Unprotected Hosts** and do the following:

- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view.
- Step 2** Enter a **Name** and **Description** for the report.
- Step 3** From the **Network Address Sets** field, select a preconfigured Network Address Set. You can view information for <All Addresses> or only for those you select.

**Note**

You can create a new Network Address Set or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

- Step 4** From the list field, select a preconfigured **Network Services**. You can view information for <All Ports> or only for those you select.

**Note**

You can create a new Network Service or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

- Step 5** Enter a **Time Frame** by which to view the collected data.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.

- Step 6** Select the primary and secondary criteria by which to sort the report. You can sort by operation, host, unprotected address, or protocol.
- Step 7** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.
- Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
- Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

Figure 13-9 Unprotected Hosts Page

The screenshot shows the Management Center for Cisco Security Agents V5.2 interface. The breadcrumb trail is: Analysis > Application Deployment Reports > Unprotected Hosts > External network connections observed.

**Name:** External network connections obser | **Version:** 5.2 r119

**Description:** Network connects to and accepts from non CSA hosts

**Criteria:**  
 Collect data on all IP addresses used in network connections during the specified time frame that are not associated with Cisco Security Agents. Results can be filtered by Network Address Sets and Network Services. Verbose network data collection must be enabled to gather data relevant to this report.

**Network Address Sets:** <All Addresses>  
 All IP addresses [V5.2 r119]  
 Authorized Port Scanners [V5.2 r119]  
 External IP addresses [V5.2 r119]  
 Internal IP addresses [V5.2 r119]

**Network Services:** <All Ports>  
 ALT-HTTP [V5.2 r119]  
 Cisco Trust Agent EAP [V5.2 r119]  
 Cisco VPN Service Protocols [V5.2 r119]  
 DHCP and BOOTP [V5.2 r119]

**Time frame:**  
 From: 1 week ago  
 Until: now  
 All times

**Sort by:** Host and then by Operation

**Viewer type:** PDF document

Buttons: Save, View report, Delete, Generate rules. Status: 9 rule changes pending. Logged in as: admin.

191614

## Unprotected Products Report

Use this report type to view hosts that have products installed which have no associated Cisco Security Agent policies (i.e. Hosts running products for which there is no deployed policy.) Note that this report type is the most complex report to configure as it requires both product associations to be configured and network data to be collected.

From the **Analysis>Application Deployment Reports** option, select a report type. In this case, click on **Unprotected Products** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-10](#).
  - Step 2** Enter a **Name** and **Description** for the report.
  - Step 3** From the **Products** list field, you can select one or more products and view which hosts and or groups have used that product on their system (verbose) but have no policy for that product enforced. You can also select <All Products> depending on the type of report you wish to generate.

**Note**

You must first associate products with application classes to run this report type.

**Note**

Network data collection must be enabled to gather data relevant to this report.

- Step 4** From the **Groups matching** field, you can select a specific group for which to generate unprotected product information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.
- Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.
- Step 6** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.
- Step 7** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.
- Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
- Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

Figure 13-10 Unprotected Products Report Page

The screenshot shows the Management Center for Cisco Security Agents V5.2 interface. The browser window title is "Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer". The address bar shows "https://bichazard/csamc52/webadmin". The main navigation bar includes "Events Systems Configuration Analysis Maintenance Reports Search Help". The current page is "Analysis" > "Application Deployment Reports" > "Unprotected Products" > "Unprotected IIS Installations".

The report configuration section includes:

- Name:** Unprotected IIS installations
- Version:** 5.2 r119
- Description:** Lists CSA hosts that have IIS 5.0 installed without having the IIS policy deployed.
- Criteria:** Collect data on hosts with at least one of the selected products installed but not enforcing any of the selected policies.
- Products:** World Wide Web Publishing Service (5.0), <All Products>, Cisco Security Agent Management Console (CSA MC), Generic Windows Operating System, McAfee VirusScan Enterprise (7.0.0)
- Policies:** Web Server - Microsoft IIS - Windows [V5.2 r119], <All Policies>, Agent UI control [V5.2 r119], Application Behavior [V5.2 r119], Application Classification [V5.2 r119]
- Groups matching:** <All Groups>, <All Windows>, CSA MC Systems [V5.2 r119], Desktops - All types [V5.2 r119], Desktops - Remote or mobile [V5.2 r119] but not: <none>, <All Windows>, CSA MC Systems [V5.2 r119], Desktops - All types [V5.2 r119], Desktops - Remote or mobile [V5.2 r119]
- Hosts matching:** <All Hosts> but not: <none>
- Sort by:** Host and then by Product
- Viewer type:** PDF document

At the bottom, there are buttons for "Save", "View report", and "Delete". A status bar indicates "9 rule changes pending" and "Generate rules". The user is logged in as "admin".

## Product Usage Report

Use this report type to view the number of systems on which installed products are used or not used.



---

**Note** In order to generate this report type, you must first associate products (all or just the particular ones you're interested in) with an application class or classes. See [Configure Product Associations, page 13-7](#).

---

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Product Usage** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-11](#).
- Step 2** Enter a **Name** and **Description** for the report.
- Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information displaying the overall number of systems each product is used on. If you enable Verbose report, you will see a much longer report containing details for product usage on each host by host name.
- Product Usage non-verbose reports contain the following data:
- Product name and the overall number of hosts that have used the product.
- Product Usage verbose reports contain the following data:
- Product name and the individual name of the host(s) that have used the product.
- Step 4** If you are running a report to determine which products are not used on systems, select "List hosts which have **not used** the selected products within the specified time" in the options pulldown list. Otherwise, leave the default choice of **used** selected.
- Step 5** From the **Products** list field, you can select one or more products and view which hosts and or groups have used that product on their system (verbose). You can also select <All Products> depending on the type of report you wish to generate.
- Step 6** From the **Groups matching** field, you can select a specific group for which to generate used product information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

- Step 7** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.
- Step 8** Enter a **Time Frame** by which to view the collected data. This time indicates when the product was used on the system(s) in question.
- You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.
- Time syntax:
- You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Step 9** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.
- Step 10** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.
- Step 11** Click the **Save** button to save the parameters you've just configured for generating this report.
- Step 12** Click the **View Report** button and the report is automatically displayed in a new window.
- You can use the Delete button to delete/remove the report entirely.

