APPENDIX C

# Using CSC SSM with Trend Micro Control Manager

This appendix describes how to manage Trend Micro InterScan for CSC SSM from Trend Micro Control Manager (TMCM), and includes the following sections:


- About Control Manager, page C-1
- Register to Control Manager, page C-2
- Control Manager Interface, page C-2
- Ad Hoc Queries, page C-8


## About Control Manager

You should have already installed the Control Manager agent and registered CSC SSM with Control Manager using the CSC SSM Administration > Register to TMCM window. Control Manager is a central management console that runs on its own server, separate from the CSC SSM. It allows you to do the following:

- Manage multiple Trend Micro products and services from a single console.
- Monitor and report on activities such as infections, security violations, or virus entry points.

In the Control Manager, the CSC SSM is a managed product that appears as an icon in the Control Manager management console Product Directory. You can configure and manage the CSC SSM and other products individually or by group through the Product Directory.

With Control Manager, you can download and deploy updated components throughout the network, to ensure that protection is consistent and up-to-date. Examples of updated components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and scheduled updates.

Control Manager provides the following:

- Enterprise-wide coordination
- Proactive Outbreak Management
- Vulnerability Assessment (optional component)
- Outbreak Prevention Services (optional component)
- Damage Cleanup Services (optional component)
- Multitiered management structure

- Flexible and scalable configuration of installed products
- Ad hoc queries and reports

# Register to Control Manager

Choose **Administration > Register** to configure the communication between the TMCM Agent and the Trend Micro Control Manager server.

- Connection Settings—Specify the entity name (instance of InterScan on the particular machine). The entity name appears in the Control Manager product tree, helping you to identify the product.
- Control Manager Server Settings—Specify the Server FQDN or the IP address of the Control Manager server. The port is used for MCP agent communication with the Control Manager. If the Control Manager security is set to medium (HTTPS and HTTP communication is allowed between the Control Manager and the MCP agent of managed products), select **Connect using HTTPS**. The web server authentication username and password are used by the Internet Information Services (IIS) server for authentication.
- Port Forwarding—Specify the PIX NAT port forwarding configuration for InterScan. The IP address is filled in with the PIX WAN IP. The port is filled with the PIX specified listening port.

