TREND MICRO™

Trend Micro Control Manager™ 5

Tutorial

Control Manager

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, review the readme files, release notes, and the latest version of the Installation Guide, Administrator's Guide, and Tutorial which are available from Trend Micro's Web site at:

www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. TMEM53361/70921

Release Date: February 2008

The Tutorial for Trend Micro Control Manager™ is intended to introduce the main features of the software, installation instructions for your production environment.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

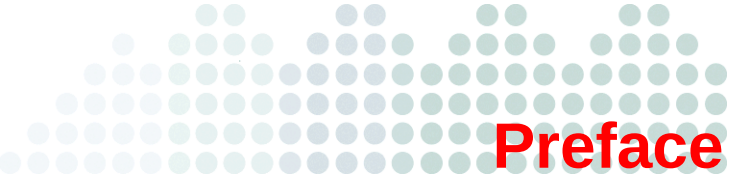
www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 4: Monitoring the Control Manager Network

Chapter 5: Administering Managed Products

Index



Preface

This Tutorial guides you through the end-to-end process of using Trend Micro Control Manager™. Each chapter focuses on a separate topic for Control Manager usage or configuration.

This preface discusses the following topics:

Trend Micro Control Manager™ Documentation

The Trend Micro Control Manager documentation consists of the following:

TABLE PREFACE-1. Control Manager Documentation

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Trend Micro Control Manager management console. The online help contains explanations of Trend Micro Control Manager components and features, as well as procedures needed to configure Control Manager.
Knowledge Base	The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: *http://esupport.trendmicro.com/support*
Readme file	The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and product release history.
Installation Guide	Printed documentation provided in the package contents and PDF form that is accessible from the Trend Micro Enterprise CD or downloadable from the Trend Micro Web site. The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".
Administrator's Guide	PDF documentation that is accessible from the Trend Micro Solutions CD for Trend Micro Control Manager or downloadable from the Trend Micro Web site. The Administrator's Guide contains detailed instructions of how to deploy, install, configure, and manage Control Manager and managed products, and explanations on Trend Micro Control Manager concepts and features.
Tutorial	PDF documentation that is accessible from the Trend Micro Solutions CD for Trend Micro Control Manager or downloadable from the Trend Micro Web site. The Tutorial contains hands on instructions of how to deploy, install, configure, and manage Control Manager and managed products Trend Micro Control Manager.

Note: Trend Micro recommends checking the Update Center at *http://www.trendmicro.com/download/* for updates to the Trend Micro Control Manager™ documentation and program file.

About this Tutorial

The Trend Micro Control Manager Tutorial provides Control Manager administrators with examples of how to install/upgrade, configure, and use Control Manager on your network. Refer to Table 2, "Tutorial High-Level Overview," on page P-iii for information regarding each section of the Tutorial

TABLE PREFACE-2. Tutorial High-Level Overview

TASK	DESCRIPTION
Pre-Installation	*Chapter 1: Preparing the Environment*: Provides system requirements for completing this tutorial.
	Chapter 2: Installing Trend Micro Control Manager for the First Time: Provides deployment and product application information
Post Installation	*Chapter 3: Getting Started with Control Manager*: Provides information on basic Web console navigation, creating and importing users, updating the server and managed products
	Chapter 4: Monitoring the Control Manager Network: Provides information on interpreting and monitoring the Control Manager environment, such as, configuring notifications, generating reports, and collecting logs
	Chapter 5: Administering Managed Products: Provides information on managing the Control Manager network and managed products
	Chapter 6: Removing Trend Micro Control Manager: Provides information on removing Control Manager from your computer
Appendices	*Appendix A: Understanding Data Views*: Provides a description of the data columns used in Ad Hoc Queries and report templates

Audience

The Control Manager documentation assumes a basic knowledge of security systems. There are references to previous versions of Control Manager to help system administrators and personnel who are familiar with earlier versions of the product. If you have not used earlier versions of Control Manager, the references may help reinforce your understanding of the Control Manager concepts.

Document Conventions

To help you locate and interpret information easily, the Control Manager documentation uses the following conventions.

TABLE PREFACE-3. Control Manager Documentation Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Monospace	Examples, sample command lines, program code, and program output
Note:	Provides configuration notes or recommendations
Tip:	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about processes that may harm your network

Chapter 1

Preparing the Environment

This chapter provides information on the items required to complete this tutorial. The chapter discusses the following topics:

System Specifications

Wherever possible the Trend Micro recommended system requirements for Control Manager servers are used. This Tutorial uses a server with the following specifications for Control Manager installation:

TABLE 1-1. Control Manager Server Specifications

HARDWARE & SOFTWARE REQUIREMENTS	SPECIFICATIONS
CPU	Intel™ Pentium™ III 600MHz
Memory	4GB RAM
Disk space	A hard drive with 80GB of free disk space
Operating system	Microsoft™ Windows™ 2003 Server Standard Edition SP 1/SP 2
Web server	Microsoft™ IIS server 6.0 (For 2003 platform)
Database	Microsoft SQL 2005 Server
Management console	Browser- Microsoft Internet Explorer 7.0

About the Control Manager Managed Product Network

For the purpose of this tutorial, a company (ACME Co.) will represent a large multi-national company. ACME Co. has offices in Asia, Europe, and North and South America. ACME Co. has one Control Manager server, with a number of managed products registered to the Control Manager server.

To use all of Control Manager's features and view, log, and query information, Control Manager requires at least one managed product. This tutorial uses the following managed product for the simulated Trend Micro managed product network

TABLE 1-2. Managed Product Servers and Users

MANAGED PRODUCT	USERS			
	GLOBAL	REGIONAL	LOCAL	LIMITED
OfficeScan 8.0	Alex	Blair	Chris	Dana
Control Manager	Erin			

- **Global users:** Have complete control over all managed products of a specific type world wide
- **Regional users:** Have complete control over all managed products of a specific type on a continent
- **Local Users:** Have complete control over a number of managed products of a specific type in a country
- **Limited:** Have limited access to the managed products

Example: Using the table above, Alex is the global OfficeScan administrator. She has access to all OfficeScan servers worldwide. Blair is the administrator for all OfficeScan servers in Europe. Chris is the OfficeScan administrator for all servers in England. While Dana is Chris' manager and only requires access to the reports, that Chris generates.

Chapter 2

Installing Trend Micro Control Manager for the First Time

This chapter guides you through installing Control Manager server. In addition to listing the system requirements for the Control Manager server the chapter also contains post-installation configuration information as well as instructions on how to register and activate your software.

This chapter contains the following topics:

System Requirements

Individual company networks are as individual as the companies themselves. Therefore, different networks have different requirements depending on the level of complexity. This section describes both minimum system requirements and recommended system requirements, including general recommendations and recommendations based on the size of networks.

Minimum System Requirements

The following table lists the minimum system requirements for a Control Manager server.

Note: Minimal requirements of child Control Manager server:

- Control Manager 3.0
- Control Manager 3.0 SP1 to SP6
- Control Manager 3.5
- Control Manager 5.0 Advanced

Control Manager 2.5 cannot be part of a cascading environment.

Refer to the managed product documentation for detailed agent system requirements.

TABLE 2-1. Control Manager server hardware minimum system requirements

HARDWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
CPU	Intel™ Pentium™ III 600MHz or higher • Single CPU • Dual CPU • Quad CPU
Memory	2GB RAM (4GB recommended)
Disk space	• 790MB for Control Manager Standard and Advanced • 300MB for SQL2005 Express (Optional)

TABLE 2-2. Control Manager server software minimum system requirements

SOFTWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
Operating system	• Microsoft™ Windows™ 2000 Server SP 3/SP 4 • Windows 2000 Advanced Server SP 3/SP 4 • Windows 2003 Server Standard Edition SP 1/SP 2 • Windows 2003 Server Standard Edition R2 without patches/SP 1 • Windows 2003 Server Enterprise Edition SP 1/SP 2 • Windows 2003 Server Enterprise Edition R2 without patches/SP 1 • WOW, 64 bit architecture of Windows 2003 Standard/Enterprise
Web server	• Microsoft IIS server 5.0 (For 2000 platform) • Microsoft IIS server 6.0 (For 2003 platform)
Database	• Microsoft Data Engine (MSDE) 2000 + SP3 • Microsoft SQL Server 2000 (2000 + SP3 is recommended) • Microsoft SQL 2005 Express • Microsoft SQL 2005 Server
Others	• SQL ODBC driver 3.7 or higher • Windows Installer 3.1 (included in Control Manager package) • MDAC 2.8 SP1 or higher • .Net Framework 2.0 (included in Control Manager package) • Visual C 2005 SP1 Redistribution Package (included in Control Manager package)
Management console	• Browser- Windows Internet Explorer 6 or higher • Java VM- Microsoft Version 5.0.0.3805 or higher • JRE 1.4.2 or 1.5.0

Refer to the URL below to download the latest Control Manager agents:

http://www.trendmicro.com/en/products/management/tmcm/evaluate/requirements.htm

Installing Control Manager Server

After deciding the topology to use for your network, you can begin to install your Control Manager server.

You need the following information for the installation:

- Relevant target server address and port information
- Control Manager registration key
- Security Level you want to use for Server-Agent communication

The following are database-related considerations:

- Decide if you want to use an SQL server with Control Manager. If the SQL server is located on a server other than the Control Manager server, obtain its IP address, fully qualified domain name (FQDN), or NetBIOS name. If there are multiple instances of the SQL server, identify the one that you intend to use
- Prepare the following information about the SQL database for Control Manager:
  - User name for the database
  - Password

  Note: Control Manager uses both Windows authentrication and SQL authentrication to access the SQL server.

- Determine the number of managed products that Control Manager will handle. If an SQL server is not detected on your server, Control Manager will install SQL Express 2005 SP2, which can only handle a limited number of connections

Installing Control Manager requires performing the following steps:

Step 1: Install all required components

Step 2: Specify the installation location

Step 3: Register and activate the product and services

Step 4: Specify Control Manager security and Web server settings

Step 5: Specify backup settings and configure database information

Step 6: Set up root account and configure notification settings

Tip: Trend Micro recommends upgrading to version 5.0 instead of doing a fresh installation.

To install a Control Manager server:

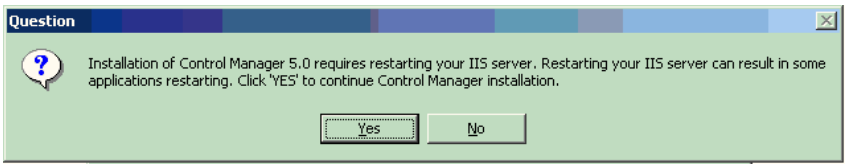
Step 1: Install all required components

1. On the Windows taskbar, click **Start** > **Run**, and then locate the Control Manager installation program (Setup.exe). If installing from the Trend Micro Enterprise Protection CD, go to the Control Manager folder on the CD. If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your computer. The installation program checks your system for required components.

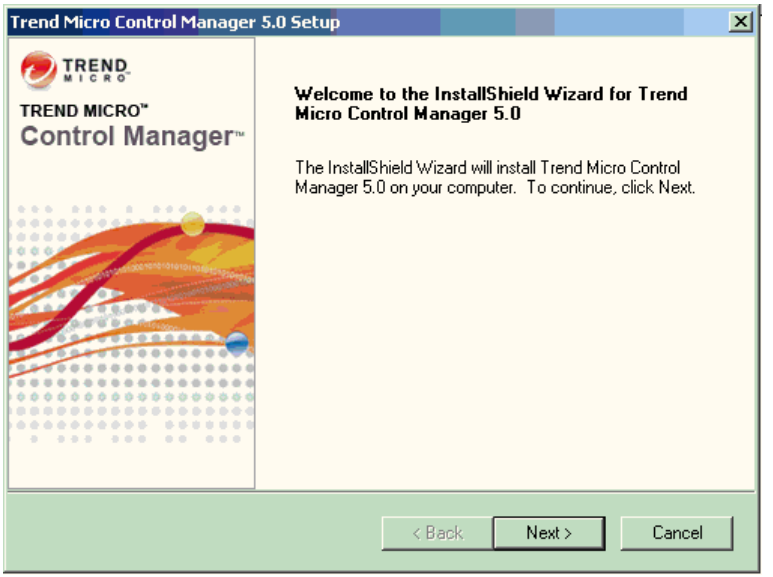
   If the installation program does not detect the following components on the server, dialog boxes appear prompting you to install the missing components:

   - **Windows Installer 3.1:** This component is included in the Control Manager installation package
   - **MDAC 2.8 SP1 or higher:** This component is **not** included in the Control Manager installation package
   - **.Net Framework 2.0:** This component is included in the Control Manager installation package
   - **Visual C 2005 SP1 Redistribution Package:** This component is included in the Control Manager installation package

2. Install all missing components. The IIS confirmation dialog box appears.



3. Click **Yes** to continue the installation. The Welcome screen appears.



The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the Microsoft Management Console.

4. Click **Next**. The Software License Agreement appears.

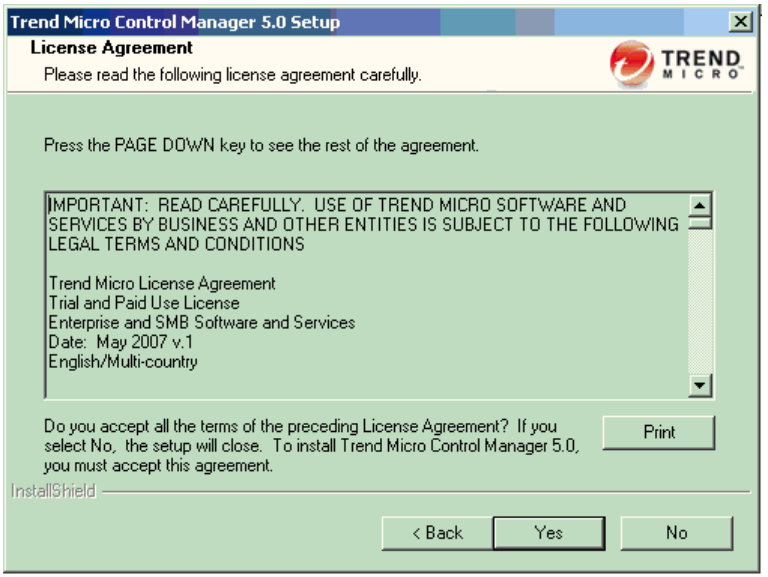


FIGURE 2-1. Choose Yes to agree with the License Agreement

If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**. A summary of detected components appears.

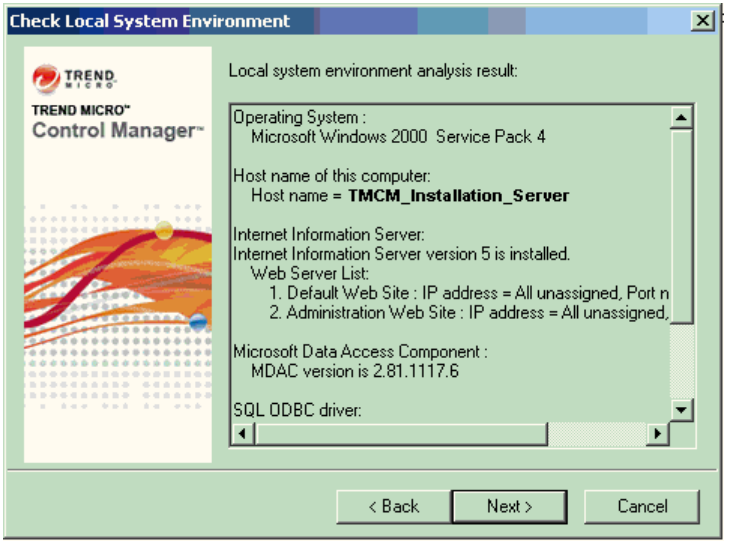


FIGURE 2-2. Displays local system environment information

Step 2: Specify the installation location

1. Click **Next**. The Select Destination Folder screen appears.

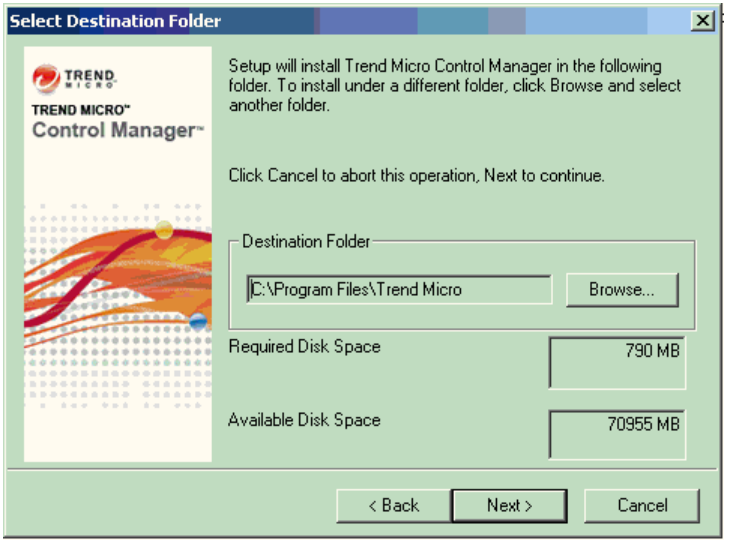


FIGURE 2-3. Select a destination folder

2. Specify a location for Control Manager files. The default location is `C:\Program Files\Trend Micro`. To change this location, click **Browse**, and then specify an alternate location.

Note: The setup program installs files related to the Control Manager communication, (the Trend Micro Management Infrastructure and MCP) in predetermined folders in the Program files folder.

Step 3: Register and activate the product and services

1. Click **Next**. The Product Activation screen appears.

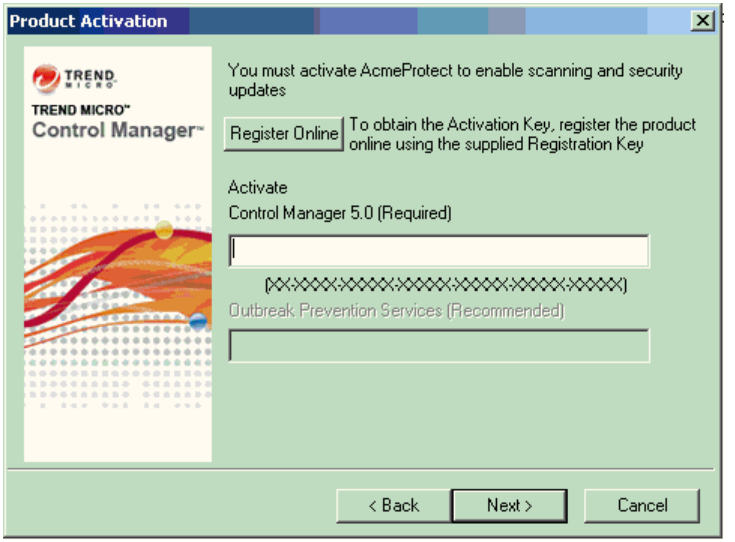


FIGURE 2-4. Enter the Activation Code to activate Control Manager and services

2. Type the Activation Code for Control Manager and any other additional purchased services (you can also activate optional services from the Control Manager console). To use the full functionality of Control Manager 5.0 and other services (Outbreak Prevention Services), you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key that you use to register your software online to the Trend Micro Online Registration Web site and obtain an Activation Code.