Figure 13-11 Product Usage Report Page

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Home Local intranet

Address <https://biohazard/csamc52/webadmin> Go Links >>

Management Center for Cisco Security Agents V5.2 Logout | Help | About

Events Systems Configuration Analysis Maintenance Reports Search Help

Analysis > Application Deployment Reports > Product Usage > SQL Server Installations

**Warning: The report generation could take a while, depending on the report selections.**

**Name**  **Version**

**Description**  
  
 Verbose report

**Criteria**  
*List hosts which have used/not used the selected products within the specified timeframe.  
 To use this report effectively you must first associate the selected products with an application class or classes.*

Used products:    
 Cisco Security Agent Management Console (CSA MC)  
 Generic Windows Operating System  
 McAfee VirusScan Enterprise (7.0.0)

Groups matching:  but not:

Hosts matching:  but not:

Time frame: From:  Until:   
 All times

Sort by:  and then by

Viewer type:

Save View report Delete 9 rule changes pending Generate rules Logged in as: admin

191612

## Network Data Flows Report

Use this report type to view, by network service, the number of data flows (unique source/destination address combinations), the number of hosts acting as clients, and the number of hosts acting as servers. This data can be filtered by protocol,

source address set, and destination address set. You could use the results of this report to constrain a host's communication to only those hosts that it typically talks to.

**Note**

Verbose network data collection must be enabled to gather data relevant to this report.

From the **Analysis>Application Deployment Investigation Reports** option, select a report type. In this case, click on **Network Data Flows** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-12](#).
- Step 2** Enter a **Name** and **Description** for the report.
- Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information displaying the overall number of data flows rather than data flows per host. If you enable Verbose report, you will see a much longer report containing details for hosts, source and destination addresses, protocols, and client/server connections.
- Network Data Flows non-verbose reports contain the following data:
- Unique Protocol/port combinations, unique combination of Source IP address, Destination IP address (including address resolved to host name whenever possible), Number of incoming and outgoing connections between the source/destination combination in the specified time frame.
- Network Data Flows verbose reports contain the following data:
- Local host, Local IP address, Local process name, Network operation, Peer host, Peer IP address, Number of network requests with the distinct combination of all items mentioned.
- Step 4** From the **Applications** list field, you can select one or more applications with which to filter this report. You can also select <All Applications> depending on the type of report you wish to generate.

- Step 5** From the **Local Groups matching** field, you can select a specific group for which to generate network data flow information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.
- Step 6** From the **Local Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.
- Step 7** From the list field, select a preconfigured **Peer Network Address Sets matching**. You can view information for <All Addresses> or only for those you select.




---

**Note** You can create a new Network Address Set or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

---

- Step 8** From the **Peer Groups matching** field, you can select a specific peer group for which to generate network data flow information. You can view information for <All Groups> or only for those you select.
- Step 9** From the **Peer Hosts matching** field, you can select a specific peer host for which to generate network data flow information. You can view information for <All Hosts> or only for those you select.
- Step 10** Optionally, enable the **Report also non-CSA host traffic (peer group/host filter is ignored)** checkbox. This will produce a much longer report and will ignore any peer settings you may have configured.
- Step 11** From the list field, select a preconfigured **Network Service**. You can view information for <All Ports> or only for those you select.




---

**Note** You can create a new Network Service or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

---

- Step 12** Enter a **Number of distinct peer hosts** by which to filter this report.
- Step 13** Enter a **Time Frame** by which to view the collected data.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

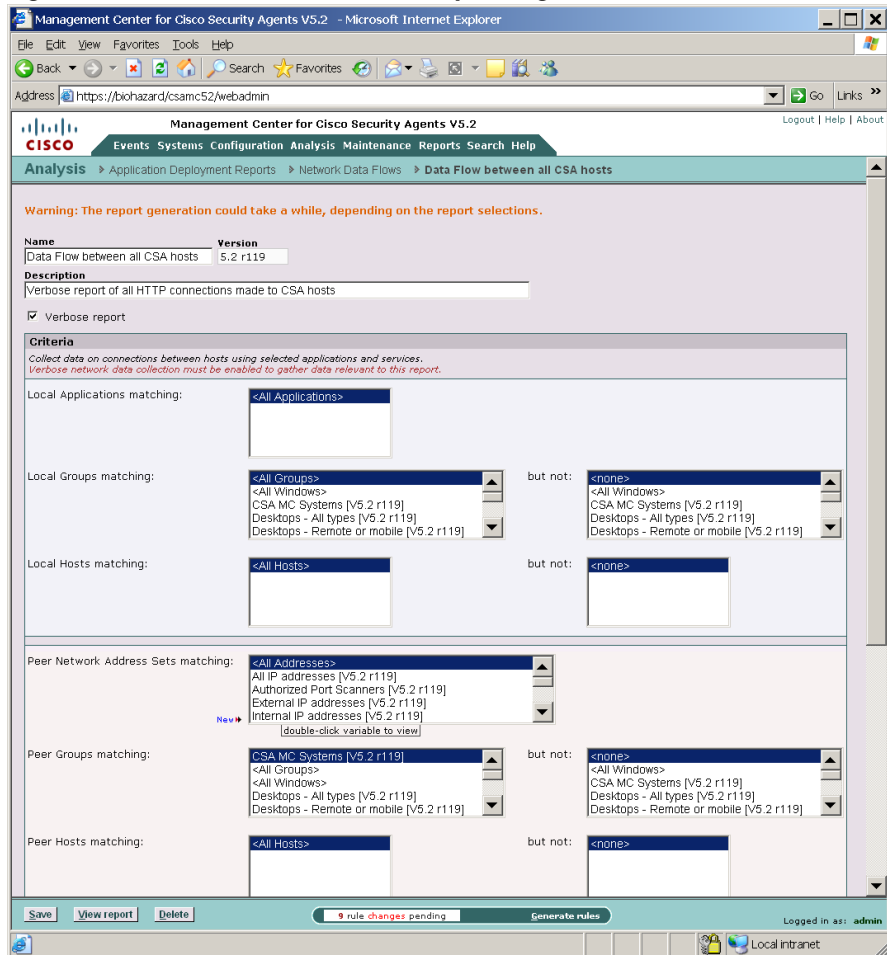
Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second.