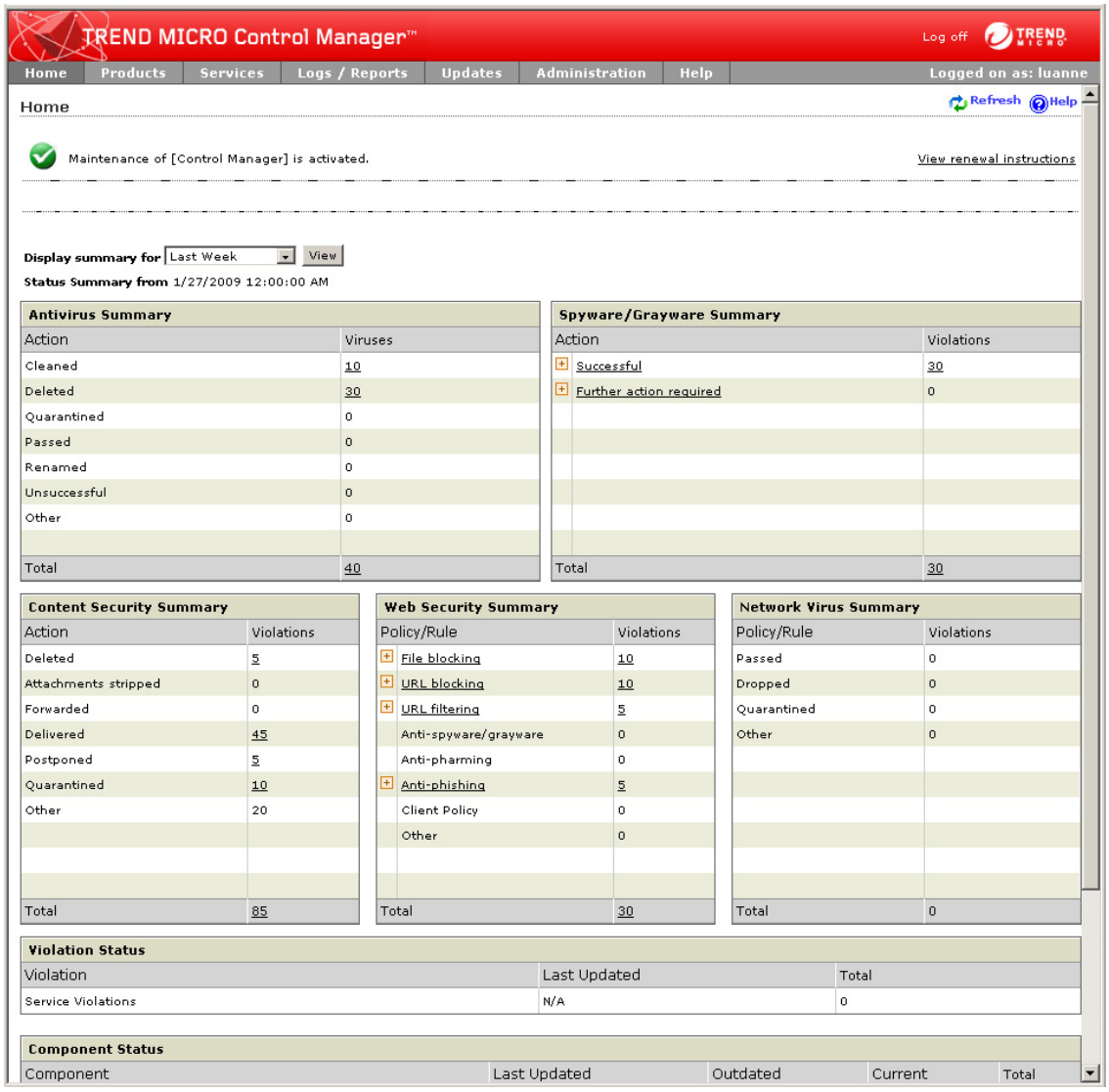
# Control Manager Interface

This section describes the Control Manager interface, and includes the following topics:

- Using the Management Console, page C-3
- Opening the Control Manager Console, page C-4
- Downloading and Deploying New Components, page C-5

Trend Micro Control Manager uses a management console to administer managed products. When you log in to Control Manager, the Home window appears, as shown in Figure C-1.

*Figure C-1 The Control Manager Management Console Home Window.*




# Using the Management Console

The management console consists of the following elements:

- The main menu bar contains Home, Products, Services, Logs/Reports, Updates, Administration, and Help, which you use to administer Control Manager and managed products.

  The Help menu provides links to the Control Manager Online Help (Content and Index), Trend Micro Knowledge Base, Trend Micro Security Information, Sales, Support, and the About screen for Control Manager.

- When you choose the Products or Services menu item, the navigation menu in the left-hand pane refreshes to display the available options.

- In addition to the navigation menu items, choose **Products** from the main menu to access the following tabs for working with managed products: Advanced Search, Configuration, Tasks, Logs, and Directory Management.

# Opening the Control Manager Console

This section describes how to access the Control Manager console, and includes the following topics:


- Accessing the HTTPS Management Console, page C-4
- About the Product Directory, page C-5


You can access the Control Manager console locally from the Control Manager server, and/or remotely through a web browser from any connected computer.

To open the Control Manager console from a remote computer, follow these steps:

**Step 1** To open the Log-on screen, in the browser address field, enter the following:

**http://{***hostname***}/WebApp/login.aspx** (for Control Manager 5.0)

where *hostname* is the FQDN for the Control Manager server, IP address, or server name. The Control Manager Log-on screen appears.

**Step 2** Enter a Control Manager username and password and click **Enter**.

**Step 3** When the Control Manager console appears, click **Products** in the top menu bar and locate the entry for the CSC SSM.

The initial screen shows the status summary for the entire Control Manager system, which is the same as the status summary generated from the Product Directory. User privileges determine the Control Manager functions you can access.

## Accessing the HTTPS Management Console

You can encrypt the configuration data as it passes from the web-based console to the Control Manager server. You must first assign web access to Control Manager and then alter the management console URL to use HTTPS through port 443. For details about how to set up HTTPS access, see the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

To open the Control Manager console using HTTPS, perform the following steps:

**Step 1** Enter the URL for encrypted communication (HTTPS) in one of the following formats:

- **https://{***hostname***}:443/ControlManager** (for Control Manager 3.5)
- **https://{***hostname***}:443/WebApp/login.aspx** (for Control Manager 5.0)

Where *hostname* is the FQDN for the Control Manager server, IP address, or server name. The port number allotted to an HTTPS session is 443.