3. Click **Next**. The World Virus Tracking screen appears.

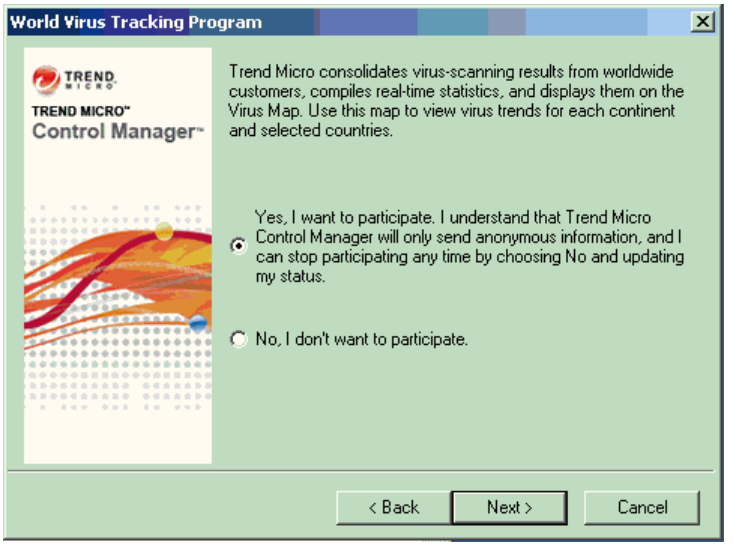


FIGURE 2-5. Participate in the World Virus Tracking Program

4. Click **Yes** to participate in the World Virus Tracking Program. You can add your data to the Trend Micro Virus Map by choosing to participate in the World Virus Tracking Program. When you choose to participate, Trend Micro Control Manager will only send anonymous information through HTTP, and you can stop participating any time by choosing No and updating your status on the Control Manager management console.

Step 4: Specify Control Manager security and Web server settings

1. Click **Next**. The Select Security Level And Host Address screen appears.

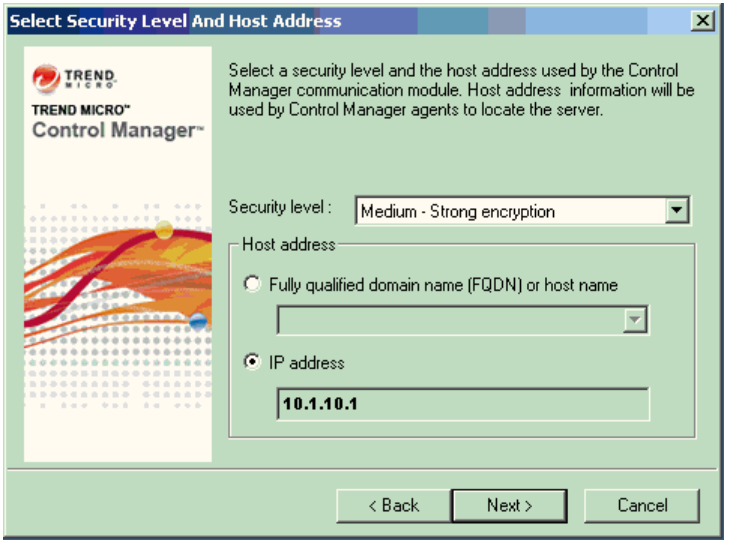


FIGURE 2-6. Select a security level

2. From the Security level list, select the security level for Control Manager communication with agents. The options are as follows:
   - **High:** All communication between Control Manager and managed products use 128-bit encryption with authentication. This ensures the most secure communication between Control Manager and managed products.
   - **Medium:** If supported, all communication between Control Manager and managed products use 128-bit encryption. This is the default setting when installing Control Manager.
   - **Low:** All communication between Control Manager and managed products use 40-bit encryption. This is the least secure communication method between Control Manager and other products.
3. Select a host address for agents to communicate with Control Manager:

Tip: Trend Micro recommends installing Control Manager using a host name. Installing using an IP address can cause issues if the IP address of the Control Manager server requires changing. Control Manager does not support changing the installation IP address. This results in an administrator having to reinstall Control Manager if the server's IP address must change. Installing using a host name avoids the issue.

To use a FQDN/host name:

a. Select **Fully qualified domain name (FQDN) or host name**.

b. Select or type an FQDN or host name in the accompanying field.

To use an IP address:

a. Select **IP address**.

b. Type an IP address in the accompanying field. Separate multiple entries using a semi-colon (**;**).

4. Click **Next**. The Specify Web Server Information screen appears.

   The settings on the Specify Web Server Information screen define communication security and how the Control Manager network identifies your server.

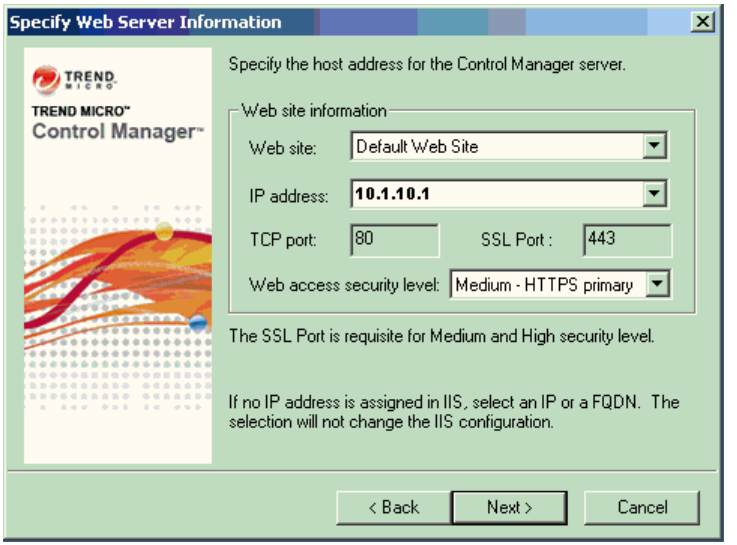


FIGURE 2-7. Specify Web server information

5. From the **Web site** list, select the Web site to access Control Manager.
6. From the **IP address** list, select the IP address or FQDN/host name you want to use for the Control Manager Management Console. This setting defines how the Control Manager communication system identifies your Control Manager server. The setup program attempts to detect both the server's fully qualified domain name (FQDN) and IP address and displays them in the appropriate field.

   If your server has more than one network interface card, or if you assign your server more than one FQDN, the names and IP addresses appear here. Choose the most appropriate address or name by selecting the corresponding option or item in the list.

   If you use the host name or FQDN to identify your server, make sure that this name can be resolved on the product machines; otherwise the products cannot communicate with the Control Manager server.

7. From the **Web access security level** list, select the security level for Control Manager communication. The options are as follows:
   - **High - HTTPS only:** All Control Manager communication uses HTTPS protocol. This ensures the most secure communication Control Manager and other products.
   - **Medium - HTTPS primary:** If supported all Control Manager communication uses HTTPS protocol. If HTTPS is unavailable, agents use HTTP instead. This is the default setting when installing Control Manager.
   - **Low - HTTP based:** All Control Manager communication uses HTTP protocol. This is the least secure communication method between Control Manager and other products.
8. If you selected **Low - HTTP based**, and if you have not specified an SSL Port value in the ISS administration console, specify the access port for Control Manager communication in the **SSL Port** field.

Step 5: Specify backup settings and configure database information

1. Click **Next**. The Choose Destination Location screen appears.

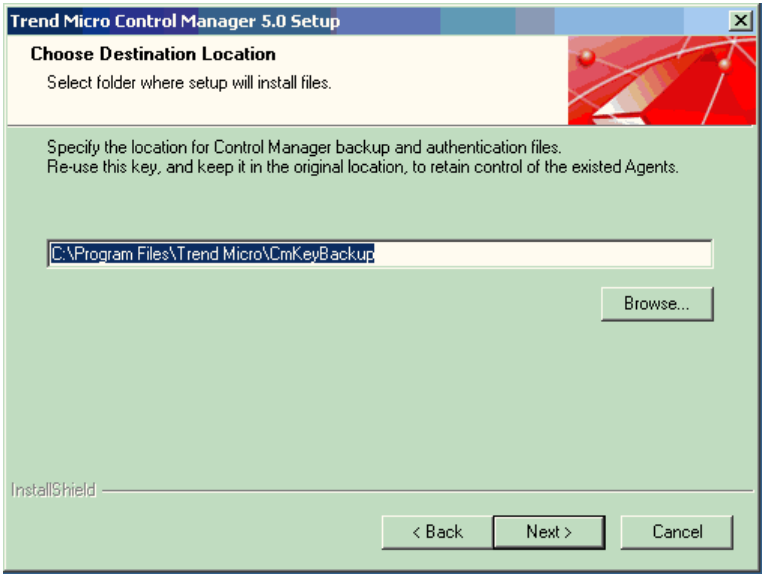


FIGURE 2-8. Choose a destination location for backup and authentication files

2. Specify the location of the Control Manager backup and authentication files. Click **Browse** to specify an alternate location.

3. Click **Next**. The Setup Control Manager Database screen appears.

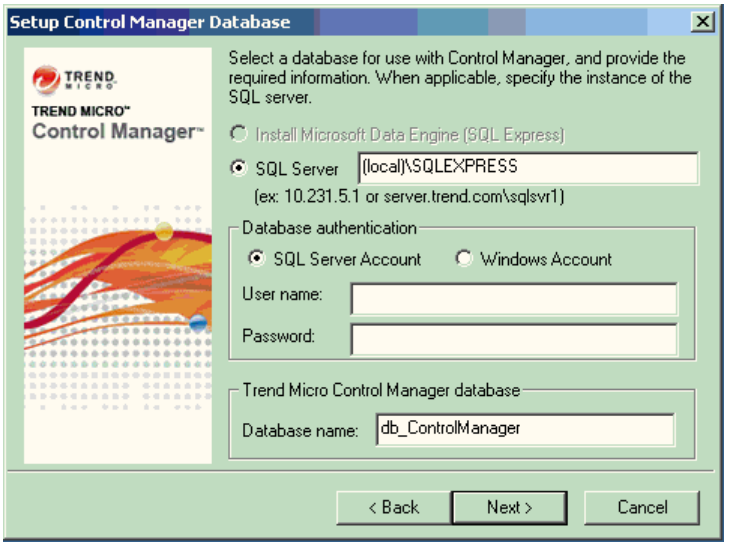


FIGURE 2-9. Choose the Control Manager database

4. Select a database to use with Control Manager.
   - **Install Microsoft SQL Express** - the setup program automatically selects this option if an SQL server is not installed on this machine. Do not forget to specify a password for this database in the field provided.

Tip: The Microsoft SQL Express is suitable only for a small number of connections. Trend Micro recommends using an SQL server for large Control Manager networks.

   - **SQL Server** - the setup program automatically selects this option if the program detects an SQL server on the server. Provide the following information:
     - **SQL Server (\Instance)** - this server hosts the SQL server that you want to use for Control Manager. If an SQL server is present on your server, the setup program automatically selects it.

To specify an alternative server, identify it using its FQDN, IP address, or NetBIOS name.

If more than one instance of SQL server exists on a host server (this can be either the same server where you are installing Control Manager, or another server), you must specify the instance. For example:

```
your_sql_server.com\instance
```

- **SQL Server Authentication** - provide credentials to access the SQL server. By default, the User name is "sa".

WARNING! **For security reasons, do not use an SQL database that is not password protected.**

5. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is "db_ControlManager".
6. Click **Next** to create the required database. If the setup program detects an existing Control Manager database you have the following options:
   - **Append new records to existing database**- the Control Manager you install retains the same settings, accounts, and Product Directory entities as the previous server. In addition, Control Manager retains the root account of the previous installation - you cannot create a new root account.

   Note: When installing Control Manager 5.0, you cannot select **Append new records to existing database** for previous Control Manager database versions.

   - **Delete existing records, and create a new database**- the existing database is deleted, and another, using the same name, is created
   - **Create a new database with a new name**- you are returned to the previous screen to allow you to change your Control Manager database name

   Note: If you append records to the current database, you will not be able to change the root account. The Root account screen appears.

Step 6: Set up root account and configure notification settings

1. Click **Next**. The following screen appears:

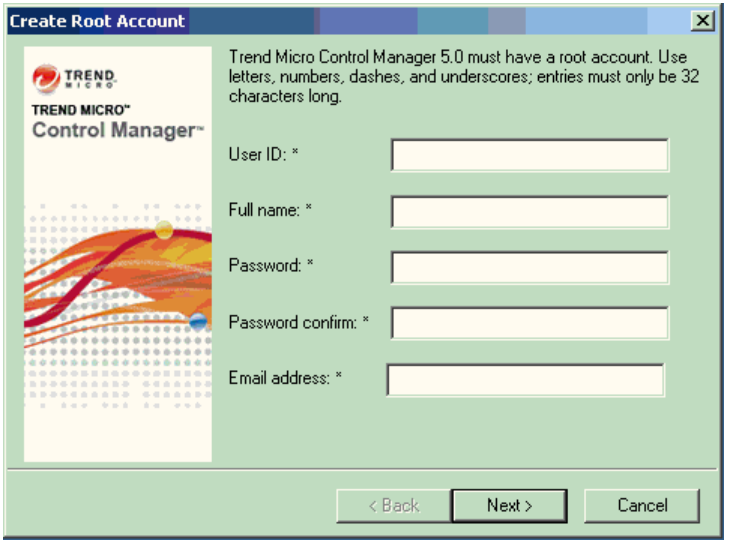


FIGURE 2-10. Provide information for the Control Manager root account

2. Provide the following required account information for the Control Manager root account:
   - User ID
   - Full name
   - Password
   - Password confirmation
   - Email address

3. Click **Next**. The Specify Message Routing Path screen appears. This screen only appears if the host server does not have TMI installed.

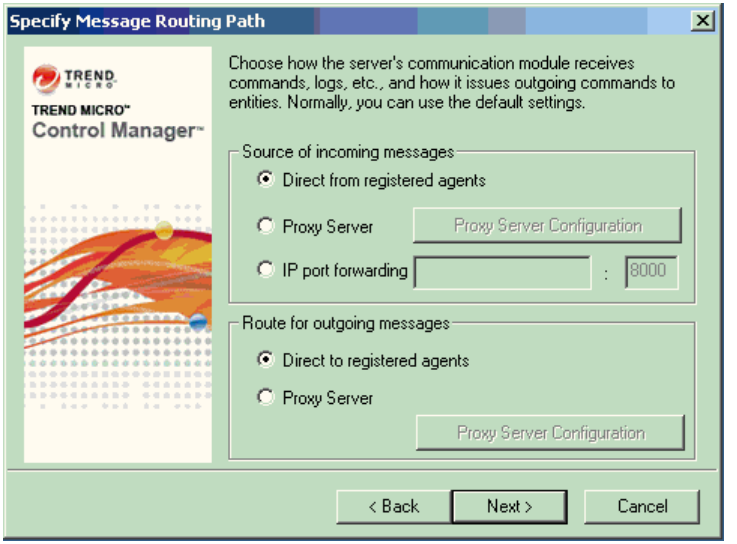


FIGURE 2-11. Define routes for messages or requests

4. Define the routes for incoming and outgoing messages or requests. These settings allow you to adapt Control Manager to your company's existing security systems. Select the appropriate route.

Note: Message routing settings are only set during installation. Proxy configurations made here are not related to the proxy settings used for Internet connectivity–though the same proxy settings are used by default.

Source of incoming messages

- **Direct from registered agents**- the agents can directly receive incoming messages.
- **Proxy server**- uses a proxy server when receiving messages.
- **IP port forwarding**- this feature configures Control Manager to work with the IP port forwarding function of your company's firewall. Provide the firewall server's FQDN, IP address or NetBIOS name, and then type the port number that Control Manager opened for communication.

Route for outgoing messages

- **Direct to registered agents** - Control Manager sends outgoing messages directly to the agents.
- **Proxy server** - Control Manager sends outgoing messages through a proxy server.

5. Click **Finish** to complete the installation.

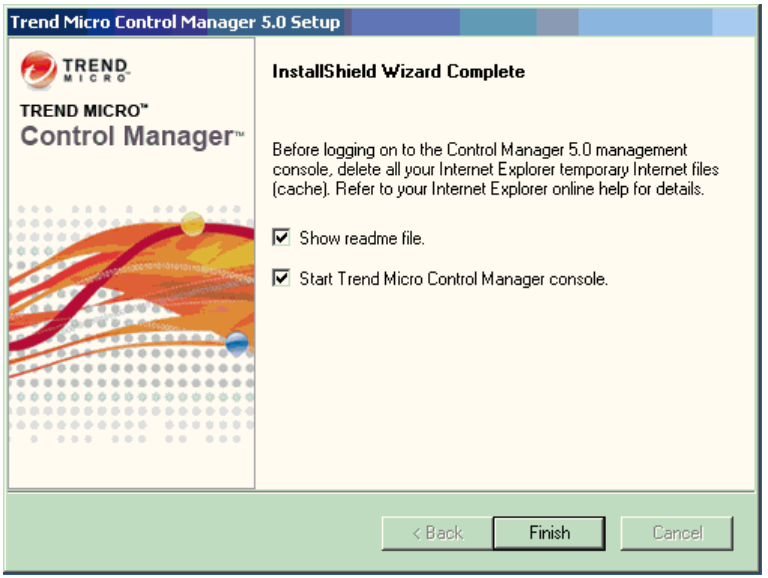


FIGURE 2-12. Setup complete

Verifying a Successful Installation

Follow the procedures below to confirm that Control Manager server has successfully installed.

To confirm a successful Control Manager server installation, check the following:

The following folders appear under the `Program Files\Trend Micro` directory:

- Common\TMI
- Common\CCGI
- Control Manager

The setup program creates the following services:

- Trend Micro Control Manager
- Trend Micro Common CGI
- Trend Micro Management Infrastructure
- Trend Micro Network Time Protocol

The following processes are running:

CCGI processes:

- Jk_nt_service.exe
- Java.exe

IIS process:

- Inetinfo.exe (Internet Information Services)

ISAPI filters:

- CCGIRedirect
- ReverseProxy
- TmcmRedirect

TMI processes:

- CM.exe (TMI-CM)
- MRF.exe (Message Routing Framework Module)
- DMServer.exe (TMI-DM full-function)

Control Manager processes:

- ProcessManager.exe
- LogReceiver.exe
- MsgReceiver.exe
- LogRetriever.exe
- CmdProcessor.exe
- UIProcessor.exe
- ReportServer.exe
- NTPD.exe
- DCSProcessor.exe
- CasProcessor.exe

Registering and Activating Control Manager

After installing Control Manager server, activate the server to continue the tutorial. To activate Control Manager, register online and obtain an Activation Code using your Registration Key.

If you install Control Manager for the first time:

- You have purchased the full version from a Trend Micro reseller, the Registration Key is included the product package

  Register online and obtain an Activation Code to activate the product

- You install an evaluation version

  Obtain a full version Registration Key from your reseller and then follow the full version instructions to activate the product.

Activating Control Manager

Activating Control Manager allows you to use its full functionality, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Note: After activating Control Manager, log off and then log on for changes to take effect.

To register and activate Control Manager:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.

3. Click **Control Manager**. The License Information screen appears.
4. Click the **Activate the product** or **Specify a new Activation Code** link.
5. In the **New** box, type your Activation Code. If you do not have an Activation Code, click the **Register online** link and follow the instructions on the Online Registration Web site to obtain one.
6. Click **Activate**, and then click **OK**.

Renewing Product Maintenance

Renew maintenance for Control Manager or its integrated related products and services (that is, Outbreak Prevention Services) using one of the following methods.

To renew your product or service maintenance, first obtain an updated Registration Key. The Registration Key allows you to acquire a new Activation Code. The procedures for renewing your product maintenance differ depending on whether you are using an evaluation or full version.

To renew product maintenance using Check Status Online:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.
4. On the working area under **Control Manager License Information**, click **Check Status Online**, and then click **OK**.
5. Log off and then log on to the Web console for changes to take effect.

To renew maintenance by manually providing an updated Activation Code:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.
4. On the working area under **Control Manager License Information**, click the **Activate the product** link.
5. Click the **Specify a new Activation Code** link and follow the instructions on the Online Registration Web site.
6. In the **New** box, type your Activation Code.
7. Click **Activate**.
8. Click **OK**.

Chapter 3

Getting Started with Control Manager

The Control Manager Web-based management console allows you to administer managed products and other Control Manager servers.

This chapter presents the tasks that let you configure the Control Manager network including details on how to:

Building the Product Directory Structure

Managed products display as icons in the Control Manager management console Product Directory. These icons change with the status of the managed product. Managed products belonging to client Control Manager servers cannot have tasks applied to them by the parent Control Manager server.