- Step 14** Select criteria by which to sort the report. You can sort by host, application, or peer address.
- Step 15** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.
- Step 16** Click the **Save** button to save the parameters you've just configured for generating this report.
- Step 17** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

Figure 13-12 Network Data Flow Report Page



191609

## Network Server Applications Report

This report is intended to break down network server application activity on a given set of hosts. You could use this report type to view which network server applications are listening on ports but not accepting any (or very few) connections. You could also use this to determine which are the most active web

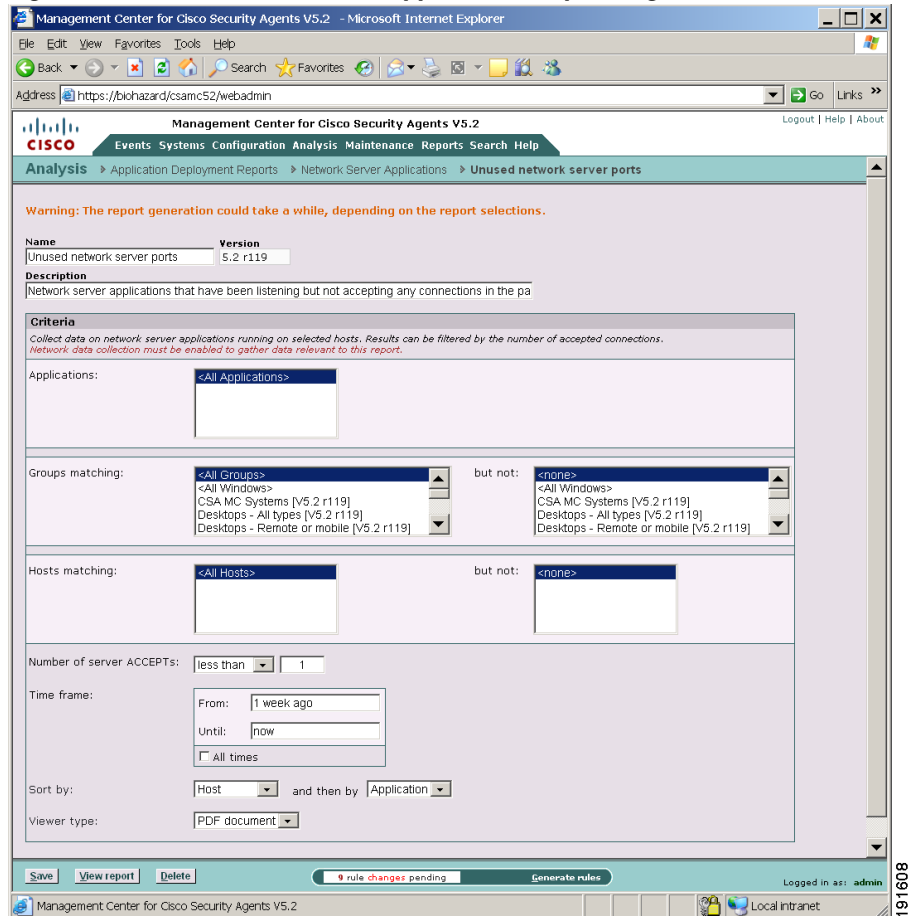
servers or database servers on your network.

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Network Server Applications** and do the following:

- 
- Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See [Figure 13-13](#).
- Step 2** Enter a **Name** and **Description** for the report.
- Step 3** From the **Applications** list field, you can select one or more applications which hosts and or groups use to listen on the network. You can also select <All Applications> depending on the type of report you wish to generate.
- Step 4** From the **Groups matching** field, you can select a specific group for which to generate unused network application information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.
- Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.
- Step 6** Enter the **Maximum number of server ACCEPTs**. By default, this field has 10 entered. Use this number to find **more than** or **less than** the specified number of network listens with no or very few subsequent network connections.
- Step 7** Enter a **Time Frame** by which to view the collected data. This time indicates when the network listen/connection was seen on the system(s) in question.
- You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.
- Time syntax:
- You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Step 8** Select criteria by which to sort the report. You can sort by port, host, or application.

- Step 9** Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.
- Step 10** Click the **Save** button to save the parameters you've just configured for generating this report.
- Step 11** Click the **View Report** button and the report is automatically displayed in a new window.
- You can use the Delete button to delete/remove the report entirely.

Figure 13-13 Network Server Applications Report Page



## Viewing Reports

When you generate your reports, you're given the option of selecting the type of viewer through which to display the report. From the Viewer type pulldown menu, you can select the following.

- **PDF:** This option will generate the complete report as a PDF file that can be viewed, printed, and saved using the browser PDF plug-in. If you do not have a PDF plug-in installed on your browser, you will have to install a PDF browser plug-in to view this report type.
- **HTML:** This option breaks the report into individual HTML pages which can be viewed one page at a time in a browser window. Only the currently viewed report page can be printed. (Supported by Internet Explorer 3.02 and higher and FireFox 1.5.0.x or higher.)