**Step 2** Press **Enter**.

**Note** When you access a secure Control Manager site, it automatically sends you its certificate, and Internet Explorer displays a lock icon on the status bar.

## About the Product Directory

For administering managed products, the Product Directory is a logical grouping of managed products in the Control Manager console that allows you to perform the following:

- Configure products.
- View product information, as well as details about the operating environment (for example, product version, pattern file and scan engine versions, and operating system information).
- View product-level logs.
- Deploy updates to the virus pattern, scan engine, anti-spam rule, and programs.

Newly registered managed products usually appear in the Control Manager "New Entity" folder, depending on the user account specified during the agent installation. The Control Manager determines the default folder for the managed product by the privileges of the user account specified during the product installation.

You can use the Control Manager Product Directory to administer the CSC SSM after it has been registered with the Control Manager server.

**Note** Your ability to view and access the folders in the Control Manager Product Directory depends on the account type and folder access rights assigned to your Control Manager log-in credentials. If you cannot see the CSC SSM in the Control Manager Product Directory, contact the Control Manager administrator.

# Downloading and Deploying New Components

This section describes downloading and deploying new components, and includes the following topics:

- Deploying New Components from the Control Manager Product Directory, page C-6
- Viewing Managed Products Status Summaries, page C-6
- Configuring CSC SSM Products, page C-7
- Issuing Tasks to the CSC SSM, page C-7
- Querying and Viewing Managed CSC SSM Product Logs, page C-8

The Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends that you update the antivirus and content security components to remain protected from the latest virus and malware threats. By default, the Control Manager enables virus pattern, damage cleanup template, and vulnerability assessment pattern downloads, even if there is no managed product registered on the Control Manager server.

The components to update follow, listed according to the frequency of recommended updates:

- Pattern files and cleanup templates refer to virus pattern files, damage cleanup templates, vulnerability assessment patterns, network outbreak rules, and network virus pattern files.
- Anti-spam rules refer to import and rule files used for spam prevention and content filtering.

- Engines refer to the virus scan engine, damage cleanup engine, and VirusWall engine for Linux.
- Product program refers to product-specific components (for example, Product Upgrades).

**Note** Only registered users are eligible for component updates. For more information, see the "Registering and Activating Your Software > Understanding product activation" online help topic,

## Deploying New Components from the Control Manager Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of the CSC SSM on demand, which is particularly useful during virus outbreaks. Download new components before deploying updates to a specific group or groups of managed products.

To manually deploy new components using the Product Directory, perform the following steps:

**Step 1** From the Control Manager console, click **Products** on the main menu. The Product Directory screen appears.

**Step 2** Select a managed CSC SSM or directory from the Product Directory. The managed product or directory highlights.

**Step 3** Mouse over **Tasks** from the Product Directory menu. A drop-down menu appears.

**Step 4** Choose Deploy <component> from the drop-down menu.

**Step 5** Click **Next**.

**Step 6** Click **Deploy Now** to start the manual deployment of new components.

**Step 7** Monitor the progress via Command Tracking.

**Step 8** Click the **Command Details** link in the Command Tracking screen to view details for the Deploy Now task.

## Viewing Managed Products Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

You can view the managed products status summary from the Home screen or the Product Directory.

To access managed products through the Home screen, open the Control Manager management console.

The Status Summary tab of the Home screen shows a summary of the entire Control Manager system. This summary is identical to the summary provided in the Product Status tab in the Product Directory Root folder.

To access managed products through the Product Directory, perform the following steps:

**Step 1** From the Control Manager console, click **Products** on the main menu.

**Step 2** On the left-hand navigation pane, click the desired folder or managed product name.

- If you select a managed product name, and then click **Status**, System information displays for the managed product summary.

- If you click the Root folder, New Entity, or another user-defined folder, and then click **Status**, summaries appear for Antivirus, Spyware/Grayware, Content Security, Web Security, and Network Virus summaries.

## Configuring CSC SSM Products

You can configure the CSC SSM from the Control Manager through folder division. Add managed products that should have the same configuration to the Temp folder to prevent the settings of other managed products from being overwritten.

The Configuration tab shows either the web console or a Control Manager-generated console.

To configure a product, perform the following steps:

**Step 1** From the Control Manager console, click **Products** on the main menu.

**Step 2** Select the managed CSC SSM from the product tree. The product status appears in the right-hand area of the screen.