You can group managed products according to geographical, administrative, or product specific reasons. Each grouping offers advantages and disadvantages:

TABLE 3-1. Advantages and disadvantages when grouping managed products

GROUPING TYPE	ADVANTAGE	DISADVANTAGE
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

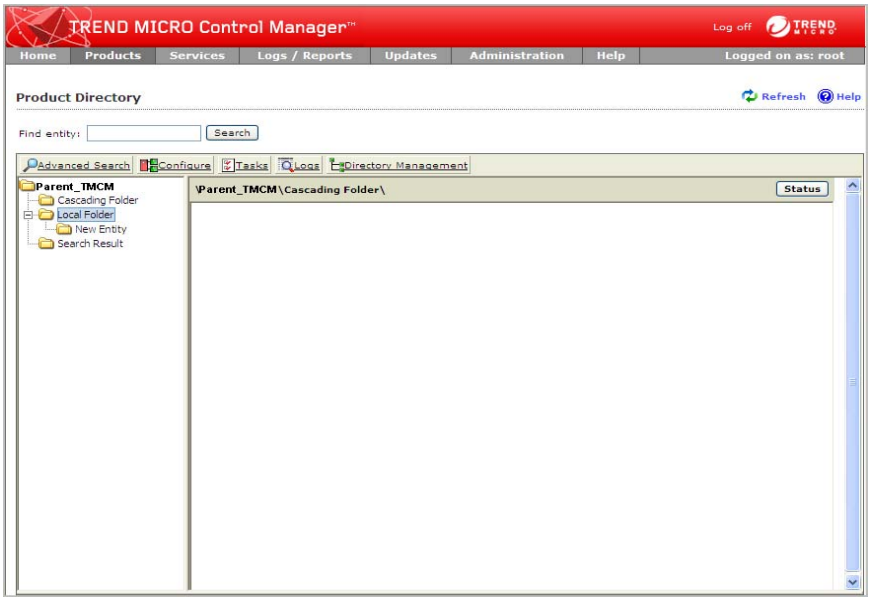
This tutorial uses a mixture of the grouping types, with product type at the top of the structure, followed by geographical location, and finally administrative function.

Note: Control Manager reorders structures alphabetically after you specify your Product Directory structure using the Directory Management dialog box.

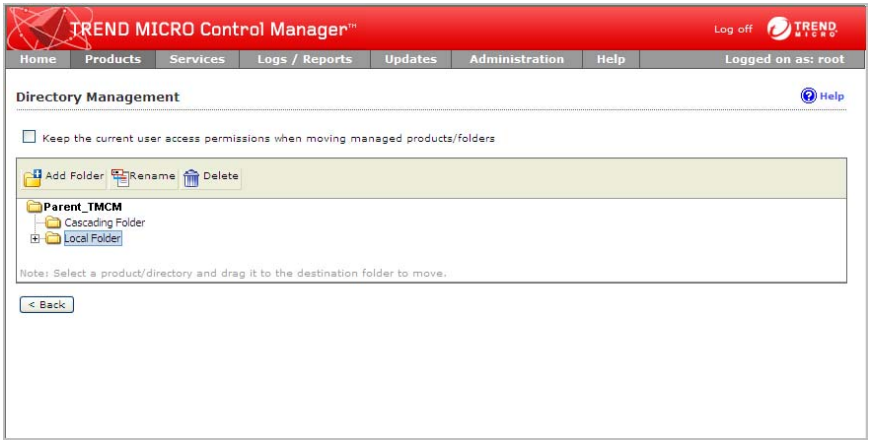
To build the Product Directory structure:

1. Log on to the Control Manager Web console using the root account information you provided during installation. See *Step 6: Set up root account and configure notification settings* on page 2-19 for more information.

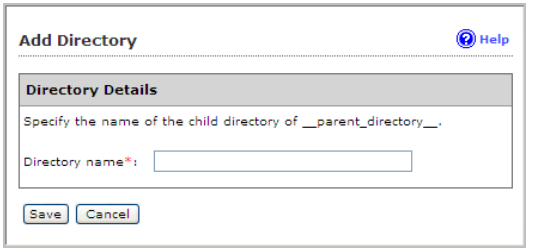
2. Click **Products** from the main menu. The Product Directory screen appears.



3. Click **Directory Management** on the Product Directory menu. The Directory Management screen appears.



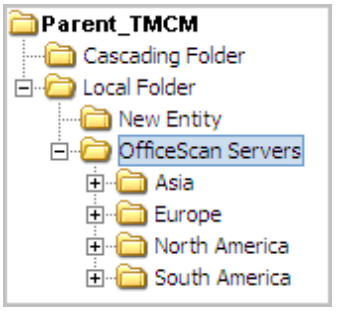
4. Select the **Local Folder**. The folder highlights.
5. Click **Add**. The Add dialog box appears.



6. Type **OfficeScan Servers** in the Directory name field.
7. Click **Save**. A confirmation dialog box appears.
8. Click **OK**. The Product Directory appears with the new folder.
9. Add the following folders under the **OfficeScan** folder:
   - **Asia**
   - **Europe**

- **North America**
- **South America**

The Product Directory should look like the following when you finish:



10. Under each of the regional folders add the following:

Asia:

- Japan
- India
- China

Europe:

- France
- Germany
- England

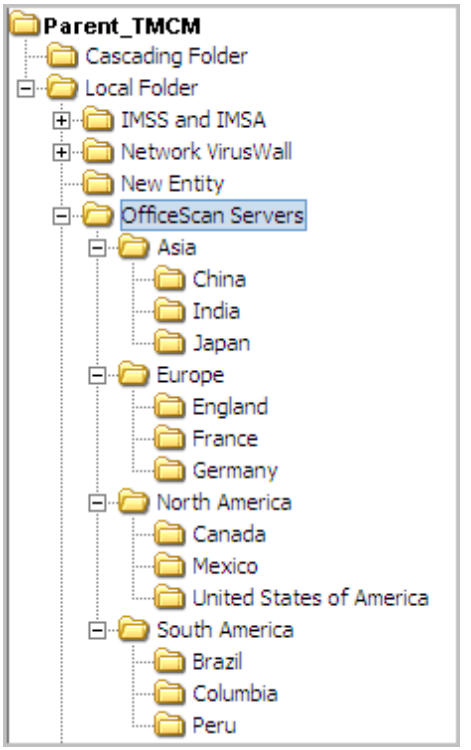
North America:

- Canada
- Mexico
- United States of America

South America

- Peru
- Brazil
- Columbia

The Product Directory should look like the following when you finish:



11. Repeat the process for the following managed products:
    - **ScanMail Servers**
    - **IMSS and IMSA**
    - **Network VirusWall**

Note: You do not need to add all the sub-directories. The structure outlined is for example purposes only.

---

12. Click **Back**. The Product Directory screen appears.

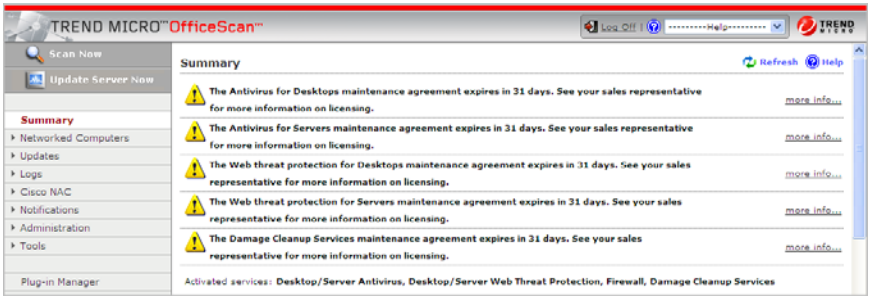
Registering Managed Products to Control Manager

After setting up the Product Directory, you can register managed products to the Control Manager server.

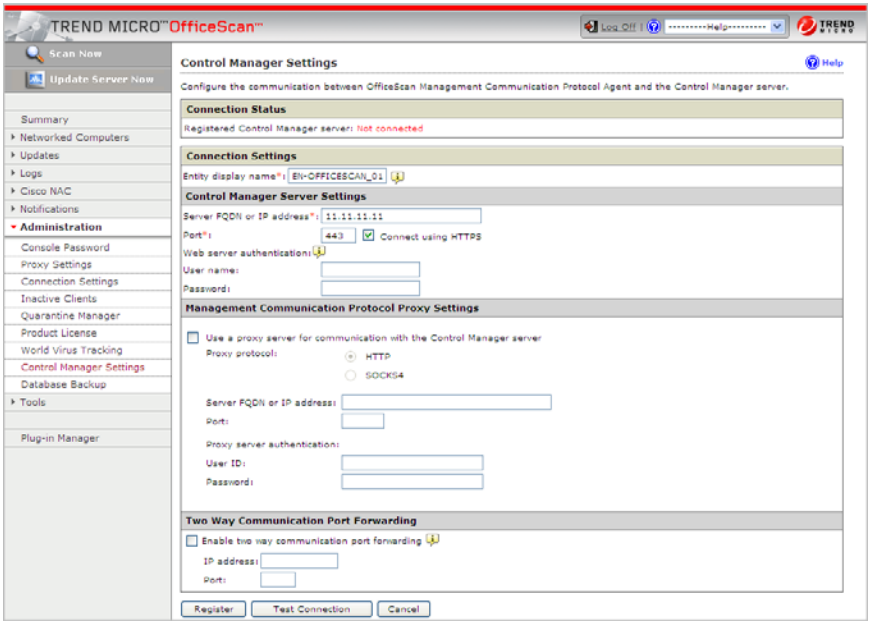
This tutorial uses an OfficeScan server as the focus for the exercises, but any Trend Micro managed product could be used as a substitute.

To register a managed product (OfficeScan) to Control Manager:

1. Log on to the managed product Web console. The Home screen for the managed product appears.



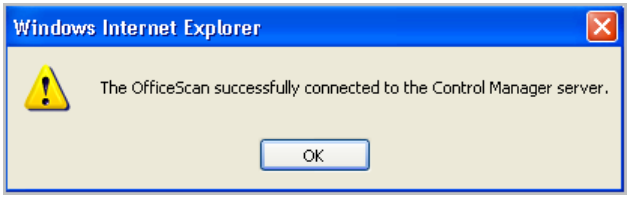
2. Click **Administration > Control Manager Settings** from the menu. The Control Manager Settings screen appears.



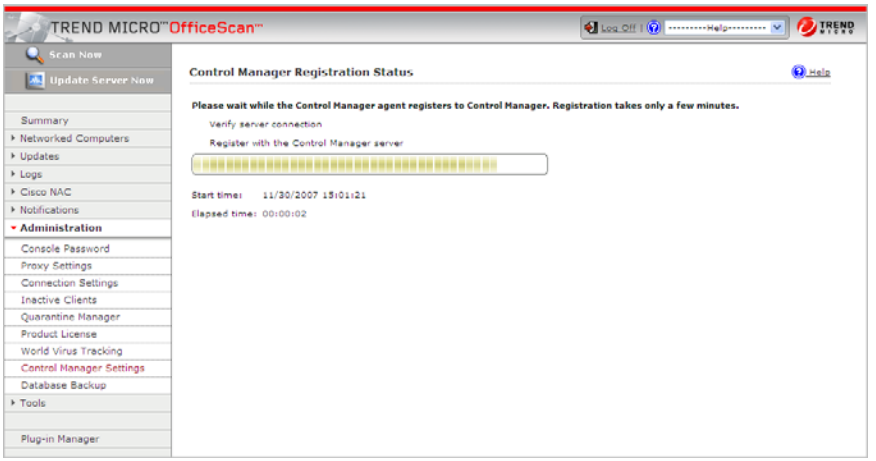
The Registered Control Manager server field displays **Not connected**.

3. Type the following in the Entity display name field: **EN-OFFICESCAN_01**.
4. Type the host name or IP address of the Control Manager server in the **Server FQDN or IP address** field**.**
5. Provide the authentication credentials for your Web server if you network requires authentication.
6. If your network uses a proxy server, provide the correct settings under **Management Communication Protocol Proxy Settings.**
7. If the OfficeScan server is behind a NAT device, provide the correct settings under **Two-Way Communication Port Forwarding**.

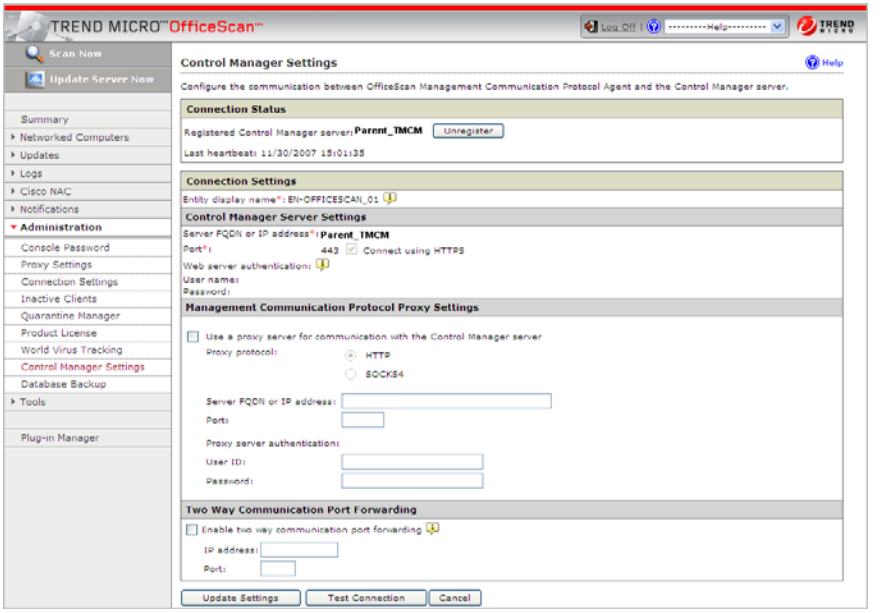
8. Click **Test Connection**. A confirmation screen appears if the managed product can connect to Control Manager.



9. Click OK.
10. Click **Register**. A progress screen appears.



After registering to Control Manager, the Control Manager Settings screen appears with the name of the Control Manager server appearing in the **Registered Control Manager server** field.



11. After registering your managed products to Control Manager, use Directory Management to move the product to the correct location in the Product Directory. In this case move the OfficeScan server under the **OfficeScan Servers > Europe > England** folder.

Configuring Control Manager User Access

After setting up the Product Directory structure, begin adding user accounts, account types, and user groups. The Control Manager User Manager from previous versions of Control Manager now consists of four sections:

TABLE 3-2. Control Manager User Account Options

SECTION	DESCRIPTION
My Account	The My Account screen contains all the account information Control Manager has for a specific user. The information on the My Account screen varies from user to user.
User Accounts	The User Accounts screen displays all Control Manager users. The screen also provides functions allowing you to create and maintain Control Manager user accounts. Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are: • Execute • Configure • Edit Directory
User Groups	The Group Accounts screen contains Control Manager groups and provides options for creating groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow Control Manager administrators to create a group, which shares the same access rights.
User Types	The Account Types screen displays all Control Manager user roles. The screen also provides functions allowing you to create and maintain Control Manager user roles. User roles define which areas of the Control Manager Web console a user can access.

Tip: Assign users with different access rights and privileges. This permits the delegation of certain management tasks without compromising security.

Understanding User Accounts

Administrators can use the functions on the User Accounts screen to assign users clearly defined areas of responsibility - by restricting their access rights to certain managed products, and limiting the actions that they can perform.

Tip: When administrators specify which products a user can access, the administrator is also specifying what information a user can access from Control Manager. This applies to component information, logs, product summary information, security information, and information available for reports and queries.

Example: Alex and Blair are OfficeScan administrators. Both have identical account type permissions (they have access to the same menu items in the Control Manager Web console). However, Alex is a global administrator and over sees operation for all OfficeScan servers. Blair on the other hand only over sees operation for OfficeScan servers protecting desktops for Europe. The information that they can view on the Web console will be very different. Blair logs on and only sees information that is applicable to the OfficeScan servers his Control Manager user account allows (the OfficeScan servers for Europe). When Alex logs on, she sees information for all OfficeScan servers worldwide because her Control Manager user account grants her access to all OfficeScan servers registered to Control Manager.

Setting Access Rights

User Access rights determine the controls available to the user in the Product Directory. For example, when you only assign a user the Execute right, then only the options associated with this right appear on the Product Directory.

You can give each user account the following access rights to a product:

TABLE 3-3. Control Manager User Account Options

SECTION	DESCRIPTION
Execute	This right permits the user to run commands on managed products in assigned folders. The following are associated with this privilege. • Start Scan Now • Deploy pattern files/cleanup templates • Enable Real-time Scan • Deploy program files • Deploy engines • Deploy license profiles
Configure	This gives the user access to the configuration consoles of the managed products in the assigned folders. Users with this right can see Configure <managed product> and similar product-specific controls (for example, OfficeScan password configuration features) on their menus.
Edit Directory	This permits the user to modify the organization of the managed products/directories the user can access.

Note: The options that actually appear also depend on the product's profile. For example, if a product does not have a scanning function, such as eManager, then the Scan Now control does not appear in the Product Directory Tasks menu.

This tutorial uses the following process to configure user accounts:

1. Specify which products/directories the user can access.
2. Specify which menu items the user can access through the user's account type.
3. Specify the account type for the user's account.

Note: Active Directory users cannot have their accounts disabled from Control Manager. To disable an Active Directory user you must disable the account from the Active Directory server.

Table 3-4, "Managed Product Servers and Users," on page 3-14 provides an example for information about managed products and assigned users.

TABLE 3-4. Managed Product Servers and Users

MANAGED PRODUCT	USERS			
	GLOBAL	REGIONAL	LOCAL	LIMITED
OfficeScan 8.0	Alex	Blair	Chris	Dana
Control Manager	Erin			

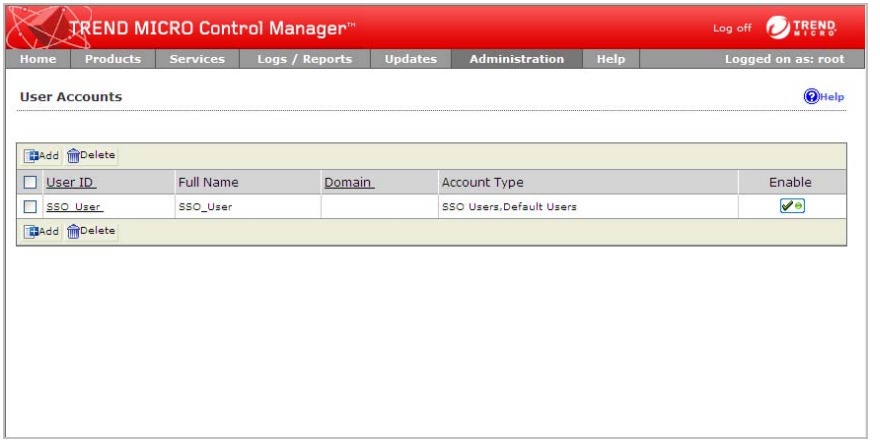
Adding a User Account for Alex (Global Administrator)

Alex is the global OfficeScan administrator for ACME CO. She needs the ability to configure and issue tasks to any OfficeScan server registered to Control Manager. Alex also needs to have the ability to modify the Product Directory as new offices open for ACME CO. around the world.