When you print reports, the formatting will vary depending on which view type you have selected and the printer settings on the printer you're using.

**Caution**

---

When you print reports, it is recommended that you print using Landscape mode. Reports do not print correctly using Portrait mode.

---

**Caution**

---

CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. If you remove the Java directory from the CSA MC system, you cannot generate reports.

---

## Exporting Reports

When you export analysis reports, you are only exporting the report itself and the names of objects referenced in the report, such as a group or policy. The group, policy objects, and product mappings are not automatically exported with the report. There is no cascading inheritance when you export either reports or event sets as occurs when other items are exported. You must select groups, policies, and product mappings separately if you want to export them for the purpose of the report.

## What is Application Behavior Investigation

Cisco Security Agent Application Behavior Investigation works with CSA MC and the Cisco Security Agent, serving as a data analysis and policy creation tool for administrators who are deploying policies across systems and networks.

Because the rules that comprise CSA MC policies are application-centric, understanding the resources applications require for normal operations is integral to building effective policies. Behavior investigation does that by analyzing applications as they operate in a normal environment and generating useful reports and rule modules (rule module creation is a separately licensed feature) based on that analysis.

## How Application Behavior Investigation Works

When deployed on a system running a Cisco Security Agent, Application Behavior Investigation monitors the actions of designated applications on that system, logging all resource access attempts made by the application. It then analyzes the logging data it collects and develops detailed reports for the application in question. It also, optionally, generates a rule module. The generated rule module enforces what is determined to be normal application behavior while restricting all other behaviors. These other behaviors could now be construed as abnormal or suspicious based on the analysis.



### Note

---

If you are creating your own policies and not using Application Behavior Investigation, refer to [Chapter 4, “Overall Policy Methodology,”](#) for information.

---

## The Application Behavior Investigation Process

The application behavior investigation is performed by three different contributing components: CSA MC, the agent (logging agent), and the behavior investigation functionality.

- Through *CSA MC*, you designate which application you want to investigate. You also select an agent host on which the investigation is to take place and a time frame within which the investigation will be completed. This investigation configuration is then sent to the agent on the selected host in the same way policies are sent to agents.

*Application Behavior Investigation* examines all the logged data it receives from the logging agent. When the analysis is complete, it creates a policy for the application and generates reports containing information on all resources

accessed by the application. The policy enforces the normal operations seen in the log file and will deny any operation attempts by the application that do not align with this normal behavior.

- The *agent* receives the analysis configuration information when it next polls in to CSA MC. This agent now becomes the "logging agent" in this process. It logs all operations performed by the designated application. As this logging takes place, it is assumed that the application is being thoroughly exercised in a normal operating environment. When the analysis is complete, the logged data is sent to the behavior investigation function for processing.

Optionally, CSA MC imports the rule module created by the behavior investigation.

## Behavior Analyses

By accessing the **Analysis>Application Behavior Investigation >Behavior Analyses(Windows or UNIX)** window, you can configure parameters for analyzing a particular application.

When you are ready to configure a behavior analysis for an application, you must have the following information:

- What application you want to analyze: You should have an appropriate application class configured for the analysis. (You can leverage existing application classes, but it is recommended that you analyze only one application at a time. See [page 13-44](#) for more information.)
- Which host you want to select for application analysis: You should have an appropriate host chosen for the behavior analysis.

## Creating, Saving, and Cancelling Analysis Data

### Management Center Button Frame

Similar to most CSA MC windows, behavior analysis action items appear in a frame at the bottom of CSA MC.

**Note**

---

The available buttons in the bottom frame change in accordance with the actions available for the page you're viewing. With a behavior analysis, several actions are performed from the same page as the behavior analysis progresses. You may have to refresh the behavior analysis page for the buttons to change appropriately.

---

Available buttons and links are as follows.

- **New**—Use the New button to create new a configuration item within the list view you have selected. Click the New button and a new item appears in the list view. Click the new item link to access the configuration view for that item.
- **Delete**—Use the Delete button in conjunction with the checkboxes beside each list view item. To delete a configuration, select its checkbox (you can select several at once) and click the Delete button. All checked items are deleted. To quickly select all checkboxes, click the very top checkbox in the list view heading bar. Clicking the Delete button then deletes all items.
- **Clone**—Use the Clone button in conjunction with the checkboxes beside each list view item. To clone a particular configuration, select its checkbox and click the Clone button. You can clone one item at a time. New links to the cloned configurations appear in the list view.

**Note**

---

When you clone an item that contains variable items like application classes, the cloned item uses the same variables used in the original item. The variables themselves are not cloned.

---

- **Save**—When you enter configuration information, whether you are entering new data or editing existing data, you must click the Save button once you are finished to save your configuration in the CSA MC database. If you do not click Save before moving to another page in CSA MC, your data is lost.
- **Stop Logging**—If you want to stop the analysis early and send collected data to the workstation for analysis, click this Stop logging button.
- **Start analysis**—When the logging for the analysis is complete, a "Start analysis" button appears in the bottom frame of the behavior analysis page. Click this button to have the analysis workstation begin to analyze the logging data.

- Optional Import—When the analysis of the logging data is complete, the behavior analysis creates a rule module which you can import into CSA MC. The "Import" button appears when the rule module creation is complete if you have a license for Analysis rule module creation and import.

# Configure a Behavior Analysis Investigation

To configure a behavior analysis investigation, do the following:

**Note**

---

In some cases, you can configure a behavior analysis investigation using the Event Management Wizard accessible from particular event log entries. See [About the Event Management Wizard, page 10-17](#) for more information.