**Step 3** Mouse over **Configure** from the product tree menu. A drop-down menu appears.

**Step 4** Choose **Configure <CSC SSM name>**. The managed product's Web-based console or Control Manager-generated console appears.

**Step 5** Log in and configure the managed CSC SSM from the web console.

## Issuing Tasks to the CSC SSM

Use the Tasks tab to make certain tasks available for a group or specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines.
- Deploy pattern files or cleanup templates.
- Deploy program files.
- Enable or disable Real-time Scan.
- Start Scan Now.

You can deploy the latest spam rules, patterns, or scan engine to managed products with outdated components.

**Note** The Control Manager server has already been updated with the latest components from the Trend Micro ActiveUpdate server.

You can perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to managed products, follow these steps:

**Step 1** From the Control Manager console, go to the Product Directory.

**Step 2** On the left-hand menu, choose the desired managed product or folder.

**Step 3** Click the **Tasks** tab.

**Step 4** Choose the task from the Select task list.

**Step 5** Click **Next.**

**Step 6** Monitor the progress through Command Tracking.

**Step 7** To view command information, click the **Command Details** link in the response screen.

## Querying and Viewing Managed CSC SSM Product Logs

Use the Configure tab to query and view logs for a group or specific managed CSC SSM using the CSC SSM console.

To query and view managed CSC SSM logs, follow these steps:

**Step 1** From the Control Manager console, click **Products** to show the Product Directory.

**Step 2** On the left-hand menu, choose the desired managed CSC SSM or folder.

**Step 3** Click the **Configure** tab.

**Step 4** Log in to the CSC SSM console.

**Step 5** Choose **Logs > Query**.

**Step 6** Select the log type form the drop-down menu.

**Step 7** Select the appropriate protocol and time filter.

**Step 8** Select the number of logs to display per page.

**Step 9** Click **Display Log**.

To filter information to be more specific, you can use an ad hoc query. For more information, see the "Creating a New Ad Hoc Query" section on page C-10.

For additional information and instructions about using Trend Micro Control Manager, see the online help or PDF file documentation available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

# Ad Hoc Queries

Trend Micro Control Manager 5.0 supports collecting the data an administrator needs from the Control Manager and managed CSC SSM logs. The Control Manager supports the display of data through the use of ad hoc queries. Ad hoc queries provide administrators with a quick method of extracting information directly from the Control Manager database. The database contains information collected from all CSC SSMs registered to the Control Manager server. (Log aggregation can affect the data available to query.) Using ad hoc queries to extract data directly from the database provides a very powerful tool for administrators.

When querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis, or save the query for future use. Control Manager also supports the sharing of saved queries, so other users can benefit from useful queries.

An ad hoc query is a direct request to the Control Manager database for information. The query uses data views to narrow the request and improve performance for the information. After specifying the data view, users can further narrow their search by specifying filtering criteria for the request.

When performing an ad hoc query, the user first specifies that the Control Manager server, where the user is currently logged on, should query a CSC SSM that the Control Manager manages.

For more information, see the *Trend Micro Control Manager 5.0 Administrator's Guide* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

# System Requirements

Table C-1 shows the system requirements for using ad hoc queries with the CSC SSM.

***Table C-1 System Requirements for Using Ad Hoc Queries***

| Language | Version of Control Manager | Version of CSC SSM |
|---|---|---|
| English | 5.0 + Patch 3 | 6.6 |
| Japanese | 5.0 + Patch 3 | 6.6 |

# Understanding Ad Hoc Queries

Completing an ad hoc query consists of the following steps:

- Selecting the managed CSC SSM for the query.
- Selecting the Data View to query.
- Specifying filtering criteria and the specific information that appears.
- Saving and completing the query.
- Exporting the data to CSV or XML format.

For example, a CSC SSM administrator wants to check the status of pattern files for the CSC SSM. This administrator selects **Logs/Reports > New Ad Hoc Query**, then selects the managed CSC SSM from the Select Product tree and clicks **Next**. Under Product Information > Component Information, the administrator chooses the data view for Pattern File/Rule Status Summary. Proceeding to the next step, the administrator clicks **Change column display** and selects four fields that the query will display: Pattern/File Rule Name, Pattern/File Rule Version, Pattern/File Rule Up-to-Date, and Pattern/File Rule Out-of-Date. The administrator returns to the Results Display Settings and clears the Custom Criteria check boxes. After clicking **Query**, the results for the query that the administrator created appear. The results can then be exported to CSV or XML format, if needed.