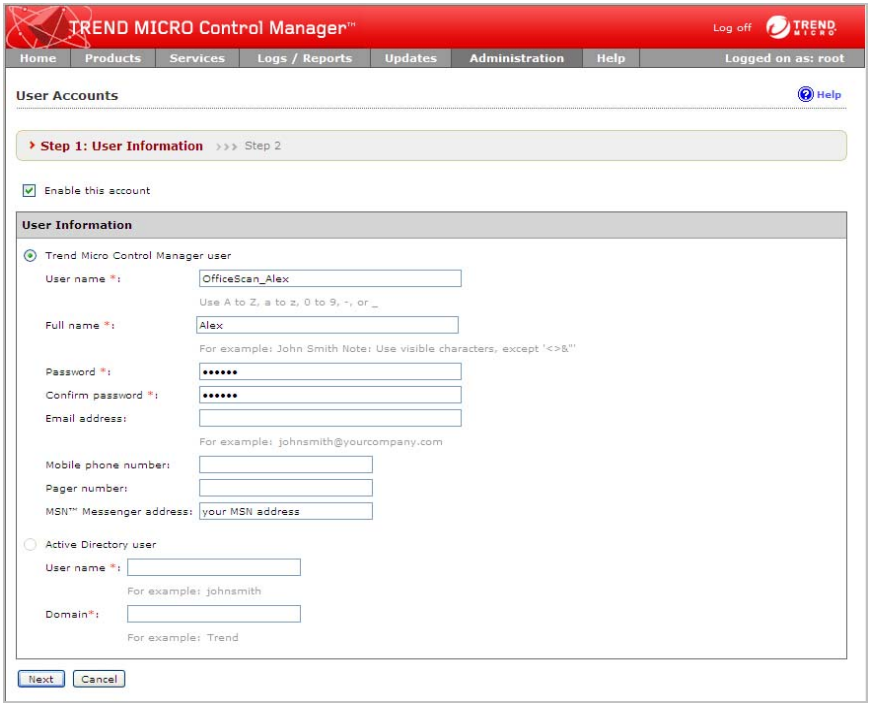
To add a user account for Alex:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.

3. Click **User Accounts** from the sub-menu. The User Accounts screen appears.

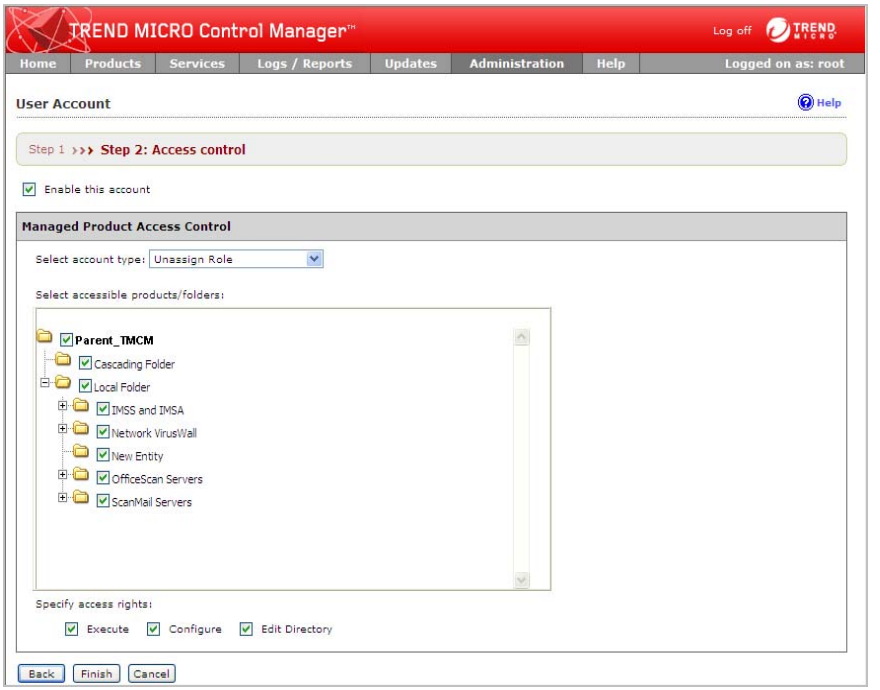


4. In the working area, click **Add**. The Add User Account Step 1: User Information screen appears.



5. Select **Enable this account** to enable the user.
6. Select **Trend Micro Control Manager user**.
7. Provide the following information for the account:
   a. **User name:** OfficeScan_Alex
   b. **Full name:** Alex
   c. **Password** and **Confirm password:** Provide a password of your choosing
   d. **Email address:** Provide your own email address
   e. **MSN Messenger address:** Provide your own MSN address if you have one.

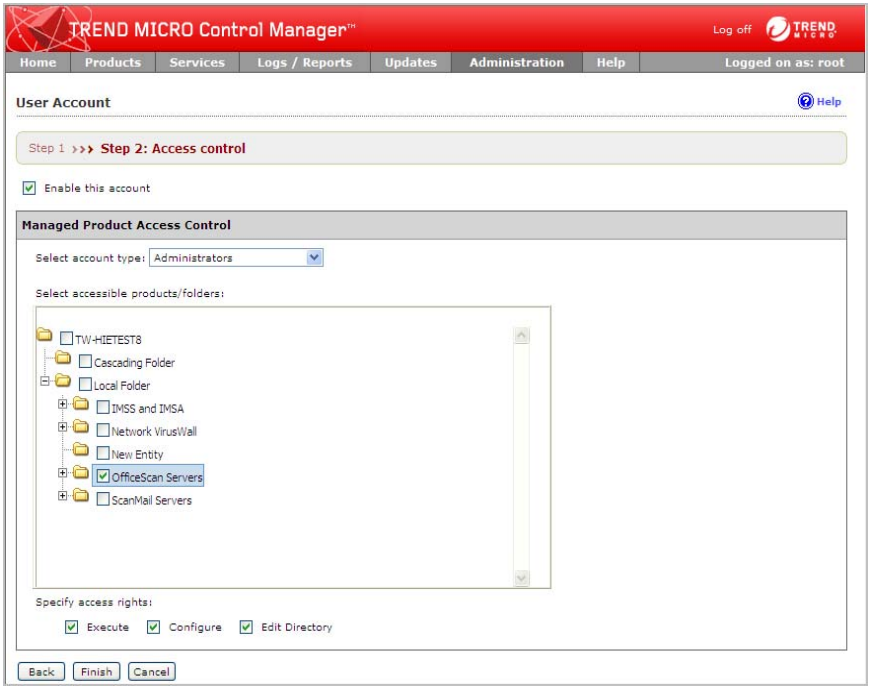
8. Click **Next**. The Add User Account Step 2: Access Control screen appears.



9. Select **Administrator** from the Account Type list.
10. Clear all the check boxes except **OfficeScan Servers** from **Select accessible products/folders**.

    This means that Alex only has access to the **OfficeScan Servers** directory, any managed products which fall under the directory, and any of **OfficeScan Servers'**

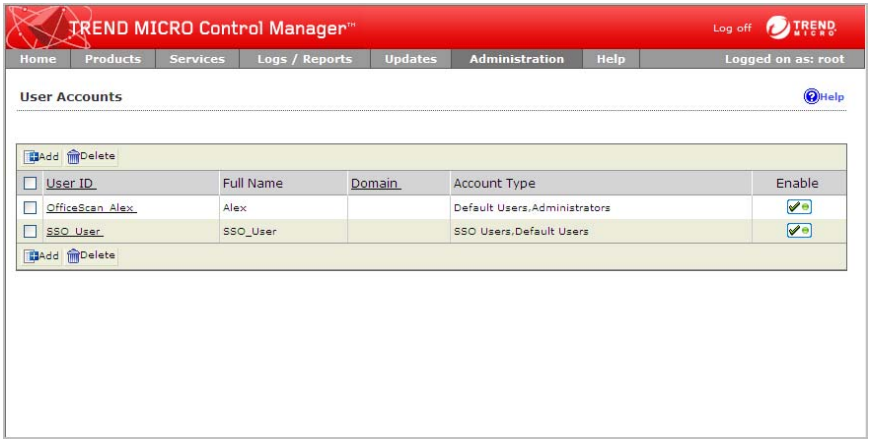
sub-directories. Alex also has access to all the information that the managed products provide (component information, log information, reports, and so on).



11. All options under **Specify access rights** are selected by default.

This means Alex has complete control over the directory **OfficeScan Servers**, any managed products which fall under the directory, and any **OfficeScan Servers'** sub-directories.

12. Click **Finish**. The User Accounts screen appears.

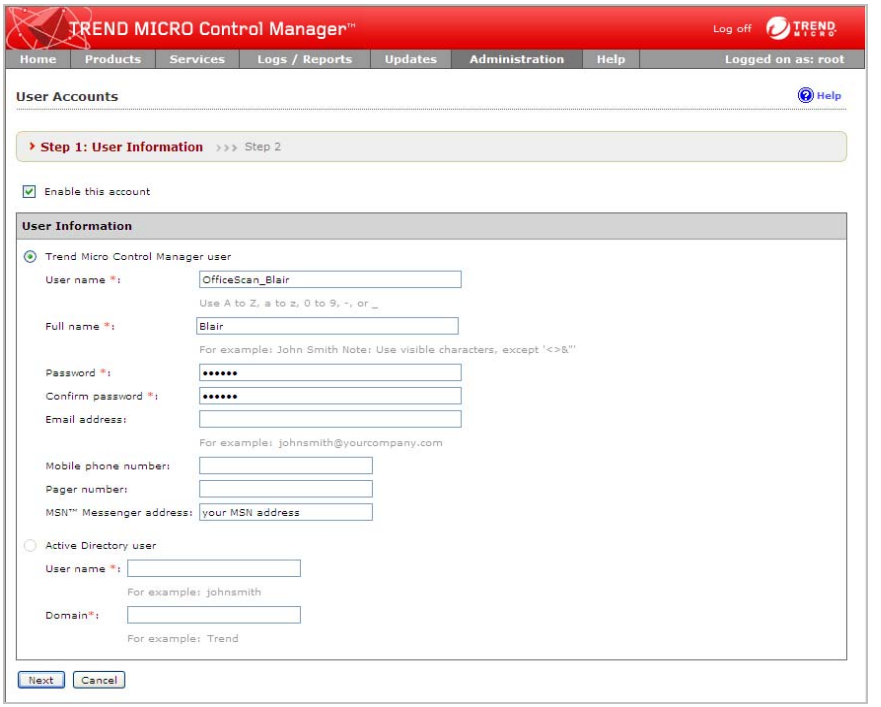


Adding a User Account for Blair (Regional Administrator)

Blair is a regional OfficeScan administrator for ACME CO. He needs the ability to configure and issue tasks to OfficeScan servers in his region that are registered to Control Manager. Blair does not need the ability to modify the Product Directory, because Alex, as the global OfficeScan administrator, handles that task.

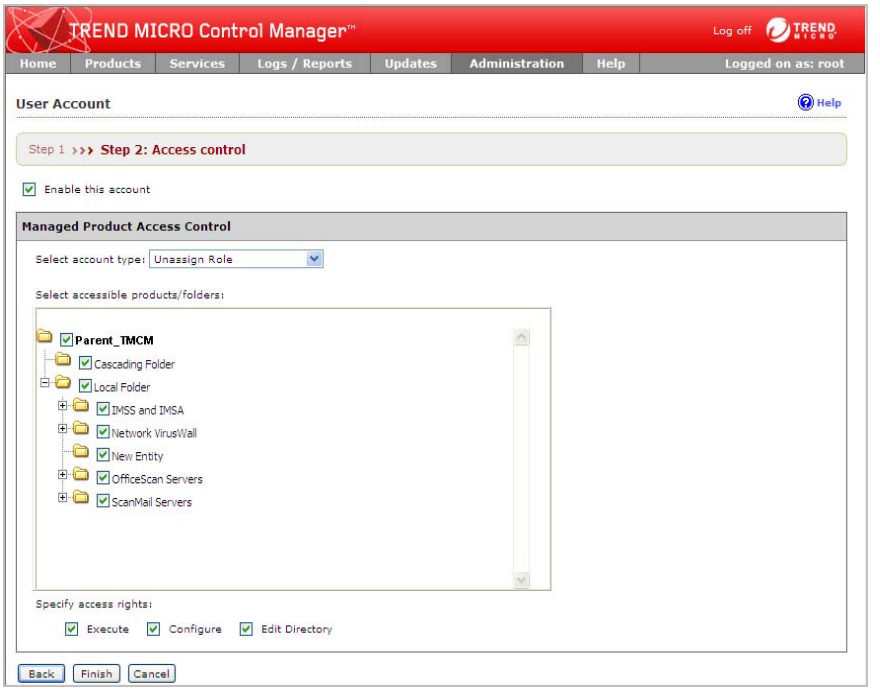
To add a user account for Blair:

1. In the working area, click **Add**. The Add User Account Step 1: User Information screen appears.



2. Select **Enable this account** to enable the user.
3. Select **Trend Micro Control Manager user**.
4. Provide the following information for the account:
   a. **User name:** OfficeScan_Blair
   b. **Full name:** Blair
   c. **Password and Confirm password:** Provide a password of your choosing
   d. **Email address:** Provide your own email address
   e. **MSN Messenger address:** Provide your own MSN address if you have one.

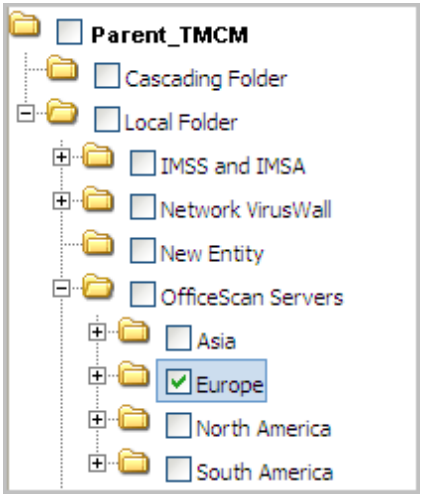
5. Click **Next**. The Add User Account Step 2: Access Control screen appears.



6. Select **Administrator** from the Account Type list.
7. Expand the **OfficeScan Servers** directory.
8. Clear all the check boxes except Europe from **Select accessible products/folders**.

   This means that Blair only has access to the **Europe** directory under the **OfficeScan Server** directory, any managed products which fall under the directory, and any of **Europe's** sub-directories. Blair also has access to the information that

those managed products provide (component information, log information, reports, and so on).



9. Clear the **Edit Directory** option under **Specify access rights**.

   This means Blair can configure and execute tasks on the OfficeScan servers under the **Europe** directory, but he cannot edit the Product Directory structure.

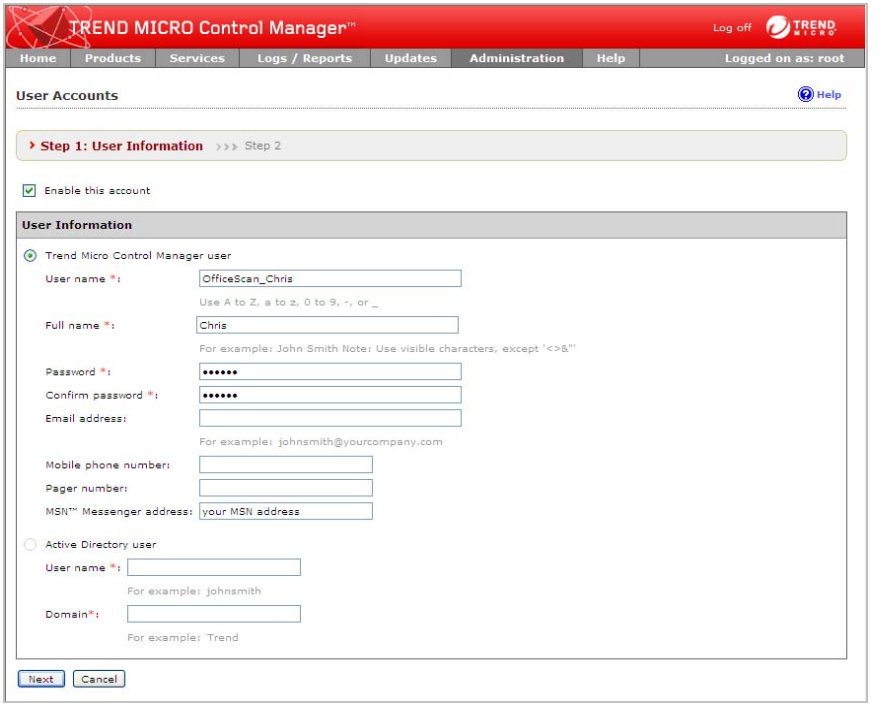
10. Click **Finish**. The User Accounts screen appears.

Adding a User Account for Chris (Local Administrator)

Chris is a local OfficeScan administrator for ACME CO. He needs the ability to configure and issue tasks to OfficeScan servers in his region that are registered to Control Manager. Chris does not need the ability to modify the Product Directory, because Alex, as the global OfficeScan administrator, handles that task.

To add a user account for Chris:

1. In the working area, click **Add**. The Add User Account Step 1: User Information screen appears.



2. Select **Enable this account** to enable the user.
3. Select **Trend Micro Control Manager user**.
4. Provide the following information for the account:

a. **User name:** OfficeScan_Chris

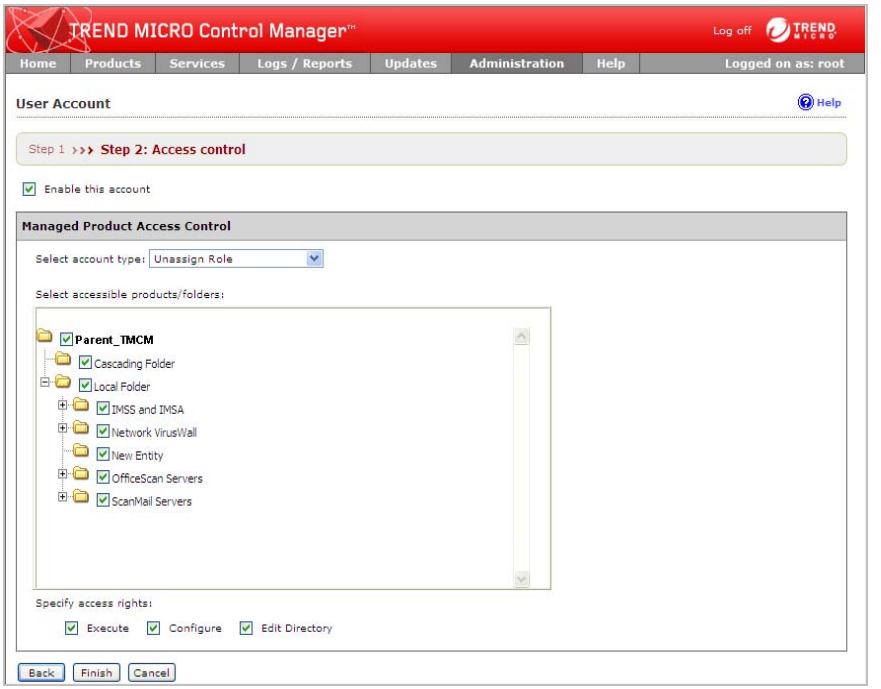
b. **Full name:** Chris

c. **Password and Confirm password:** Provide a password of your choosing

d. **Email address:** Provide your own email address

e. **MSN Messenger address:** Provide your own MSN address if you have one.

5. Click **Next**. The Add User Account Step 2: Access Control screen appears.

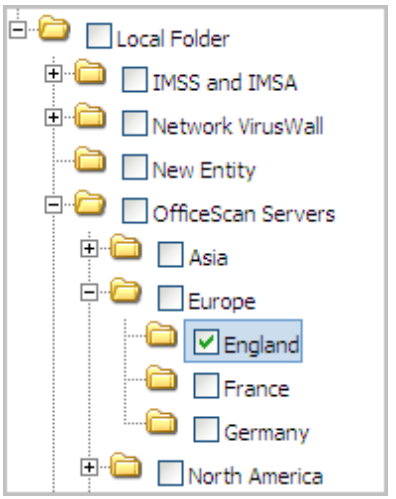


6. Select **Administrator** from the Account Type list.

7. Expand the **OfficeScan Servers > Europe** directory.

8. Clear all the check boxes except **England** from **Select accessible products/folders**.

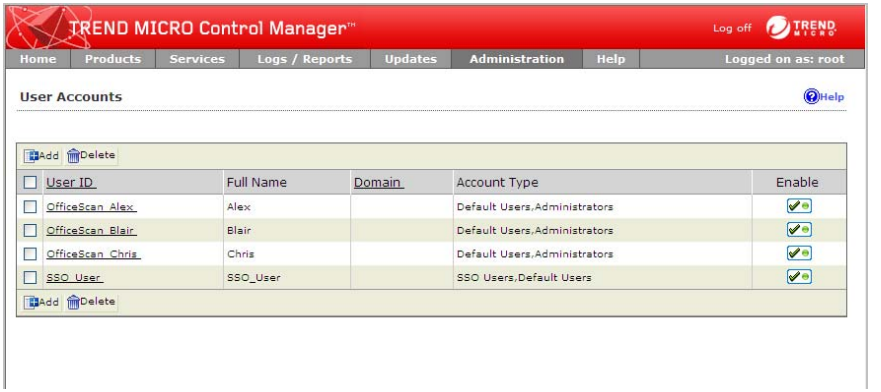
This means that Chris only has access to the **England** directory under the **OfficeScan Server** directory, any managed products which fall under the directory, and any of **England's** sub-directories. Chris also has access to the information that those managed products provide (component information, log information, reports, and so on).