---

- 
- Step 1** Move the mouse over **Analysis>Application Behavior Investigation** in the menu bar and select **Behavior Analyses (Windows or UNIX)** from the drop-down list that appears. The list of existing analyses (if any) is displayed.
- Step 2** Click the **New** button to create a new behavior analysis. This takes you the behavior analysis configuration page. (See [Figure 13-14](#).)
- Step 3** Enter a **Name** for the behavior analysis you are creating.
- Step 4** Enter a **Description** for your behavior analysis. This description becomes visible in the behavior analysis list view.
- Step 5** **Verbose logging mode:** By default, behavior analysis filters its logging process so that duplicate events are not logged. You can turn this feature off by selecting this checkbox. If you do turn this filtering off, your logs will be a great deal larger, but the advantage is that you will be able to see how often the same resource is accessed when you view the behavior analysis reports.

**Note**

---

The **Target operating system** you selected is displayed in a read-only field. The **Behavior analysis status** field is also a read-only field. It displays text, informing you of each stage of the analysis. When you first configure your behavior analysis, it displays "Not yet deployed."

---

Figure 13-14 Behavior Analysis Configuration Window

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

Address: https://biohazard/csamc52/webadmin

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Analysis > Application Behavior Investigation > Windows Behavior Analyses > Untitled\_1

OTHER BEHAVIOR ANALYSES

**Name**  
Application\_bhvr

**Description**  
See how application behaves

**Target operating system**  
Windows

**Behavior analysis status**  
Not yet deployed

Verbose logging mode

**Configuration**

Perform an analysis of the selected application classes:

Application Behavior - Application to be analyzed [V5.2 r119]  
Email clients Dynamic  
notepad

[double-click application class to view]

For the selected host: biohazard

You can turn policy enforcement off for the analyzed application on the selected host for the time frame of the behavior analysis. If you do not select this checkbox, the analysis takes place within the confines of the enforced policies.

Disable policy rule enforcement

Start behavior analysis at time: now

End behavior analysis at time: after 1 hour

Stop analysis when either of the following occurs:

Log file size exceeds [ ] MB

Application is invoked [ 3 ] times

Save | 1 rule change pending | Generate rules | Logged in as: admin

Local intranet

- Step 6** In the **Perform an analysis of the selected application classes** list box, select the application class or classes you want to analyze. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key when you click on the item in question. Press and hold the **Shift** key when you click on an item to select multiple successive items.

**Caution**

You can select an application class that contains more than one application for the analysis. But in that case, the reports created would apply equally to all applications included in the analyzed application class. For example, if the

application class you are analyzing contains both Microsoft Word and Microsoft Outlook, the reports created by the behavior analysis would be a combination of the resources required by both applications.

---

Next you must assign the behavior analysis to a specific host system.

- Step 7** Select the host you are assigning the behavior analysis to in the **For the selected host** list box. e.g. Note that you cannot have more than one behavior analysis running on a host at one time.



**Note** Once the behavior analysis begins, you can click the **Stop logging** button that appears in the bottom frame. The behavior analysis stops automatically according to the parameters you enter on this behavior analysis page. But if you want to stop the analysis early and send collected data to the workstation for analysis, click this Stop logging button.

---

- Step 8** Optionally, you can select to **Disable policy rule enforcement** for the time frame of the analysis. Otherwise, the analysis takes place only within the confines of enforced policies. Some events may be denied by rules and therefore the analysis may not be complete.



**Caution**

If you select the Disable policy rule enforcement checkbox, when the logging agent receives a behavior analysis investigation, any policies relevant to the application being analyzed are disabled on the selected host until the analysis is completed. This may be undesired if the application in question is unknown or is in any way suspicious.

---

**Step 9** Next you must enter behavior analysis time frames.

- **Start behavior analysis at time**—From the pulldown options, select a time for the behavior analysis to start once the host polls in and receives the behavior analysis. If you specify no time here, "now" is automatically entered. This means the behavior analysis will start immediately when the host receives it.
- **End behavior analysis at time**—You must enter a time for the behavior analysis to end. The behavior analysis process will not allow you to save the analysis until you do. When you enter a *log size* parameter or an *application invocation number* in the fields below, they act as overrides of this end time.

You can specify a relative time using any of the following terms: tomorrow, yesterday, today, now, last, this, next, ago, year, month, week, day, hour, minute. Enter a specific time using any of the following time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional. Enter a specific month and day with optional year in the formats: mm/dd/yy, monthname dd, yy. The default year is the current year.

**Step 10** Stop behavior analysis when either of the following occurs:

- **Log file size exceeds \_\_ MB**—You can enter a size restriction on the log file. When it reaches the size you indicate, the analysis is finished. (Note that the maximum log file size you can enter here is 256 MB. This is also the default value.)
- **Application is invoked \_\_ times**—You can specify an application invocation restriction. Once the application is invoked on the system the number of times you indicate, the analysis is finished.



**Caution**

It is not always appropriate to use an invocation number limit. For example, for server applications, time frame parameters might be a more appropriate criteria for ending a behavior analysis.



**Note**

If you enter analysis completion parameters in more than one field, the parameter that is reached first is the one that applies.

**Step 11** Click the **Save behavior analysis** button in the bottom frame of CSA MC to save it.

**Step 12** Once your behavior analysis is configured to your satisfaction, click the **Generate rules** link in the bottom frame and continue by clicking the subsequent **Generate** link to distribute the behavior analysis to the group hosts you've selected.

Depending on the behavior analysis parameters you've configured, the selected host will begin the behavior analysis after it polls in to CSA MC and receives the new rules.

**Note**

---

Keep in mind that if you have configured your behavior analysis to begin immediately and your agents are configured to poll in to CSA MC once every hour, the behavior analysis will not begin until the agent next polls in. In this example case, that time frame could be up to one hour. Additionally, be careful not to designate the end time as a time frame that could occur before the agent polls in and receives the behavior analysis. In this case, the analysis will not run at all.