# Understanding Data Views

A data view is a table consisting of clusters of related data cells. Data views provide the foundation on which users perform ad hoc queries of the Control Manager database. The Control Manager separates data views into two major categories: Product Information and Security Threat Information.

For more information about data views, see Appendix B of the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

The Control Manager web console displays the types of data views and the information available from each type.

***Table C-2 Control Manager Major Data View Categories***

| Major Data View Category | Details |
|---|---|
| Product Information | Managed Product Information includes:<br>• CSC SSM Distribution Summary<br>• CSC SSM Status Information<br>• CSC SSM Event Information<br>Component Information includes:<br>• CSC SSM Scan Engine Status<br>• CSC SSM Pattern File/Rule Status<br>• CSC SSM Component Deployment<br>• Scan Engine Status Summary<br>• Pattern File/Rule Status Summary |
| Security Threat Information | Displays the following information about security threats that managed CSC SSMs detect:<br>• Virus/Malware Information<br>• Spyware/grayware Information<br>• Content Violation Information<br>• Spam Violation Information<br>• Web Violation/Reputation Information<br>• Overall Threat Information |

# Creating a New Ad Hoc Query

After you create and save an ad hoc query, you can run that query as often as needed. This example shows how to create a query that displays a summary of detected web violations.

To create a new ad hoc query, perform the following steps:

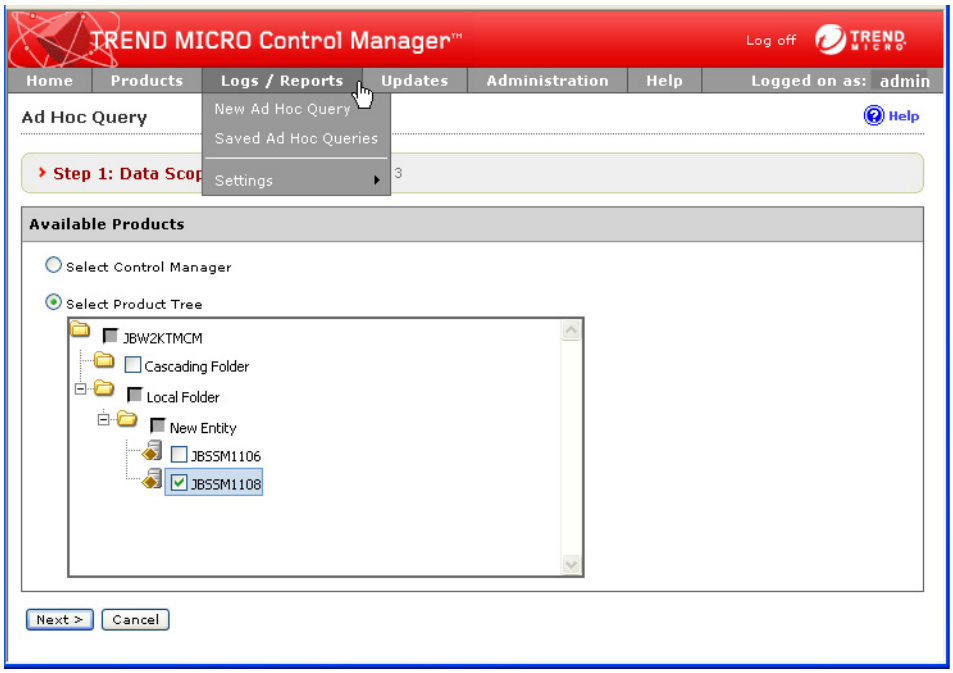
**Step 1** Point to **Logs/Reports** on the main menu.

**Step 2** Click **New Ad Hoc Query**. The Available Products screen appears.

**Step 3** Click the **Select Product Tree** radio button to specify that the query data should originate from the managed CSC SSM(s) and not Control Manager. See Figure C-2.