9. Clear the **Edit Directory** option under **Specify access rights**.

   This means Chris can configure and execute tasks on the OfficeScan servers under the **England** directory, but he cannot edit the Product Directory structure.

10. Click **Finish**. The User Accounts screen appears.



Adding a User Account for Dana (Manager)

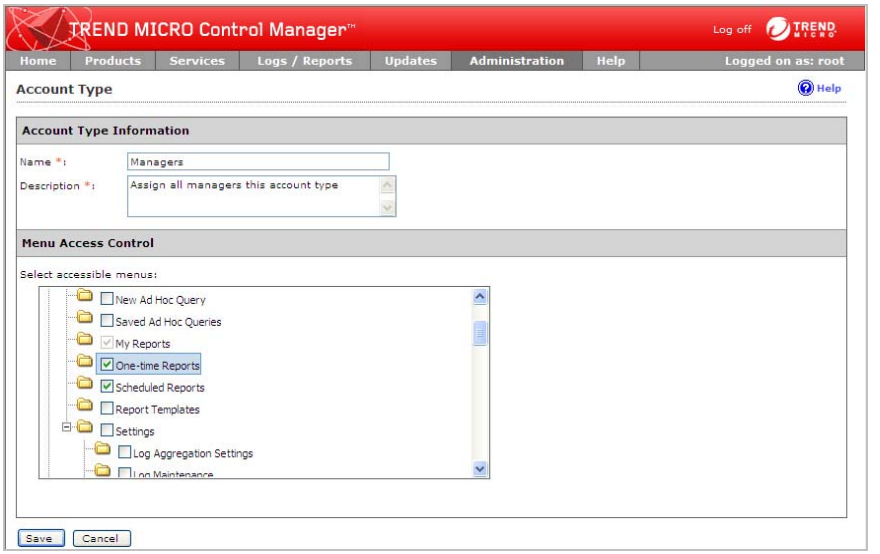
Dana is not an OfficeScan administrator. She has a management-oriented job. As a result, Dana does not need the same level of access to the Control Manager Web console that Alex, Blair, and Chris require. While the default account types are sufficient for Alex, Blair, and Chris, Dana needs a customized account type. Dana only really needs access to the reports Chris generates. That means she does not need access to the entire Control Manager Web console. Her access to the Web console can be scaled according to her needs. Knowing that Dana needs a custom account type means that before creating her user account, first the account type should be created.

Adding a custom account type for Dana:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.

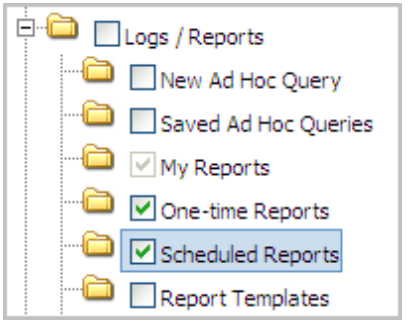
3. Click **Account Types** from the sub-menu. The Account Types screen appears.

4. Click **Add**. The Add Account Type screen appears.



5. Provide the following information for the account type:
   - **Name:** Managers
   - **Description:** Assign all managers this account type
6. Select only the following from the **Select available menus** list:
   - **One-time Reports**
   - **Scheduled Reports**

   Selecting only these menu items allows users assigned this account type to view and generate one-time and scheduled reports for managed products or directories assigned to their user account.



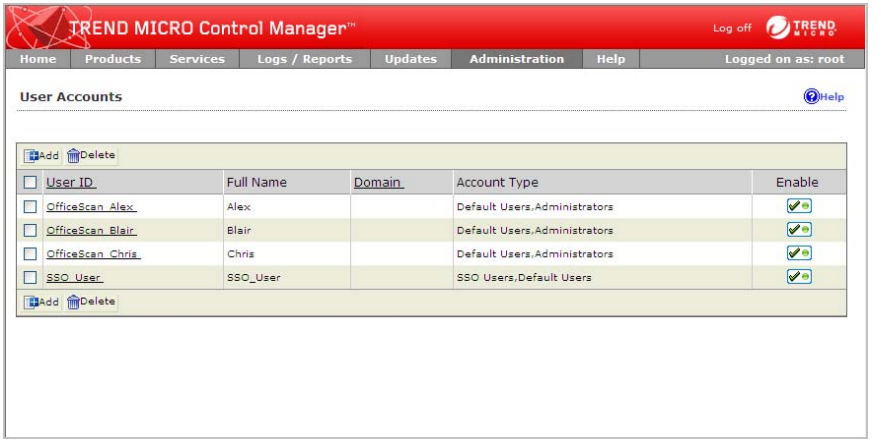
7. Click **Save**. The Account Type screen appears.

Now that the Account Type for Dana (and other managers) is ready, configure her user account.

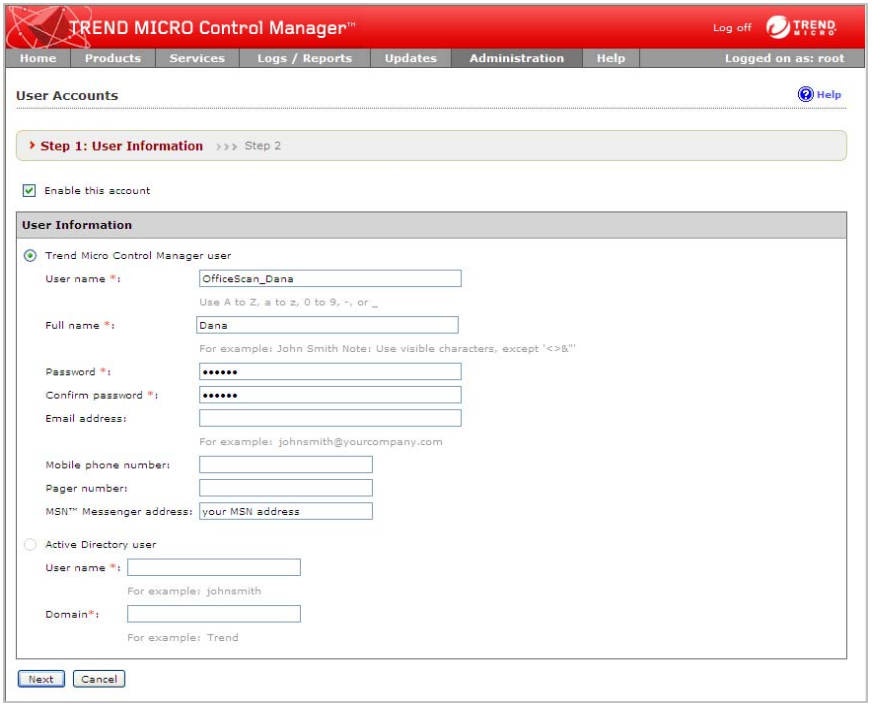
To add a user account for Dana:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.

3. Click **User Accounts** from the sub-menu. The User Accounts screen appears.

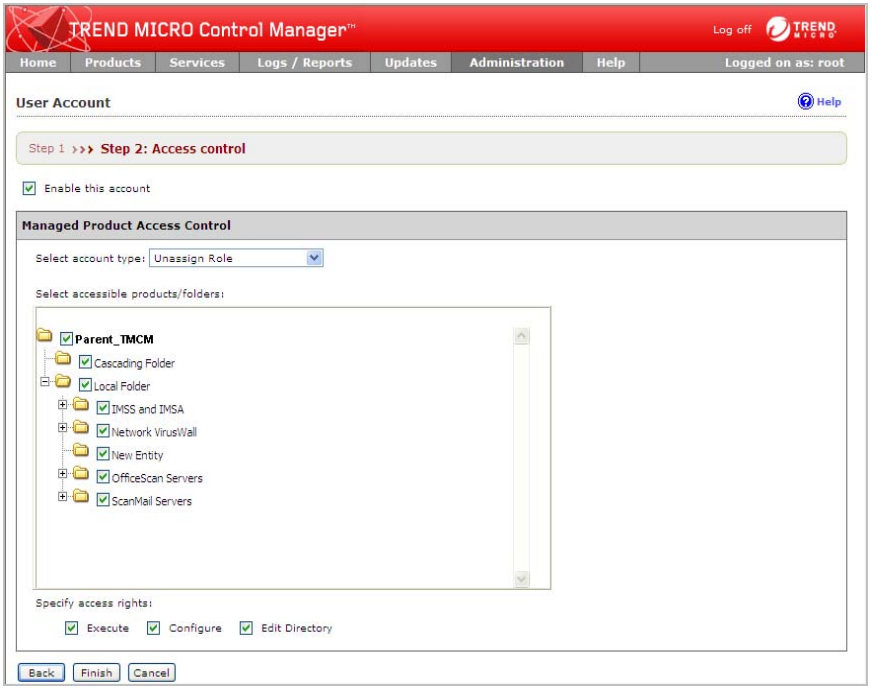


4. In the working area, click **Add**. The Add User Account Step 1: User Information screen appears.



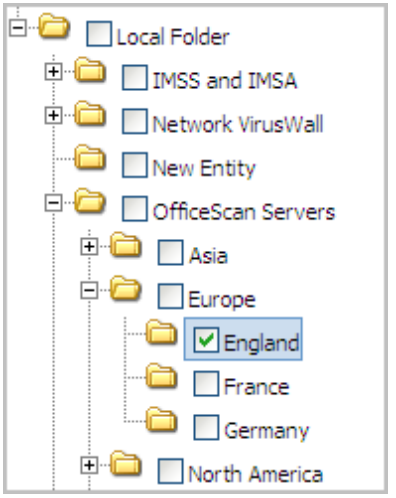
5. Select **Enable this account** to enable the user.
6. Select **Trend Micro Control Manager user**.
7. Provide the following information for the account:
   a. **User name:** OfficeScan_Dana
   b. **Full name:** Dana
   c. **Password and Confirm password:** Provide a password of your choosing
   d. **Email address:** Provide your own email address
   e. **MSN Messenger address:** Provide your own MSN address if you have one.

8. Click **Next**. The Add User Account Step 2: Access Control screen appears.



9. Select **Managers** from the Account Type list.
10. Expand the **OfficeScan Servers > Europe** directory.
11. Clear all the check boxes except **England** from **Select accessible products/folders**.

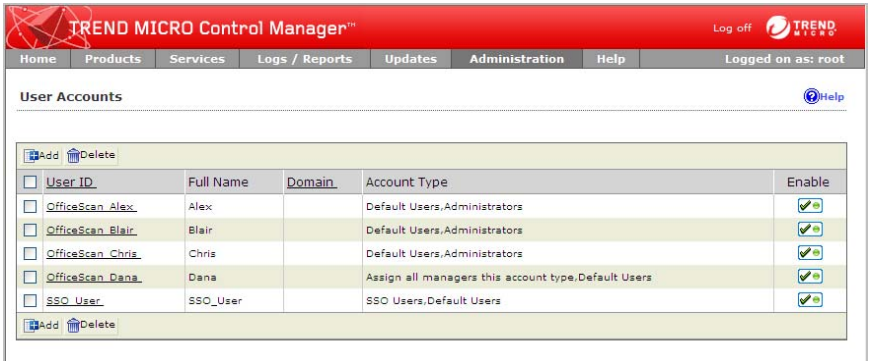
This means that Dana only has access to OfficeScan servers under the **England** directory.



12. Clear all the options under **Specify access rights**.

    This means Dana only has access to information from the OfficeScan servers under the **England** directory. She cannot configure any servers, execute any tasks to the servers, or modify the Product Directory structure.

13. Click **Finish**. The User Accounts screen appears.



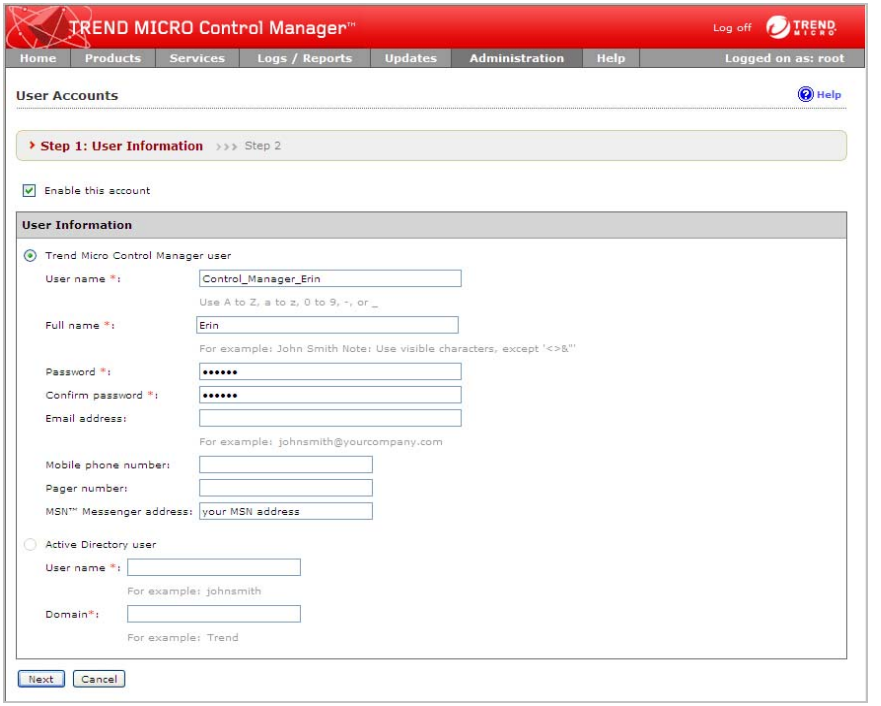
Adding a User Account for Erin (Control Manager Administrator)

You can add all of the user accounts from Table 3-4, "Managed Product Servers and Users," on page 3-14. However, to see the largest difference in user accounts you really only need to add one more account type; that of an administrator who can view all the managed products registered to a Control Manager server.

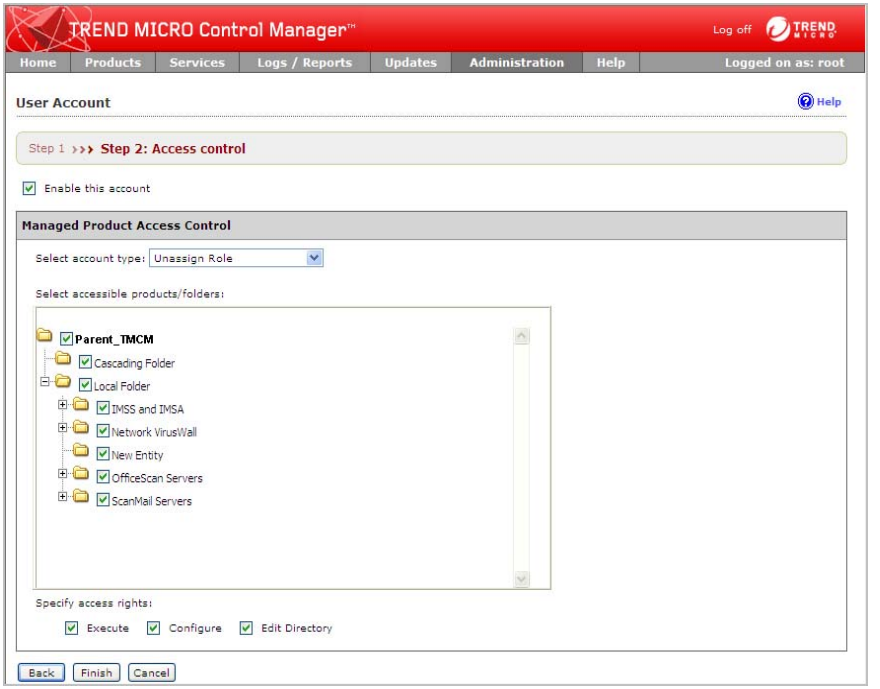
Erin will have complete access to all managed products and the complete Control Manager Web console. She will be able to configure and execute tasks on any managed product registered to Control Manager, and she will also be able to modify the Product Directory as she sees fit.

To add a user account for Erin:

1. In the working area, click **Add**. The Add User Account Step 1: User Information screen appears.

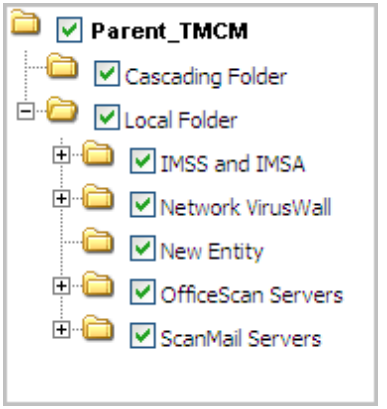


2. Select **Enable this account** to enable the user.
3. Select **Trend Micro Control Manager user**.
4. Provide the following information for the account:
   a. **User name:** Control_Manager_Erin
   b. **Full name:** Erin
   c. **Password and Confirm password:** Provide a password of your choosing
   d. **Email address:** Provide your own email address
   e. **MSN Messenger address:** Provide your own MSN address if you have one.
5. Click **Next**. The Add User Account Step 2: Access Control screen appears.



6. Select **Administrator** from the Account Type list.
7. All the check boxes in **Select accessible products/folders** are selected by default.

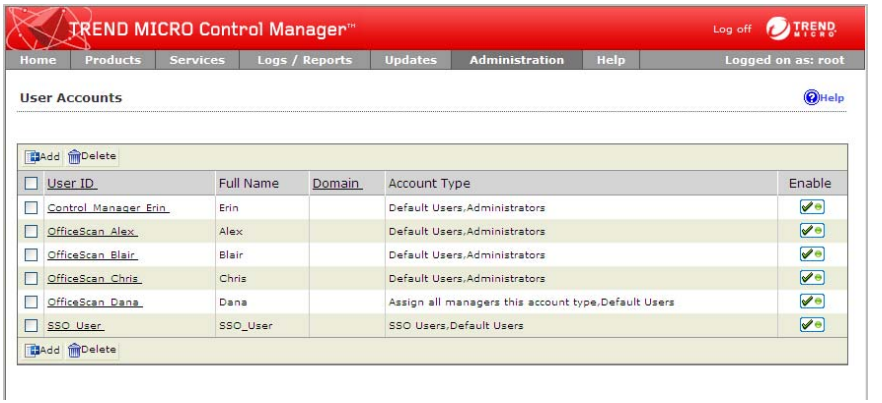
This means that Erin has access to all managed products registered to Control Manager.



8. All options under **Specify access rights** are selected by default.

   This means Erin has complete control over all managed products registered to Control Manager. She can configure and issue tasks to any managed product registered to Control Manager, and modify the Product Directory structure as she sees fit.

9. Click **Finish**. The User Accounts screen appears.



What Each User Views and Can Perform

After adding the user accounts, it is useful to know what each user will actually have permission to view or perform on the Control Manager Web console.

TABLE 3-5. User Access

USER	DESCRIPTION
Alex	Alex has complete access to the Control Manager Web console. She also has permission to view, configure, and issue tasks to all managed products (OfficeScan servers and clients) under the **OfficeScan Servers** directory. Which means she has permission to access all the OfficeScan servers and clients registered to the Control Manager server.
Blair	Blair has almost complete access to the Control Manager Web console. Blair cannot access the Directory Management screen to modify the Product Directory structure. He has permission to view, configure, and issue tasks to managed products (OfficeScan servers and clients) under the **Europe** directory of the **OfficeScan Servers** directory.
Chris	Chris has almost complete access to the Control Manager Web console. Chris cannot access the Directory Management screen to modify the Product Directory structure. He has permission to view, configure, and issue tasks to managed products (OfficeScan servers and clients) under the **England** directory of the **OfficeScan Servers > Europe** directory.
Dana	Dana has very limited access to the Control Manager Web console. She can only access the One-time Reports and Scheduled Reports screens (along with the other default areas all users can access). She only has permission to access information from managed products (OfficeScan servers and clients) under the **England** directory of the **OfficeScan Servers > Europe** directory.
Erin	Erin has complete access to the Control Manager Web console. She also has permission to view, configure, and issue tasks to all managed products registered to Control Manager.