---

## Monitoring the Behavior Analysis

You can check your CSA MC **Event Log** to view the behavior analysis progression. An event is sent when the behavior analysis begins and again when it finishes.

You can also monitor **Progress Status** fields in the Behavior Analysis configuration page. These fields appear when the analysis is in progress. You can monitor the size of the log file and if you've set an application invocation limit, you can monitor the number of application innovations as well. These progress fields update each time the logging agent polls in to the MC.

When reports and the rule module are ready to be imported to CSA MC, an event log message appears indicating this.

Figure 13-15 Behavior Event Log Messages

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

Management Center for Cisco Security Agents V5.2  
Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

21 events [change filter](#)

Event log generation time: 12/1/2006 3:38:06 PM  
Severity: Information - Emergency  
Host: All  
Rule Module: All  
Events per page: 50  
Sort by: Order received  
Filter out similar events: Yes (filtered out ~86% of 152 events)  
Show suppressed events: No [1 event suppression filter defined]

#	Date	Host	Severity	Event
21	12/1/2006 3:35:25 PM	-	Information	Administrator 'admin' logged in from 172.31.10.12 (S11). <a href="#">10 similar events (same Type/Rule ID/Application)</a> <a href="#">Find Similar</a>
20	12/1/2006 3:33:31 PM	biohazard	Information	Log files for analysis 'Application_bhvr' were sent to the analysis workstation. <a href="#">Details</a> <a href="#">Behavior Analysis</a> <a href="#">Find Similar</a>
19	12/1/2006 3:33:25 PM	biohazard	Information	Logging for analysis 'Application_bhvr' has ended. <a href="#">Details</a> <a href="#">Behavior Analysis</a> <a href="#">Find Similar</a>
18	12/1/2006 3:31:57 PM	biohazard	Information	Logging for analysis 'Application_bhvr' has started. <a href="#">Details</a> <a href="#">Behavior Analysis</a> <a href="#">Find Similar</a>
17	12/1/2006 3:25:52 PM	biohazard	Notice	The process 'C:\Program Files\Cisco Systems\CSAgent\bin\okclient.exe' (as user BIOHAZARD\Administrator) attempted to access a resource which resulted in the user being asked the following question: 'An attempt is being made to disable security for the Cisco Security Agent. Do you wish to allow this?' The user was queried and a 'Yes' response was received. <a href="#">Details</a> <a href="#">Rule 707</a> <a href="#">Wizard</a> <a href="#">2 similar events (same Type/Rule ID/Application)</a> <a href="#">Find Similar</a>
16	12/1/2006 3:25:31 PM	biohazard	Alert	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 172.31.10.17 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation was denied. <a href="#">Details</a> <a href="#">Rule 287</a> <a href="#">Wizard</a> <a href="#">52 similar events (same Type/Rule ID/Application)</a> <a href="#">Find Similar</a>
15	12/1/2006 3:25:31 PM	biohazard	Alert	The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\LOCAL SERVICE) attempted to initiate a connection as a client on TCP port 139 to 172.31.10.17 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation

1 rule change pending [Generate rules](#) Logged in as: admin

Management Center for Cisco Security Agents V5.2 Local intranet

191602

## Start Behavior Analysis

When the Event Log in CSA MC displays "Log files for behavior analysis were sent to the analysis workstation", you can begin the data analysis of the logging information.

Begin this analysis by accessing the behavior analysis window for this particular analysis and clicking the **Start analysis** button in the bottom frame. This begins the analysis. An Event Log message appears informing you that "Data analysis has started."

- When the analysis is complete, you can “View reports”.
- If you have a license for rule module creation, when the analysis is complete, the Event Log file displays the message "Rule module creation for behavior analysis completed successfully". Once rule module creation is complete, you can import the module.

## Importing the Rule Module

**Note**

---

If you do not have a separate license for importing behavior analysis rule modules, the behavior analysis results in report creation without the added step of creating a rule module.

---

When the behavior analysis has completed its analysis of the logging data, the rule module it created is ready to be imported into CSA MC.

Import the rule module by once again accessing the behavior analysis window for this particular analysis. Click the **Import** button in the bottom frame. (This button only appears when the rule module is ready for importing.)

**Note**

---

The rule module and its accompanying "variables" are imported into CSA MC. The behavior analysis creates its own variables for use in the rules it also creates. See [Figure 13-16](#).