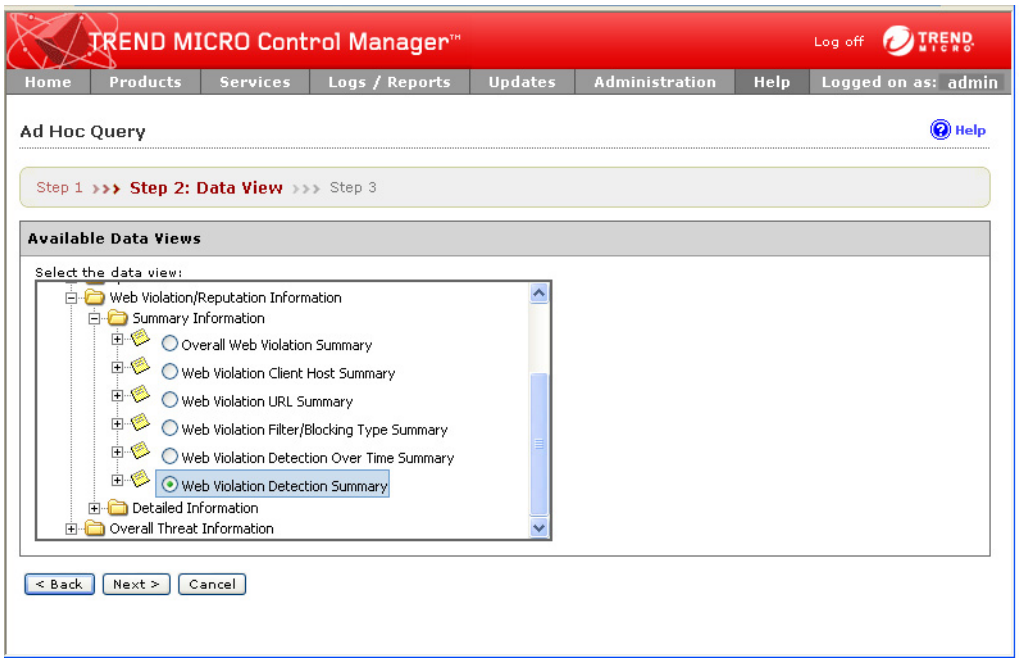
**Step 4** Check the check box to designate which managed CSC SSM(s) to query or select a folder to query all the products in that folder.

***Figure C-2 Step 1: Data Scope***




**Step 5** Click **Next** to select the data view. The Ad Hoc Query Step 2: Select Data View screen appears. See Figure C-3.

*Figure C-3 Step 2: Select the Data View*




**Step 6** Specify the data view for the log by performing the following steps:

**a.** Select the data to query from the Available Data Views area.

Select multiple items using the Shift or Ctrl key.

**b.** Click **Next**. The Step 3: Query Criteria screen appears. See Figure C-5.

**Note** Selecting CSC SSM in the managed product/directory dictates the data views that are available in the Data Views list to those associated with the CSC SSM. For more information about data views, see the "Understanding Data Views" section on page C-10 or the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

**Step 7** Specify the data to appear in the log and the order in which the data appears by doing the following:

**a.** Click **Change column display**. The Select Display Sequence screen appears. See Figure C-4.

*Figure C-4 Select Fields to Display and Arrange Order*


**b.** To remove fields, select them in the Selected Fields list.

Select multiple items using the Shift or Ctrl key.

**c.** Click the less than sign (**<**) to remove unnecessary fields.

**Note** Items appearing at the top of the Selected Fields list appear in the left-most column of the query results table. Removing a field from Selected Fields list removes the corresponding column from the ad hoc query returned table.