The Main Menu

After logging on Alex, Blair, Chris, and Erin see the full main menu for the Control Manager Web console. This is because the users have access to every feature due to their account type (**Administrators**).

Note: Even if a user does not access to every feature on the Control Manager Web console it is still possible to see the complete main menu. This is because even though the user does not have access to every feature, the features the user does have access to involve all the main menu items.

After logging on Dana does not see the complete main menu. Dana's access to the Web console is restricted by her account type (**Managers**).

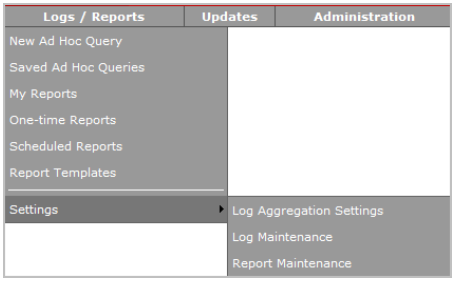
FIGURE 3-1. Main Menu

Drop-Down Menus

When accessing any of the menu items Alex, Blair, Chris, and Erin see all items, a drop-down list from the main menu contains. This is because they have access to every feature due to their account type (**Administrators**).

Dana has limited access to the features the Control Manager Web console provides. Dana's access to the Web console is restricted by her account type (**Managers**).

FIGURE 3-2. Drop-down menu for Logs/Reports

LOGS/REPORTS DROP-DOWN MENU FOR ALEX, BLAIR, CHRIS, AND ERIN	LOGS/REPORTS DROP-DOWN MENU FOR DANA
	

Product Directory and Product Directory Structure

When accessing the Product Directory or Product Directory Structure each user sees a different structure. This is due to eh user's account privileges (not their account type).

TABLE 3-6. Product Directory

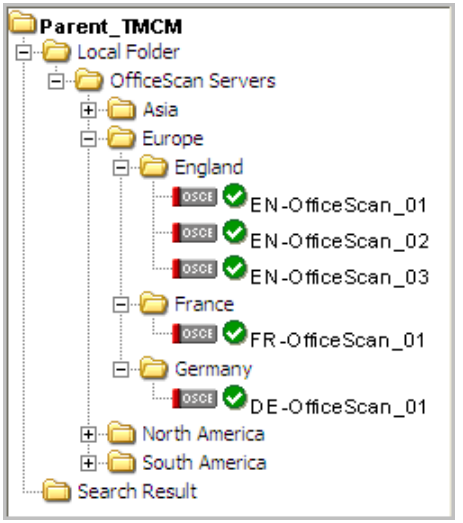
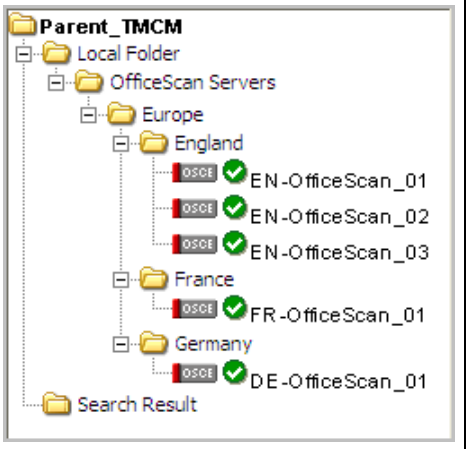
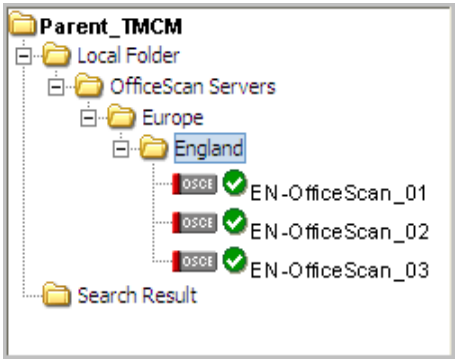
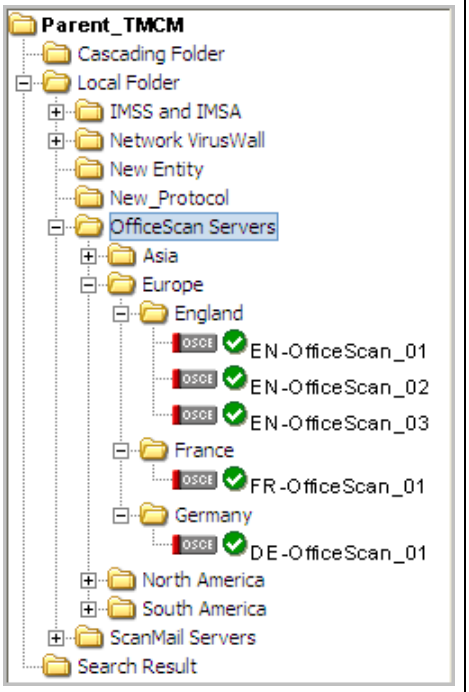
ALEX	BLAIR
 Alex has access to all managed products under the OfficeScan Servers directory. This means she has access to all OfficeScan servers across the globe. Alex will see this structure on the following screens: • **Entity Tree and Directory Management screens:** The true Product Directory appears on these screens • **Query Managed Product Logs screen:** A Product Directory structure appears on this screen • **Logs/Reports screens:** A Product Directory structure appears on these screens • **Add/Edit Deployment Plan:** A Product Directory structure appears on these screens • **User Accounts screen:** A Product Directory structure appears on these screens • **License Management screens:** A Product Directory structure appears on these screens	 Blair has access to all managed products under the Europe directory of the OfficeScan Servers directory. This means he has access to all OfficeScan servers in Europe. Blair will see this structure on the following screens: • **Entity Tree and Directory Management screens:** The true Product Directory appears on these screens • **Query Managed Product Logs screen:** A Product Directory structure appears on this screen • **Logs/Reports screens:** A Product Directory structure appears on these screens • **Add/Edit Deployment Plan:** A Product Directory structure appears on these screens • **User Accounts screen:** A Product Directory structure appears on these screens • **License Management screens:** A Product Directory structure appears on these screens

TABLE 3-6. Product Directory

CHRIS AND DANA	ERIN
 Chris has access to all managed products under the England directory of the OfficeScan Servers > Europe directory. This means he has access to all OfficeScan servers in England. Chris will see this structure on the following screens: • **Entity Tree and Directory Management screens:** The true Product Directory appears on these screens • **Query Managed Product Logs screen:** A Product Directory structure appears on this screen • **Logs/Reports screens:** A Product Directory structure appears on these screens • **Add/Edit Deployment Plan:** A Product Directory structure appears on these screens • **User Accounts screen:** A Product Directory structure appears on these screens • **License Management screens:** A Product Directory structure appears on these screens Dana does not have access to the Product Directory directly. She will see the Product Directory structure on the Logs/Reports screens.	 Erin can view the entire Product Directory or Product Directory structure on any of the applicable screens.

Home and Summary Screens

All users can access the Home screen for an at-a-glance summary of the product network Control Manager manages. Only users with access to the Product Directory can view the Summary screen. A user's account type specifies whether they can access the Product Directory.

The Home and Summary screens contain the following sections:

TABLE 3-7. Control Manager Home Screen and Product Directory Status View Information

SECTION	DESCRIPTION
Antivirus Summary	Displays summary information for all registered managed products with antivirus protection/detection capabilities. For example, OfficeScan, InterScan Messaging Security, or Total Discovery.
Spyware/Grayware Summary	Displays summary information for all registered managed products with spyware/grayware protection/detection capabilities. For example, OfficeScan, InterScan Messaging Security, or Total Discovery.
Content Security Summary	Displays summary information for all registered managed products with content protection/detection capabilities. For example, InterScan Messaging Security, or Total Discovery.
Web Security Summary	Displays summary information for all registered managed products with Web protection/detection capabilities. For example, OfficeScan, InterScan Web Security, or Total Discovery.
Network Virus Summary	Displays summary information for all registered managed products with network virus protection/detection capabilities. For example, Network VirusWall Enforcer, or Total Discovery.
Violation Status	Displays summary information for all clients that violate administrator created policies of Network VirusWall Enforcer.
Component Status	Displays component summary information for all registered managed products. Only component information for products registered to the Control Manager server display. For example, the Control Manager server has only OfficeScan servers, so only OfficeScan components display.

TABLE 3-8. Product Directory Managed Product Status View Information

SECTION	DESCRIPTION
System Information	Displays the managed product information (managed product name, version, language version, and agent version) and component summary information for the selected managed product.
Product License Information	Displays managed product license information for OfficeScan: • Managed service name • License status • The type of license (full or evaluation) • Activation Code • Number of Activation Codes • Expiration date of the product license • The number of seats the license covers

Tip: Clicking the underlined numbers that display in the right-hand column of each table opens a detailed summary screen with information for the row.

Example: In the Antivirus Summary table, clicking the corresponding number for the row **Cleaned** opens a Detailed Information screen. The Detailed Information screen displays information about all the computers that have been cleaned.

The information a user can view depends on the access privileges granted to their user account. The information in the Component Status area, the Antivirus Summary, Spyware/Grayware Summary, and Web Security Summary areas will differ for each of the users (Alex, Blair, Chris, Dana, and Erin) because of the access privileges specified in their user account.

TABLE 3-9. Home and Summary Screens

ALEX

Alex can see information for all OfficeScan servers registered to Control Manager on the Product Directory, on the Home screen, and on the Summary screen.

Violation Status

Violation	Last Updated	Total
Service Violations	n/a	0

Component Status

Component	Latest Version		Outdated	Current	Total
Virus Pattern File	3.203.00		0	32	32
Damage Cleanup Template	704		0	32	32
Common Firewall Pattern	10265		1	31	32
Spyware Active-monitoring Pattern	n/a		0	32	32
IntelliTrap Pattern	n/a		0	32	32
IntelliTrap Exception Pattern	n/a		0	32	32
Spyware pattern	n/a		0	32	32
Anti-rootkit Driver (32-bit)	n/a		0	32	32
Virus Cleanup Engine (Digitally signed, 32-bit)	5.300.1103		0	32	32
Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)	5.300.1103		0	32	32
Spyware Scan Engine (32-bit)	n/a		0	32	32
Spyware Scan Engine (64-bit)	n/a		0	32	32
Virus Scan Engine	NTKD	8.550.1001	0	32	32
	Scan Engine for Windows XP/Server 2003 on x64 architecture	8.550.1001	0	32	32

BLAIR

Blair can see information for OfficeScan servers registered to Control Manager under the Europe folder in the Product Directory, on the Home screen, and on the Summary screen.

Violation Status

Violation	Last Updated	Total
Service Violations	n/a	0

Component Status

Component	Latest Version		Outdated	Current	Total
Virus Pattern File	3.203.00		0	5	5
Damage Cleanup Template	704		0	5	5
Common Firewall Pattern	10265		1	4	5
Spyware Active-monitoring Pattern	n/a		0	5	5
IntelliTrap Pattern	n/a		0	5	5
IntelliTrap Exception Pattern	n/a		0	5	5
Spyware pattern	n/a		0	5	5
Anti-rootkit Driver (32-bit)	n/a		0	5	5
Virus Cleanup Engine (Digitally signed, 32-bit)	5.300.1103		0	5	5
Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)	5.300.1103		0	5	5
Spyware Scan Engine (32-bit)	n/a		0	5	5
Spyware Scan Engine (64-bit)	n/a		0	5	5
Virus Scan Engine	NTKD	8.550.1001	0	5	5
	Scan Engine for Windows XP/Server 2003 on x64 architecture	8.550.1001	0	5	5

TABLE 3-9. Home and Summary Screens

CHRIS AND DANA

Chris can see information for OfficeScan servers registered to Control Manager under the England folder in the Product Directory, on the Home screen, and the Summary screen. Dana does not have access to the Product Directory, so she will not see the information on the Summary screen.

Violation Status

Violation	Last Updated	Total
Service Violations	n/a	0

Component Status

Component	Latest Version		Outdated	Current	Total
Virus Pattern File	3.203.00		0	3	3
Damage Cleanup Template	704		0	3	3
Common Firewall Pattern	10265		1	2	3
Spyware Active-monitoring Pattern	n/a		0	3	3
IntelliTrap Pattern	n/a		0	3	3
IntelliTrap Exception Pattern	n/a		0	3	3
Spyware pattern	n/a		0	3	3
Anti-rootkit Driver (32-bit)	n/a		0	3	3
Virus Cleanup Engine (Digitally signed, 32-bit)	5.300.1103		0	3	3
Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)	5.300.1103		0	3	3
Spyware Scan Engine (32-bit)	n/a		0	3	3
Spyware Scan Engine (64-bit)	n/a		0	3	3
Virus Scan Engine	NTKD	8.550.1001	0	3	3
	Scan Engine for Windows XP/Server 2003 on x64 architecture	8.550.1001	0	3	3

TABLE 3-9. Home and Summary Screens

ERIN

Erin can see information for all managed products registered to Control Manager on the Product Directory, on the Home screen, and on the Summary screen.

Violation Status

Violation	Last Updated	Total
Service Violations	11/14/2007 6:31:03 PM	108

Component Status

Component	Latest Version		Outdated	Current	Total
Virus Pattern File	3.203.00		4	48	52
Damage Cleanup Template	704		0	12	12
Damage Cleanup Engine	3.980.1012		0	12	12
Spyware/Grayware Scan pattern file	0.335.00		2	44	46
Spyware/Grayware Cleanup pattern file	218		0	10	10
Common Firewall Pattern	10234		0	11	11
Common Firewall Driver (NTKD)	n/a		0	11	11
Phish pattern for InterScan Web Security product line (IWSS/IWSA/ISVW)	232		0	1	1
Anti-spam Pattern	15504		2	0	2
Anti-spam Engine (Windows)	3.000.1153		0	3	3
URL Filtering Database (Full)	n/a		0	1	1
URL Filtering Database (Delta)	n/a		0	1	1
URL Filtering Engine (Linux)	n/a		0	1	1
Spyware Active-monitoring Pattern	n/a		0	3	3
IntelliTrap Pattern	n/a		0	4	4
IntelliTrap Exception Pattern	n/a		0	4	4
Spyware pattern	n/a		0	2	2
Anti-rootkit Driver (32-bit)	n/a		0	2	2
Virus Cleanup Engine (Digitally signed, 32-bit)	n/a		0	1	1
Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)	n/a		0	1	1
Spyware Scan Engine (32-bit)	n/a		0	2	2
Spyware Scan Engine (64-bit)	n/a		0	1	1
Anti-spam Pattern (Master)	15504		1	0	1
Anti-spam Pattern (Incremental)	1.55040.00		1	0	1
Virus Scan Engine	VxD	8.000.1001	0	10	10
	32-bit DLL(NT/2000)	8.000.1001	2	25	27
	NTKD	8.000.1001	0	12	12
	IA 64-bit Scan Engine	8.000.1008	0	11	11
	NLM	7.510.1002	0	1	1
	Solaris/SPARC	8.100.1002	0	3	3
	Linux/x86	8.100.1002	2	7	9
	Scan Engine for Windows XP/Server 2003 on x64 architecture	8.000.1003	0	9	9

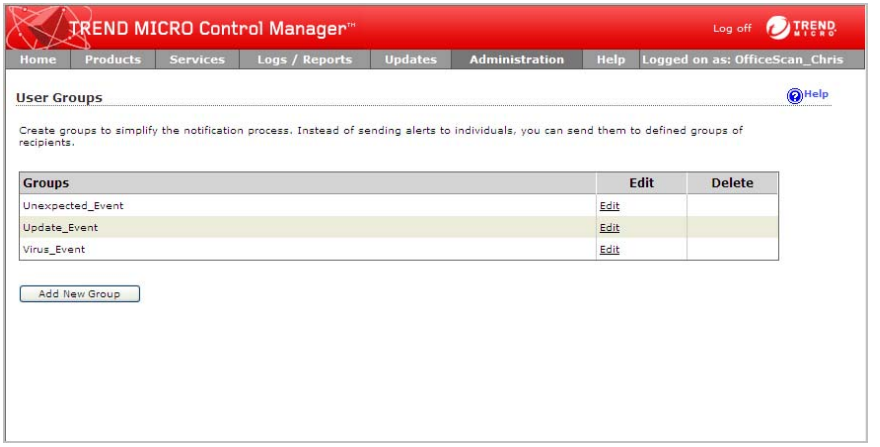
Configuring User Groups

Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. You can add users to groups according to similar properties including user types, location, or the type of notifications they should receive. Even if a user does not have a Control Manager user account, you can still add them to a group by typing their email address. However, they only receive notifications if the group has been added to the recipient list for specific events.

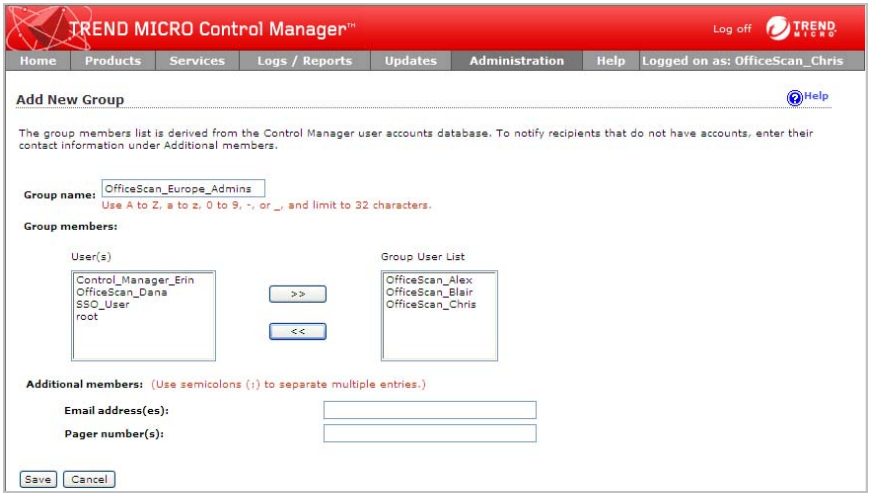
Example: All OfficeScan administrators for a region would want to be informed of an outbreak, even if the outbreak was not on a server that was managed by that particular administrator.

To add a user group for OfficeScan administrators:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.
3. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
4. Click **User Groups** from the sub-menu. The User Groups screen appears.