---

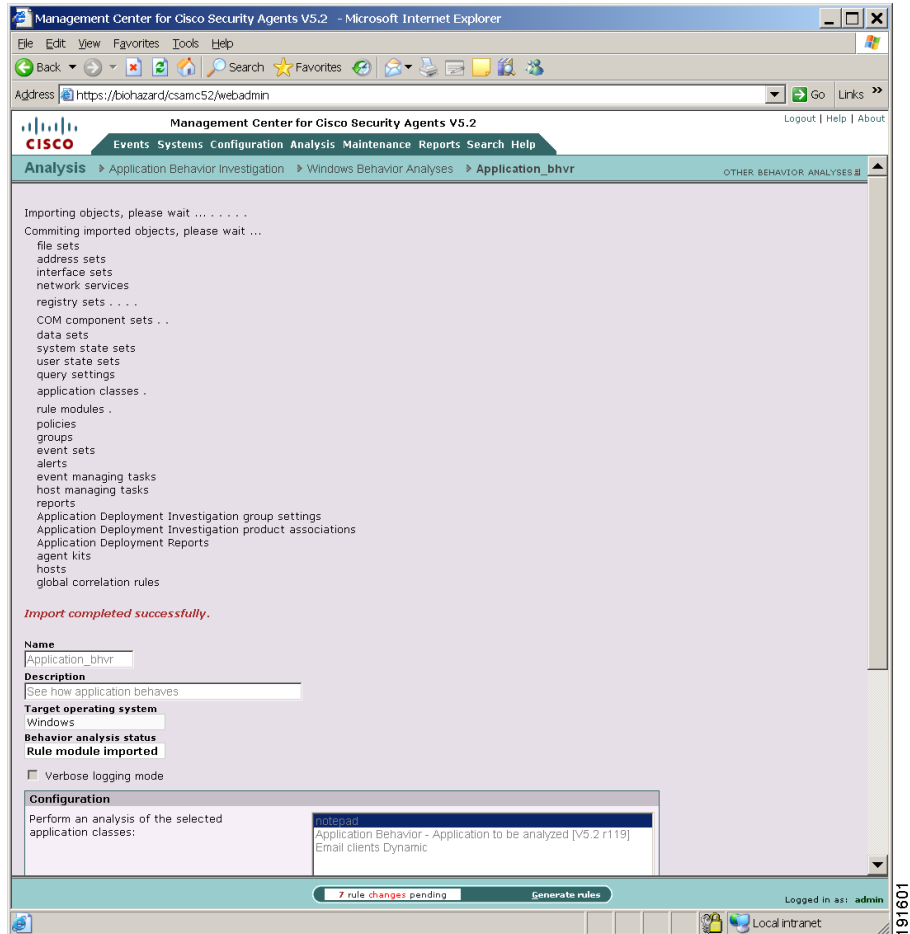
**Note**

---

In order to deploy the rule module that the behavior analysis has created, you must associate it with an existing policy or with a new policy that you create. This policy must be attached to a group for the rules to be deployed to hosts.

---

Figure 13-16 Import Process



191601

# Application Behavior Reports

During the analysis process, the behavior analysis sorts the logging data it receives from the logging agent into categorized reports. You can view these reports on the CSA MC system by accessing the **Analysis>Application Behavior Reports>Behavior Report(Windows or UNIX)**.

Reports on specific analyses only become available once the behavior analysis has successfully completed. The CSA MC Event Log displays a message to inform you that reports have been created.

**Figure 13-17 File Events Report**

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface. The main content area displays a report titled "File Events Report" for job "Application\_bhvr" corresponding to host "biohazard". The report is filtered by the "Directory" field and shows 47 events. The events are listed in a table with columns for Time, Directory, File Name, File Extension, Operation, PID, and Process Name.

Time	Directory	File Name	File Extension	Operation	PID	Process Name
2006-12-01 15:29:00	C:\WINDOWS\WinSxS\96_Microsoft.Windows-Common-Controls_6595b64144ccf1df_6-0.3790.1830_x-ww_7AE80CCF	COMCTL32.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\system32	WINSPOOL.DRV	DRV	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\system32	ShimEng.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\system32	apphelp.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\AppPatch	sysmain.sdb	SDB	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS	WindowsShell.Manifest	MANIFEST	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\system32	SHELL32.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:00	C:\WINDOWS\system32	UxTheme.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:06	C:\WINDOWS\system32	IMM32.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:11	C:\WINDOWS\system32	hhctrl.ocx	OCX	READ	2200	notepad.exe
2006-12-01 15:29:11	C:\WINDOWS\system32	rpsess.dll	DLL	READ	2200	notepad.exe
2006-12-01 15:29:26	C:\WINDOWS\WinSxS\96_Microsoft.Windows-Common-Controls_6595b64144ccf1df_6-0.3790.1830_x-ww_7AE80CCF	COMCTL32.dll	DLL	READ	204	notepad.exe
2006-12-01 15:29:26	C:\WINDOWS\system32	WINSPOOL.DRV	DRV	READ	204	notepad.exe
2006-12-01 15:29:26	C:\WINDOWS\system32	ShimEng.dll	DLL	READ	204	notepad.exe

The interface also shows a sidebar with navigation options like "File Events", "Registry Events", and "Network Events". At the bottom, there is a status bar indicating "7 rule changes pending" and a "Generate rules" button. The user is logged in as "admin".

101604

## Report Components

When you access the application behavior reports window, you can view individual reports for all completed analysis from the same window by selecting a particular behavior analysis from the **Reports for behavior investigation** pulldown list at the top of the window.

Reports are broken down into the system and network resource types that were accessed by the application during the behavior analysis logging session. Each report category has several sub-topics you can select from for organizing information.

Each category drop-down menu provides an overall summary view. This view displays all the data of that particular category which was accessed during the analysis time frame. If you select to view **Behavior Summary** for a report category (see [Figure 13-18](#)), additional views further sort the information the behavior analysis has collected by time frame, individual resource (e.g. single file or registry key), source and destination address in the case of network resources, and other criteria depending on the resource type in question.

**Figure 13-18 All Events Report Sorting**

The screenshot displays the Management Center for Cisco Security Agents V5.2 interface. The main content area shows a table of events sorted by the number of events. The table has two columns: the event category and the number of events. The categories and their counts are as follows:

Event Category	# of Events
COM (All Events)	0
FILE (All Events)	47
FILE - Read Operations	45
FILE - Write Operations	2
FILE - Writes of Executables	0
NETWORK (All Events)	0
NETWORK - Acting as Client	0
NETWORK - Acting as Server	0
REGISTRY (All Events)	866

The interface also shows a navigation menu on the left with categories like File Events, Registry Events, and Network Events. At the bottom, there is a status bar indicating '7 rule changes pending' and a 'Generate rules' button. The user is logged in as 'admin'.

Use the data from these reports to further refine your policies or to understand why particular rules were created for the policy.

You can view reports from the following categories:

## File Event Reports

File reports display information such as the name of the file accessed, the application accessing the file, and the operation performed on the file. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Directory—This is the directory location (local or network share) of the file resource accessed in the event.