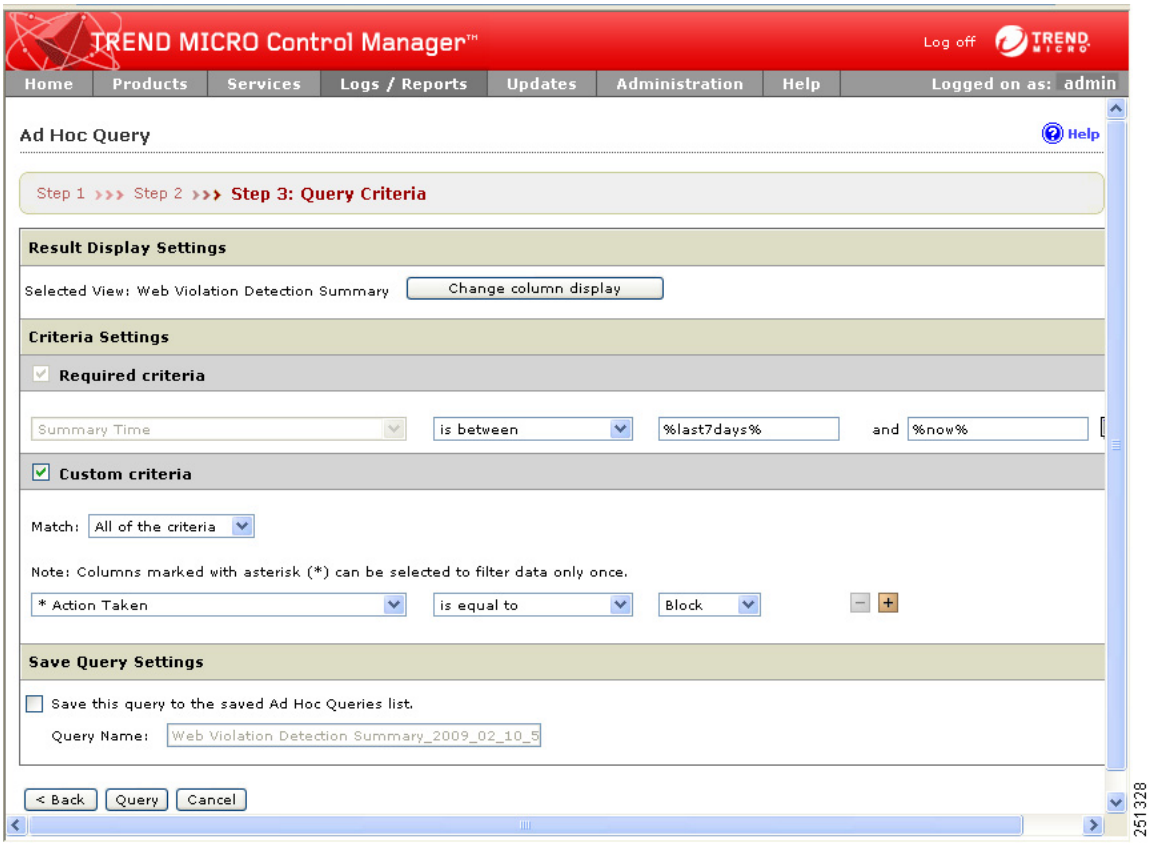
**d.** Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

**e.** Click **Back** when the sequence fits your requirements.

**Step 8** Specify the filtering criteria for the data:

**Note** When querying for summary data, you must specify the items under Required criteria.

*Figure C-5 Setting Required and Custom Criteria*




Required criteria

- Specify a Summary Time for the data. The default is between the “last 7 days” and “now.”

Custom criteria

a. Specify the criteria filtering rules for the data categories:
   - **All of the criteria:** This selection acts as a logical “AND” function. Data appearing in the report must meet all the filtering criteria.
   - **Any of the criteria:** This selection acts as a logical “OR” function. Data appearing in the report must meet any of the filtering criteria.

b. Specify the filtering criteria for the data. The Control Manager supports up to 20 criteria for filtering data.

**Tip** If you do not specify any filtering criteria, the ad hoc query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

**Step 9** (Optional) To save the query, perform the following steps:

a. Click the **Save this query to the saved Ad Hoc Queries list** check box.

b. Type a name for the saved query in the Query Name field. The default name is Web Violation Detection Summary_<date>. For example, type “Web Violation Detection Summary_last7days.”

**Step 10** Click **Query**. The Results screen appears.

**Step 11** (Optional) To save the report to CSV format:

a. Click **Export to CSV**. A dialog box appears.

b. Click **Save**. A Save As dialog box appears.

c. Specify the location to save the file.

d. Click **Save**.

**Step 12** (Optional) To save the report to XML format:

a. Click **Export to XML**. A dialog box appears.

b. Click **Save**. A Save As dialog box appears.

c. Specify the location to save the file.

d. Click **Save**.

**Tip** To query for more results on a single screen, select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

**Step 13** (Optional and only necessary if not saved in Step 9.) To save the settings for the query, do the following:

a. Click **Save query settings**. A confirmation dialog box appears.

b. Accept the default name for the query or type a different name in the **Query Name** field.

c. Click **OK**.

d. To locate the saved query, choose **Logs/Report > Saved Ad Hoc Queries > My Queries**.