5. Click **Add New Group**. The Add New Group screen appears.

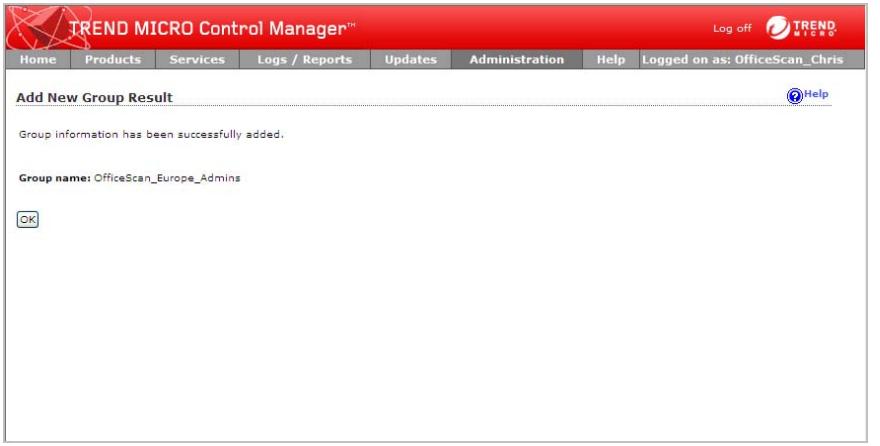


6. Type the following in the **Group name** field:

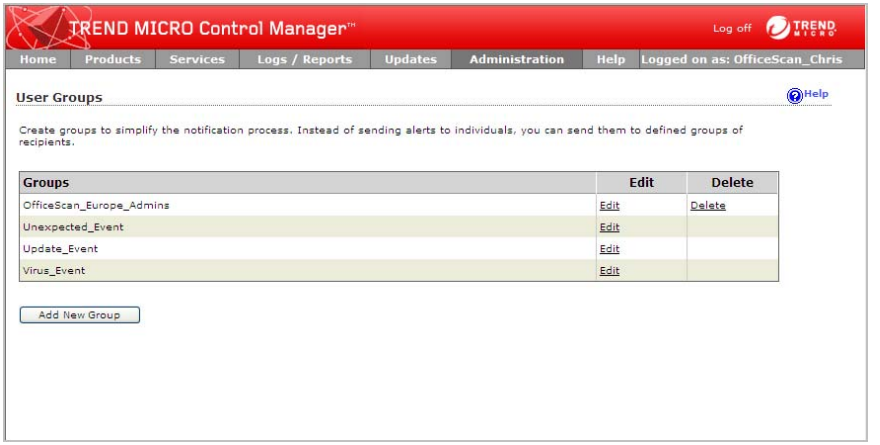
   OfficeScan_Europe_Admins

7. Under Group Members, add the following users to the group list:
   - **OfficeScan_Alex**
   - **OfficeScan_Blair**
   - **OfficeScan_Chris**

8. Click **Save**. The Add New Users Result screen appears with the details of the new group.



9. Click **OK**. The new group appears in the User Groups table.



Downloading and Deploying New Components

After setting up the user accounts for Control Manager, Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager selects the components for managed products registered to Control Manager that the user has been granted access to through their user account.

For example, Alex, Blair, and Chris will see the following components (all are OfficeScan components) enabled on the Manual Download and Scheduled download screens.

TABLE 3-10. Pattern files/Cleanup templates

OFFICESCAN COMPONENTS	DESCRIPTION
Virus Pattern	OfficeScan uses this file to detect viruses/malware (for example, I_LOVE_YOU, NIMDA) on desktops in your network • NTKD: Used for endpoint protection • Scan Engine for Windows XP/Server 2003 on x64 architecture: Common Firewall driver for early Windows products used for endpoint protection
Damage Cleanup Template	Damage Cleanup Services pattern
Common Firewall Pattern	Pattern used by desktop products for firewall protection
Spyware Active-monitoring Pattern	Pattern file the scan engine uses to detect spyware/grayware
IntelliTrap Pattern	Pattern file used by the IntelliTrap scan engine to detect security risks
IntelliTrap Exception Pattern	Pattern file used by the IntelliTrap scan engine to detect security risks
Spyware Pattern	Pattern file the scan engine uses to detect spyware/grayware
Anti-rootkit Driver (32-bit)	Anti-root kit prevention
Virus Cleanup Engine (Digitally signed, 32-bit)	Virus cleanup engine used for removing spyware/grayware on 32-bit computers.
Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)	Virus cleanup engine used for removing spyware/grayware on 32-bit/64-bit computers.

TABLE 3-10. Pattern files/Cleanup templates

OFFICESCAN COMPONENTS	DESCRIPTION
Spyware Scan Engine (32-bit)	Scan engine used for detecting spyware/grayware on 32-bit computers.
Spyware Scan Engine (64-bit)	Scan engine used for detecting spyware/grayware on 64-bit computers.
Virus Scan Engine	At the heart of all Trend Micro products lies a proprietary scan engine, known as virus scan engine application interface (VSAPI), that is capable of detecting all virus/malware known to be "in the wild," or actively circulating. The 32-bit, multi-threaded scan engine checks files in real-time using the process called pattern matching. VSAPI also employs a number of heuristic scanning technologies that even allows it to detect new viruses/malware, not yet seen in the wild. In addition to viruses, the scan engine protects against mass mailing worms such as Nimda and CodeRed, macro and polymorphic viruses, Trojans, and Distributed Denial of Service (DDoS) attacks. The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help manage bandwidth).

Configuring Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Configuring manual component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

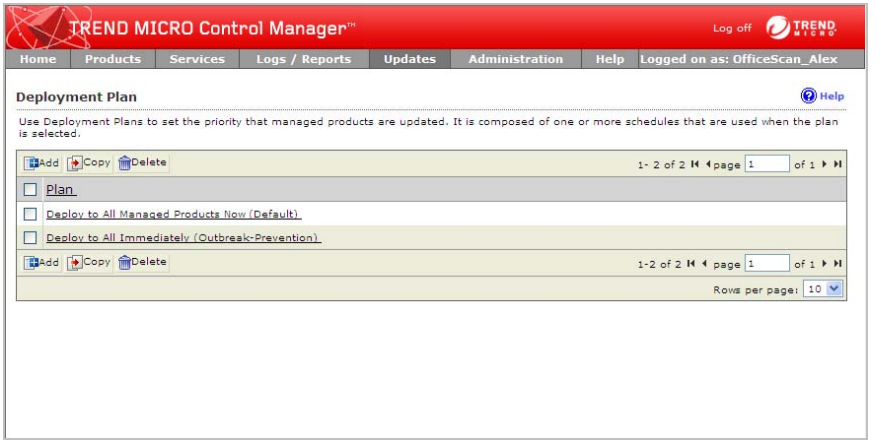
Step 6: Complete the manual download

To manually download components:

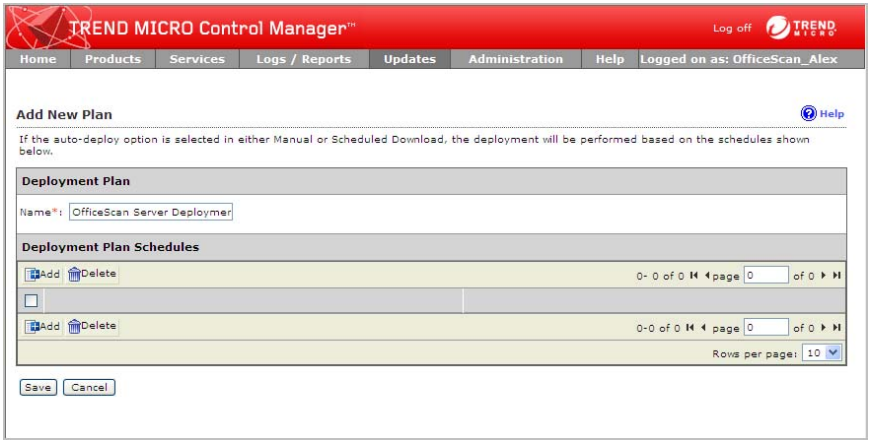
1. Log on to the Control Manager Web console as **Alex**.

Step 1: Configure a Deployment Plan for your components

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Deployment Plan** from the drop-down menu. The Deployment Plan screen appears.

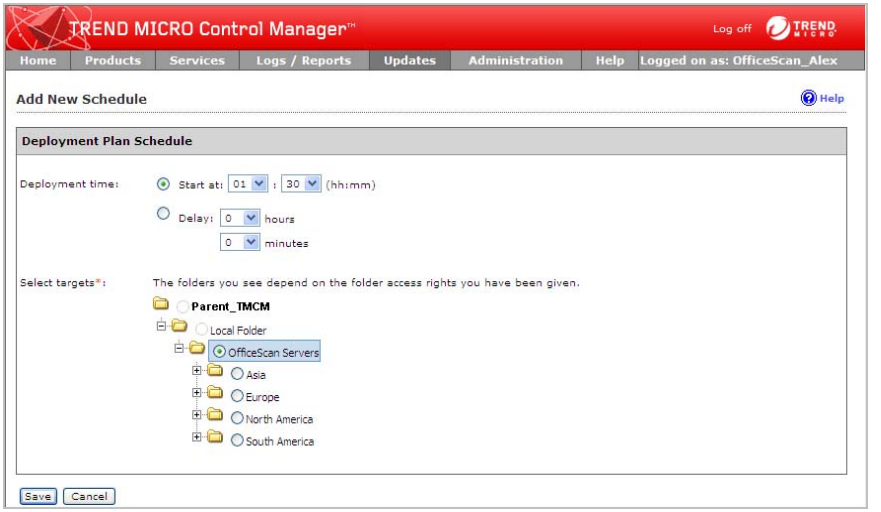


3. Click **Add**. The **Add New Plan** screen appears.



4. Type the following in the **Name** field:
   OfficeScan Server Deployment Plan

5. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.



Deployment time has the following options:

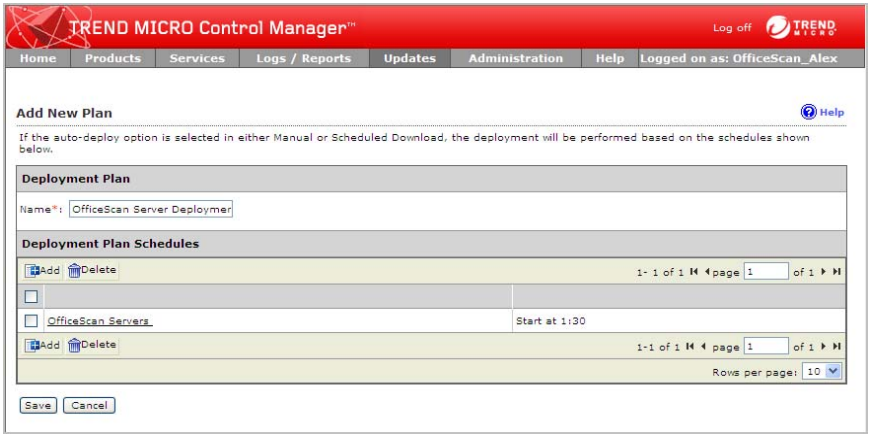
- **Start at:** Performs the deployment at a specific time
- **Delay:** after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

6. Specify the following for Deployment time:
   - Start at: **01:30**
7. Select the **OfficeScan Servers** from the Product Directory. Control Manager assigns the schedule to all the products under the selected folder.

Note: The managed products that appear in the Product Directory are based on the access privileges for the user's account.

---

8. Click **OK**. The Add New Schedule screen appears.

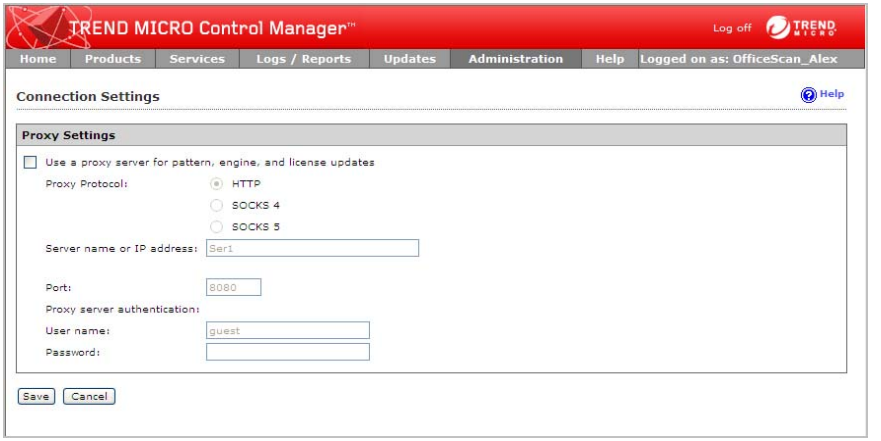


9. Click **Save** to apply the new deployment plan. The Deployment Plan screen appears.

Step 2: Configure your proxy settings, if you use a proxy server

1. Mouseover **Administration**. A drop-down menu appears.
2. Mouseover **Settings**. A sub-menu appears.

3. Click **Proxy Settings**. The Connection Settings screen appears.

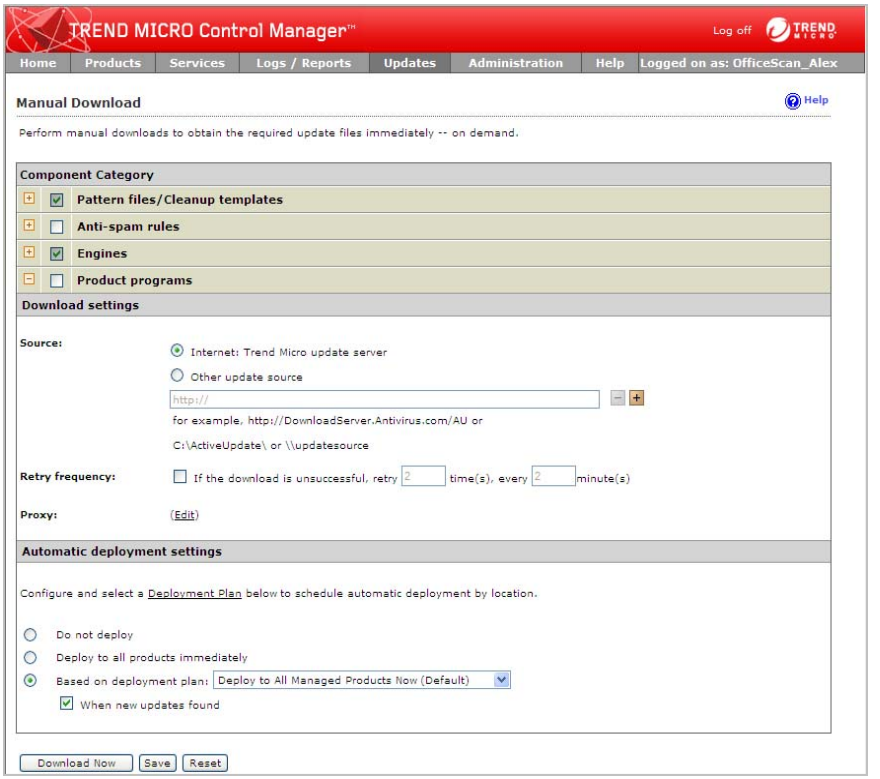


4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Select the protocol your proxy server uses:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
6. Type the host name or IP address of the proxy server in the **Server name or IP address** field.
7. Type the port number for the proxy server in the **Port** field.
8. Type a log on name and password if your server requires authentication.
9. Click **Save**.

Step 3: Select the components to update

1. Mouseover **Updates** on the main menu. A drop-down menu appears.

2. Click **Manual Download**. The Manual Download screen appears.



3. Click the + icon to expand the Pattern files/Cleanup templates list.
4. Alex is only interested in downloading OfficeScan components, so verify the following are selected from the Pattern files/Cleanup templates list:
   - **Virus Pattern**
   - **Damage Cleanup Template**
   - **Common Firewall Pattern**
   - **Spyware Active-monitoring Pattern**
   - **IntelliTrap Pattern**
   - **IntelliTrap Exception Pattern**

- **Spyware pattern**

5. Click the + icon to expand the Engines list.
6. Alex is only interested in downloading OfficeScan components, so verify that the following are selected from the Engines list:
   - **NTKD**
   - **Anti-rootkit Driver (32-bit)**
   - **Virus Cleanup Engine (Digitally signed, 32-bit)**
   - **Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)**
   - **Spyware Scan Engine (32-bit)**
   - **Spyware Scan Engine (64-bit)**
   - **Virus Scan Engine**

Step 4: Configure the download settings

1. Select **Internet: Trend Micro update server** as the update source. This means components download from the official Trend Micro ActiveUpdate server.

   If Alex wanted to download components from another update source (for example, from a server or Web location on her network), she would select **Other update source**. She could specify multiple update sources by clicking the + icon to add additional update sources. She can configure up to five update sources.
2. Enable **Retry frequency** and specify the following:
   - Number of retries: **3**
   - Time between retries: **5 minutes**

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

Step 5: Configure the automatic deployment settings

1. Under Schedule select the following:
   - **Based on deployment plan**
   - **When new updates found**

   This means Control Manager downloads new components as they become available and deploys the components to products based on the deployment plan you select.

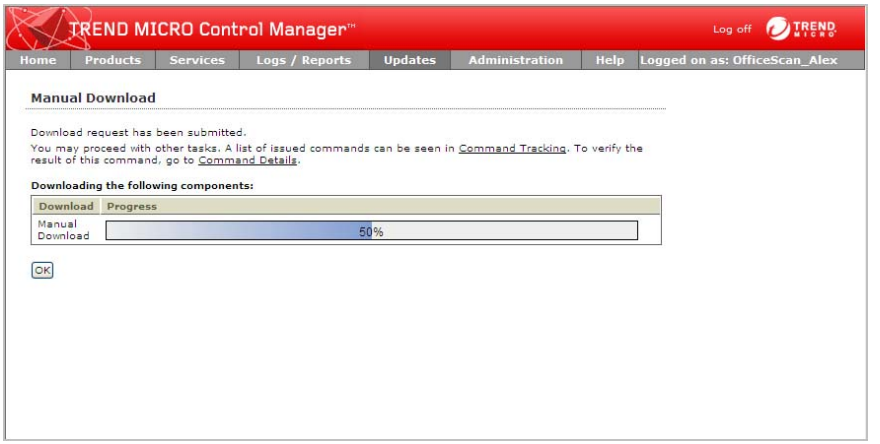
Alex could also have selected **Do not deploy**. If that option is selected components download to Control Manager, but do not deploy to managed products. Alex would use this option under the following conditions:

- Deploying to the managed products individually
- Testing the updated components before deployment

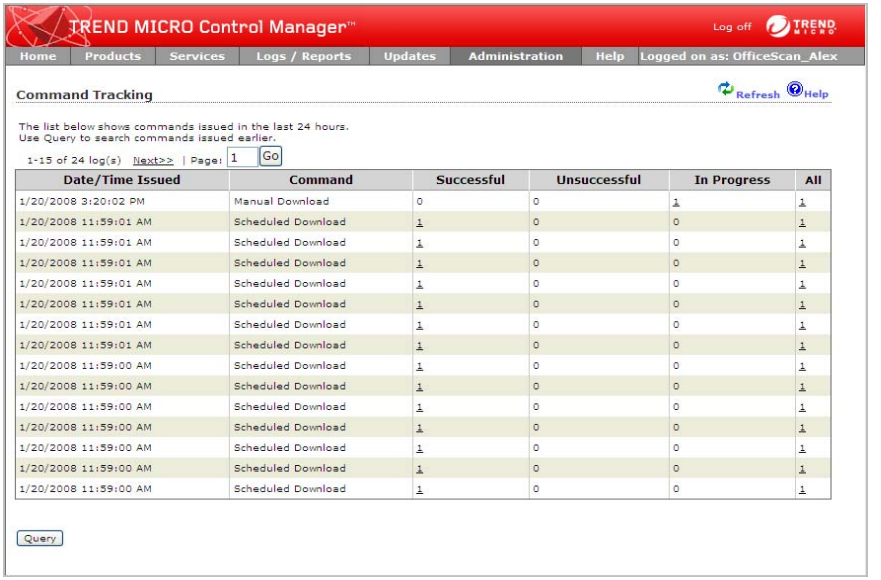
2. Select **OfficeScan Servers Deployment** from the Deployment plan list.
3. Click **Save**.

Step 6: Complete the manual download

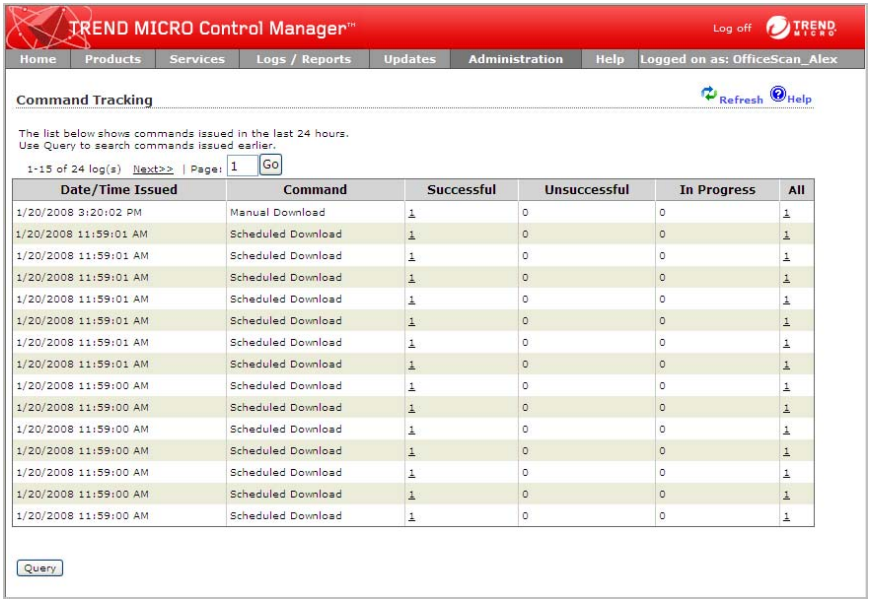
1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.