- File type—This is the individual file accessed in the event.
- Operation—This is the operation (read, write) performed on the accessed file.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Registry Event Reports (Windows only)

Registry reports provide details such as the name and value of the registry key that was accessed and the process that accessed it. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Key name—This is the name of the registry key accessed during the event.
- Value name—This is the registry value accessed during the event.
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## COM Event Reports (Windows only)

COM reports display information on the COM Class ID that was accessed and the process that made the request. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Object name—This is the unique identifier for the COM object accessed during the event.
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Network Event Reports

Network reports display details such as the protocol accessing the network, the source and destination addresses of the connection, and the source and destination ports. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Role—This indicates whether the system in question was acting as a client or server during the network event.
- Protocol—This indicates whether this event was a TCP or UDP network connection.
- Source address—This is address where the connection originated from during the event.
- Source port—This is the port used during the event.
- Destination address—This is the destination address of the network connection for the event.
- Destination port—This is the destination port used for the connection. (Note that this port is used for the associated network rule that is generated as part of the policy.)
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Summary Reports

Summary reports display the number of times each resource type was accessed during the logging time frame.

## Working with Reports

Behavior analysis reports contain a great deal of application information. You can search through this data using the browser window's own search capabilities. From the report page you want to search on, press and hold the **Ctrl** button and press the **F** key. The browser search window appears.

You can also highlight, copy and paste report text into an application such as Microsoft Excel. From Excel, you can then organize the data in any manner you choose.

# The Behavior Analysis Rule Module

Once imported, the behavior analysis rule module is added to your list of rule modules (Windows or UNIX) with the word "Analysis" appended to the original behavior analysis name. For example, if the analysis name is "Word\_application", the name of the policy would be "Analysis Word\_application Rule module."

## Reviewing the Rule Module

The rule modules created by the behavior analysis process enforce normal application behavior and maintain application and system integrity. To achieve this, the general strategy behind the creation of behavior analysis rule modules is to protect the application from the system and to protect the system from the application.

As with all new rule modules you create, you should review the rules generated by the behavior analysis and run the module in Test Mode for some period of time to ensure that it works as intended. You should also review the reports generated during the analysis as they are valuable resources for understanding the application as well as the rule module.

**Note**

---

Behavior analysis does not add system hardening or global correlation "built-in" rules to the policy. For example, you can add System API control to the policy.

---

## Behavior Analysis Methodology

Protecting the application from the system

As part of the rule module, the behavior analysis creates file access control rules with the purpose of protecting the application data. These rules are left disabled by default as they restrict all other applications from accessing the analyzed application's data files. This is a fairly restrictive approach and, depending on the application itself, you may or may not want to enable these rules as part of the module.

Protecting the system from the application

Resources accessed by the application are broken down into file, network, registry, and COM categories and then rules for each category are created by the behavior analysis. Allow rules permit what was seen as normal application behavior while deny rules prevent access to all resources were not used by the application during the logging period.

Because security requirements may vary from site to site, the behavior analysis generates several rules that are disabled by default. The disabled rules are generally network and registry restrictions. The behavior analysis creates these rules but keeps them disabled, leaving it up to the administrator to decide whether or not to impose these added restrictions. These rules are disabled by default because, generally, you should use the application-specific policies created by the behavior analysis in combination with the Sample Network (Permissive, Selective, and Restrictive) policies shipped with the CSA MC.

If you decide to edit behavior analysis rule modules based on your site's requirements, the reports generated during the logging analysis process contain information on all the resources accessed by the application during the logging period. The "summary" reports generated for each resource type are particularly useful in helping to pinpoint what resources may require more or less restrictive rules. (See [Application Behavior Reports](#), page 13-51 for details.)

The general methodology behind the creation of rules for each resource type is as follows:

- File access control rules

The behavior analysis creates file set variables that are combinations of file extension and directory pairs for accessed resources. These are used in allow file access control rules. It then creates a deny file access control rule that prevents access to all other files and directories.

Use File Directory Summary and Individual File Summary reports to help refine these rules, if needed.

- COM component access control rules (Windows only)

The behavior analysis creates COM component set variables which it then uses in a COM component access control rule to allow access to the required COM components. It then creates a COM component deny rule to deny all applications access to the COM components not used during the logging period.

Use COM Object Summary reports to help refine these rules as needed.

- Registry access control rules (Windows only)

The behavior analysis creates these rule types but disables them by default. Registry access control rules are very powerful system control tools. Restricting access to a required registry key could produce undesired results.

The behavior analysis creates Registry Set variables based on the registry resources accessed during the logging period. These registry variables are broken into those that should be allowed and those that can be denied. Those allowed are registry keys accessed during the logging period. All others fall in the deny range. This deny applies only to write access. All registry keys are still allowed read access. You can enable these rules, but you should understand the restrictions you are imposing.

Use Registry Key Summary reports to help refine these rules, if needed.

- Network access control rules

The behavior analysis creates network access control rules but disables network deny rules by default. Network allow rules are created to allow network services for all addresses, both client and server, that were accessed during the logging period. The disabled deny rules then deny all services, client and server, on all ports for the analyzed application. These are fairly restrictive rules. If you intend to enable them or refine them (change port number restrictions or address information), you should refer to the Network Summary reports for information on network services used by the application.

## Variable and Application Class Creation

When the behavior analysis creates the rules for the rule module, it also creates all the registry and COM component variables required by the rules. All Windows files are entered as literals. (Note that UNIX files are grouped into sets.)

Additionally, the behavior analysis creates a new application class for the analyzed application and uses this new application class in all rules that make up the rule module. You should note that if you select more than one application class for the analysis, the application class created for the rule module is an aggregate of all the analyzed applications.

If you decide that the application is not dangerous and it can run without any rule module restrictions, you can begin to configure the behavior analysis.