# Performing an Ad Hoc Query

The "Creating a New Ad Hoc Query" section on page C-10 shows how to create a sample ad hoc query called "Web Violation Summary_last7days." That query shows a summary of web violations for the last week. You can run this saved query as many times as needed.

This section includes the following topics:

- Available Headings in the Web Violation Query, page C-16
- Creating an Available Query, page C-17
- Running an Available Query, page C-18

## Available Headings in the Web Violation Query

The "Web Violation Summary_last7days" sample query created in the "Creating a New Ad Hoc Query" section on page C-10 shows the statistics described in Table C-3.

***Table C-3 Details Available in the Prepackaged Ad Hoc Query***

| Parameter | Shows | Drills Down to |
|---|---|---|
| Unique Policies in Violation Count | Number of policies violated | • Name of violated policy<br>• Filter/Blocking type such as URL filtering, web reputation, or file name<br>• Number of unique clients in violation count*<br>• Number of unique URLs in violation count*<br>• Number of web violation detection count* |
| Unique Clients in Violation Count | Number of clients in violation | • IP address of the host of the client in violation<br>• Number of unique policies in violation*<br>• Number of unique URLs in violation*<br>• Number of web violation detection count* |
| Unique URLs in Violation Count | Number of URLs in Violation. Drills | • URL in violation<br>• Filter/Blocking type such as URL filtering, web reputation, or file name<br>• Number of unique clients in violation*<br>• Number of web violation detection count* |
| Unique Users/IP Addresses in Violation Count | Number users in violations | • IP address or user name (if available) involved in the violation<br>• Web violation detection count* |
| Unique User Groups in Violation Count | Number of user groups in violation | • Name of the group involved in the violations<br>• Number of unique users/IP addresses in violation count*<br>• Number of web violation detection count* |

*Table C-3 Details Available in the Prepackaged Ad Hoc Query (continued)*

| Parameter | Shows | Drills Down to |
|---|---|---|
| Web Violation Detection Count | Number of web violations | • Time received from entity<br>• Time generated at entity<br>• Entity display name*<br>• Managed product name<br>• Inbound/Outbound traffic/connection<br>• Protocol involved (HTTP or FTP)<br>• URL involved in the violation<br>• User name or IP address involved in the violation<br>• User group involved in the violation<br>• IP address of the client host<br>• IP address of the server host<br>• Filter or blocking type<br>• Name of the blocking rule violated<br>• Name of the policy violated<br>• File in violation (if any)<br>• Web reputation rating (if applicable)<br>• Action taken: block or pass for example<br>• Number of web violations detected |

*Item drills down to further details.

## Creating an Available Query

The web violations query created in the "Creating a New Ad Hoc Query" section on page C-10 was saved to the saved queries list on the My Queries tab, which means it can only be run by the administrator who created it. The Control Manager supports the modification of a personal, saved ad hoc query from the My Queries tab to become an available query, which can be shared with other administrators.

To share a query from My Queries to Available Queries, perform the following steps:

**Step 1** To access My Queries, click the **Logs/Reports > Saved Ad Hoc Queries > My Queries** tab.

**Step 2** Check the check box beside the name of the query to be shared.

**Step 3** Click the **Share** icon.

**Step 4** Verify that the query has been shared by clicking the **Available Queries** tab.

The newly shared query is listed in the Name column. The name of the query creator appears in the Owner column.

## Running an Available Query

Queries available through the Available Queries tab have been created and saved as a shared, available query. See the "Creating an Available Query" section on page C-17 for more information. Saved queries can run as often as needed.

To run an available ad hoc query, perform the following steps:

**Step 1** Mouse over **Logs/Reports** on the main menu. A drop-down menu appears.

**Step 2** Click **Saved Ad Hoc Queries**.

**Step 3** Click the **Available Queries** tab.

**Step 4** Click **View** in the View Results column. The query runs and the results appear.

# Working with Reports

Usage of the reporting feature requires an Advanced License for the Control Manager.

Control Manager reports consist of two parts: report templates and report profiles.

- Report templates determine the look and feel of the reports.
- Report profiles specify the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 allows administrators to design their own custom report templates.

- User-defined customized report templates that use direct database queries (database views) and report template elements (charts, graphs, and tables).
- Users have greater flexibility in specifying the data that appears in their reports compared to report templates from earlier Control Manager versions.

**Note** For more information about Control Manager 5.0 templates, see "Understanding Control Manager 5.0 Templates" in Chapter 6 of the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7