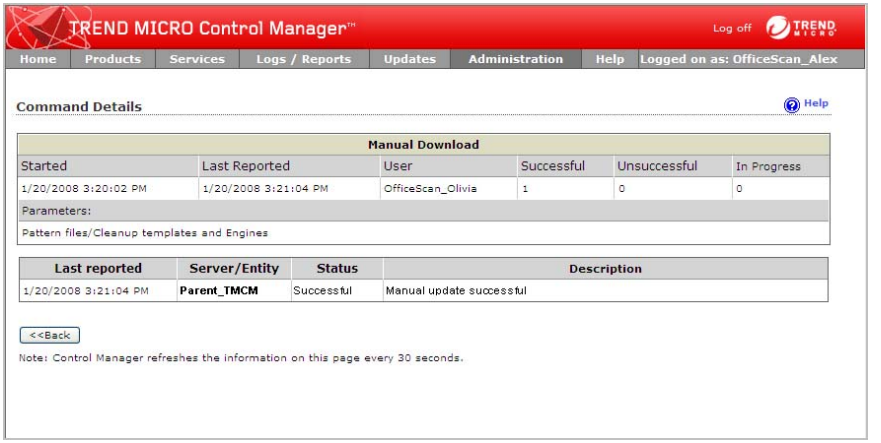
2. Click the **Command Details** to view details from the Command Details screen.



3. Click **Refresh** after a few minutes to verify if the download is successful.



4. Click the **1** in the **Successful** column for the **Manual Download** row. The Command Details screen appears.



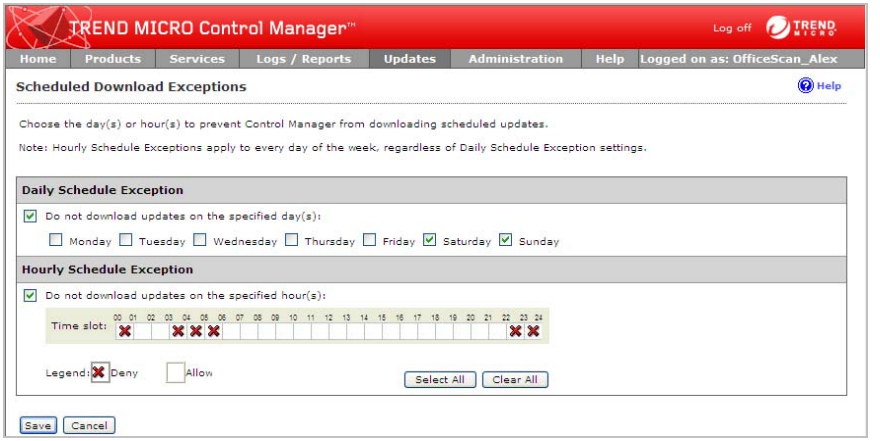
Configuring Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire days or for a certain time period every day.

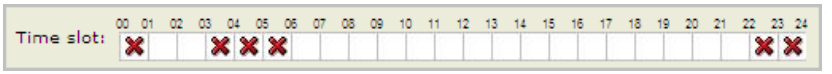
To configure scheduled download exceptions:

1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Updates** on the main menu. A drop-down menu appears.
3. Mouseover **Settings**. A sub-menu appears.

4. Click **Scheduled Download Exceptions**. The Scheduled Download Exceptions screen appears.



5. Select the following under Daily Schedule Exception:
   - **Do not download updates on the specified day(s)**
   - **Saturday**
   - **Sunday**

   Specifying these settings means downloads do not occur on Saturday and Sunday of every week.
6. Select the following under Hourly Schedule Exception:
   - **Do not download updates on the specified hour(s)**
   - 

   This means that downloads do not occur everyday between the hours of 22:00 to 01:00 and 03:00 to 06:00.
7. Click **Save**.

Configuring Scheduled Downloads

After configuring Manual Download settings, Trend Micro recommends configuring Scheduled Download settings. By default, Control Manager selects the components for managed products registered to Control Manager that the user has been granted access to through their user account.

Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component updates
- **Enabled:** Indicates if the schedule for the component is enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

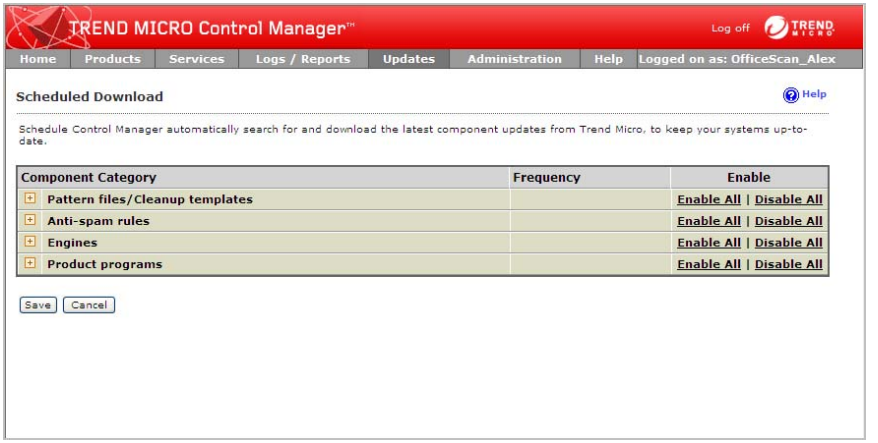
When configuring settings for scheduled downloading of components **Step 1** and **Step 2** of the process were completed, so the process will start at **Step 3**.

To configure scheduled downloads for components

Step 3: Select the components to update

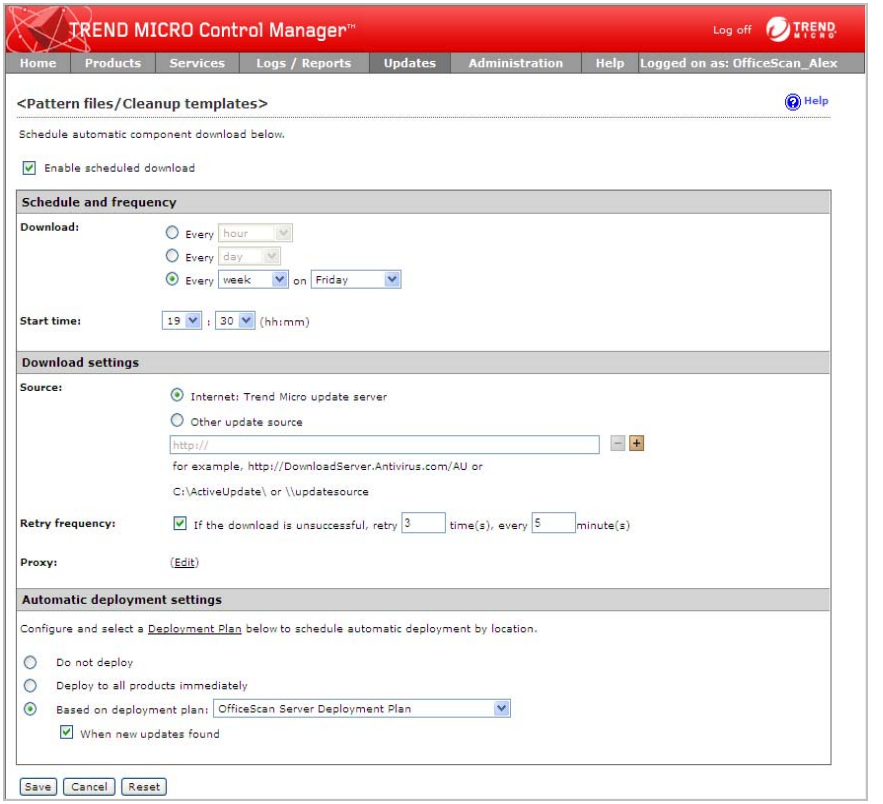
1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Updates** on the main menu. A drop-down menu appears.

3. Click **Scheduled Download**. The Scheduled Download screen appears.



4. Click the + icon to expand the Pattern files/Cleanup templates list.

5. Alex is only interested in downloading OfficeScan components, so click **Virus Pattern** from the Pattern files/Cleanup templates list:. The <Pattern files/Cleanup templates> screen appears.



Step 4: Configure the download schedule

6. Select the **Enable scheduled download** checkbox.
7. Under Schedule and Frequency specify the following:
   - Every: **week** on **Friday**
   - Start time: **19:30**

By default OfficeScan 8.0 servers download updates from their update source every Sunday at 00:00. To be prepared for the OfficeScan server download, Alex wants to download the Virus pattern every Friday at 19:30. She has many other options available to her and if the OfficeScan 8.0 download schedule is different from the default settings, she would have to adjust her settings accordingly.

Step 5: Configure the download settings

1. Select **Internet: Trend Micro update server** as the update source. This means components download from the official Trend Micro ActiveUpdate server.

   If Alex wanted to download components from another update source (for example, from a server or Web location on her network), she would select **Other update source**. She could specify multiple update sources by clicking the + icon to add additional update sources. She can configure up to five update sources.

2. Enable **Retry frequency** and specify the following:
   - Number of retries: **3**
   - Time between retries: **5 minutes**

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

Step 6: Configure the automatic deployment settings

1. Under Schedule, select the following:
   - **Based on deployment plan**
   - **When new updates found**

   This means Control Manager downloads new components as they become available and deploys the components to products based on the deployment plan you select.

   Alex could also have selected **Do not deploy**. If that option is selected components download to Control Manager, but do not deploy to managed products. Alex would use this option under the following conditions:
   - Deploying to the managed products individually
   - Testing the updated components before deployment

2. Select **OfficeScan Servers Deployment** from the Deployment plan list.
3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click the status button in the Enabled column.
2. Click **Save**.
3. Repeat steps 3 to 7 for the following:
   - **Damage Cleanup Template**
   - **Common Firewall Pattern**
   - **Spyware Active-monitoring Pattern**
   - **IntelliTrap Pattern**
   - **IntelliTrap Exception Pattern**
   - **Spyware pattern**
   - **NTKD**
   - **Anti-rootkit Driver (32-bit)**
   - **Virus Cleanup Engine (Digitally signed, 32-bit)**
   - **Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)**
   - **Spyware Scan Engine (32-bit)**
   - **Spyware Scan Engine (64-bit)**
   - **Virus Scan Engine**

Chapter 4

Monitoring the Control Manager Network

Control Manager provides several options to monitor the Control Manager network. Summary screens, notifications, logs, and reports all provide ways for you to monitor the network.

This chapter covers the following topics:

Using Command Tracking

The Control Manager server maintains a record of all commands issued to managed products and child servers. Commands refer to instructions given to managed products or child server to perform specific tasks (for example, performing a component update). Command Tracking allows you to monitor the progress of all commands.

For example, after issuing a Start Scan Now task, which can take several minutes to complete, you can proceed with other tasks and then refer to Command Tracking later for results.

The Command Tracking screen presents the following details in table format:

TABLE 4-1. Command Tracking Details

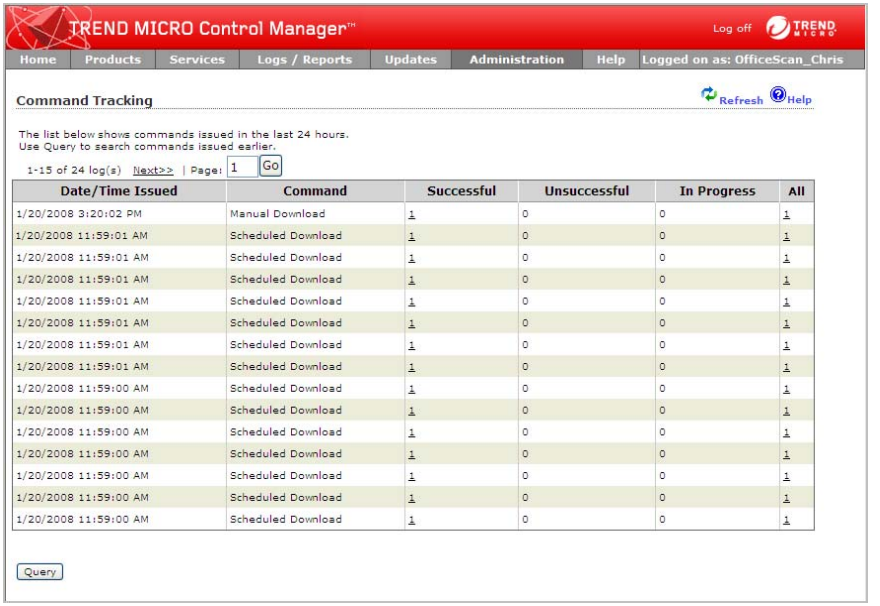
INFORMATION	DESCRIPTION
Date/Time Issued	The date and time when the Control Manager server issued the command to the managed product or child server
Command	The type of command issued
Successful	The number of managed products or child servers that completed the command
Unsuccessful	The number of managed products or child servers unable to perform the command
In Progress	The number of managed products or child servers that currently perform the command
All	The total number of managed products and child servers to which Control Manager issued the command

Clicking the available links in the **Successful**, **Unsuccessful**, **In Progress**, or **All** column opens the Command Details screen.

Example: Chris wants to check the status on component updates to OfficeScan servers.

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.

3. Click **Command Tracking** from the menu. The Command Tracking screen appears.



Everything looks fine, but if there was a problem with one of the component downloads Chris could check the command details.

Using Event Center

Alex wants to be notified if there is unusual activity on the ACME CO. network. She decides to hold meetings with the other OfficeScan administrator's to gather their input before she puts a plan into action. After careful internal discussion Alex and the other OfficeScan administrators are most concerned with the following:

- Outbreaks
- Issues dealing with a security risk
- Issues with OfficeScan and OfficeScan's component updates

In the future, she would also consider configuring special virus and spyware/grayware alerts but for now Alex needs to configure the following notifications:

TABLE 4-2. Alert Events Notifications

ALERT	DESCRIPTION
Virus outbreak alert	Alex can configure settings for what she considers a serious enough outbreak before sending a notification.
Virus found - first action unsuccessful and second action unavailable	Alex has a notification sent to all administrators when OfficeScan detects a virus, but OfficeScan is unable to handle the virus correctly.
Virus found - first and second actions unsuccessful	Alex has a notification sent to all administrators when OfficeScan detects a virus, but OfficeScan is unable to handle the virus correctly.
Spyware/Grayware found - further action required	Alex has a notification sent to all administrators when OfficeScan detects spyware/grayware, but OfficeScan is unable to handle the virus correctly.

TABLE 4-3. Update Events Notifications

UPDATE	DESCRIPTION
Scan engine update unsuccessful	For the ACME CO. network to remain protected, all components must be up-to-date. Alex wants to be informed immediately when an issue occurs while updating components.
Pattern files/Cleanup templates update unsuccessful	

TABLE 4-4. Unusual Events Notifications

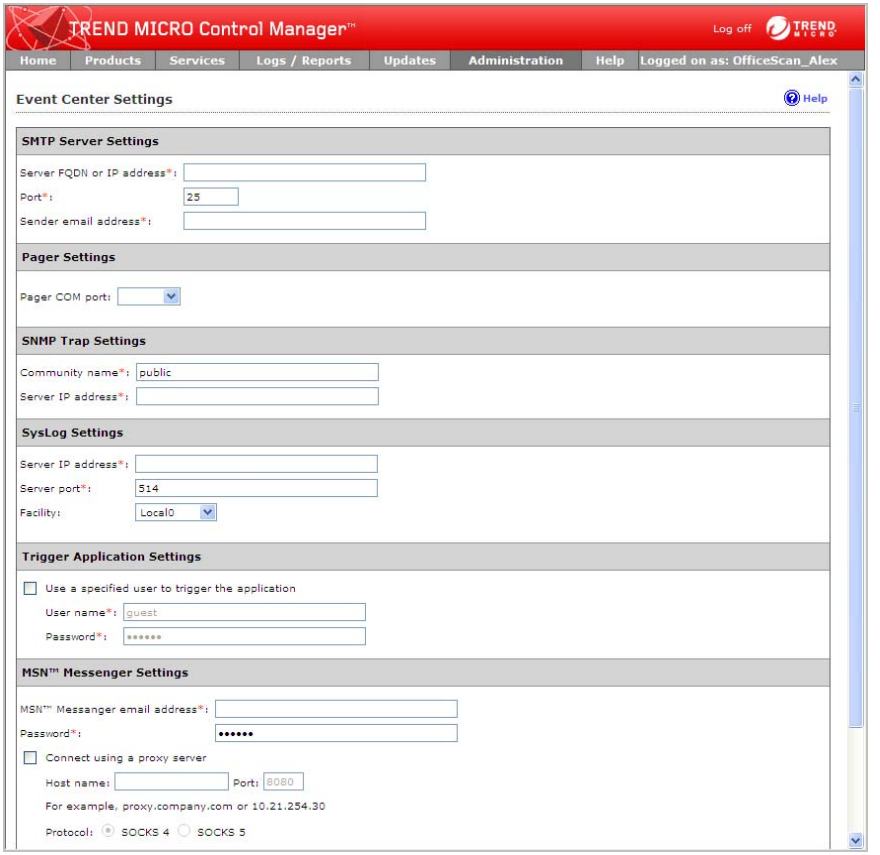
UNUSUAL	DESCRIPTION
Real-time scan disabled	For the ACME CO. network to remain protected, OfficeScan and Real-time Scan must be working properly. Alex wants to be informed immediately when an issue occurs with OfficeScan or Real-time Scan.
Product service stopped	

Configuring Event Notification Methods

Before anyone can receive notifications, Alex needs to configure the notification methods for all notification types.

To configure notification method settings:

1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.
3. Mouseover **Settings** on the drop-down menu. A sub-menu appears.
4. Click **Event Center Settings** from the sub-menu. The Event Center Settings screen appears.



5. Configure the notification method:

   To set email notifications:

   a. On the working area under **SMTP Server Settings**, type the **host name** and **port number** of the SMTP server in the fields provided. Use the fully qualified domain name (FQDN) (example, `proxy.company.com`), or the IP address of the SMTP server.

   b. Type the Control Manager **Sender's email address**. Control Manager will use this address as the sender's address (a requirement for some SMTP servers).

   To set pager notifications:

   • On the working area under **Pager COM Port**, select the appropriate **COM port** from the list.

   To set SNMP notifications:

   a. On the working area under **SNMP Trap Settings**, specify the **Community name**.

   b. Specify the SNMP trap server **IP address.**

   To set syslog notifications:

   a. On the working area under **Syslog Settings**, type the **host name** and **port number** of the syslog server in the fields provided. Use the fully qualified domain name (FQDN) (example, `proxy.company.com`), or the IP address of the syslog server.

   b. Specify the facility for syslogs.

   To trigger a specified application:

   a. On the working area under **Trigger Application Settings**, select **Use a specified user to trigger the application**.

   b. Type the **user name** and **password** of the user who triggers the specified application.

To set MSN Messenger notifications:

a. On the working area under **MSN Messenger Settings**, specify the **MSN Messenger email address**. This is the user name in MSN Messenger.

b. Type the .Net Passport email address **password**.

c. If you use a proxy server to connect to the Internet, select **Use a proxy server to connect to MSN server**.

   i. Specify the proxy server **host name** and **port**.

   ii. Select the proxy server protocol—**Socks 4** or **Socks 5**.

   iii. Type the **log on name** and **password** used for proxy authentication.

6. Click **Save**.

Configuring Notification Recipients and Testing Notification Delivery

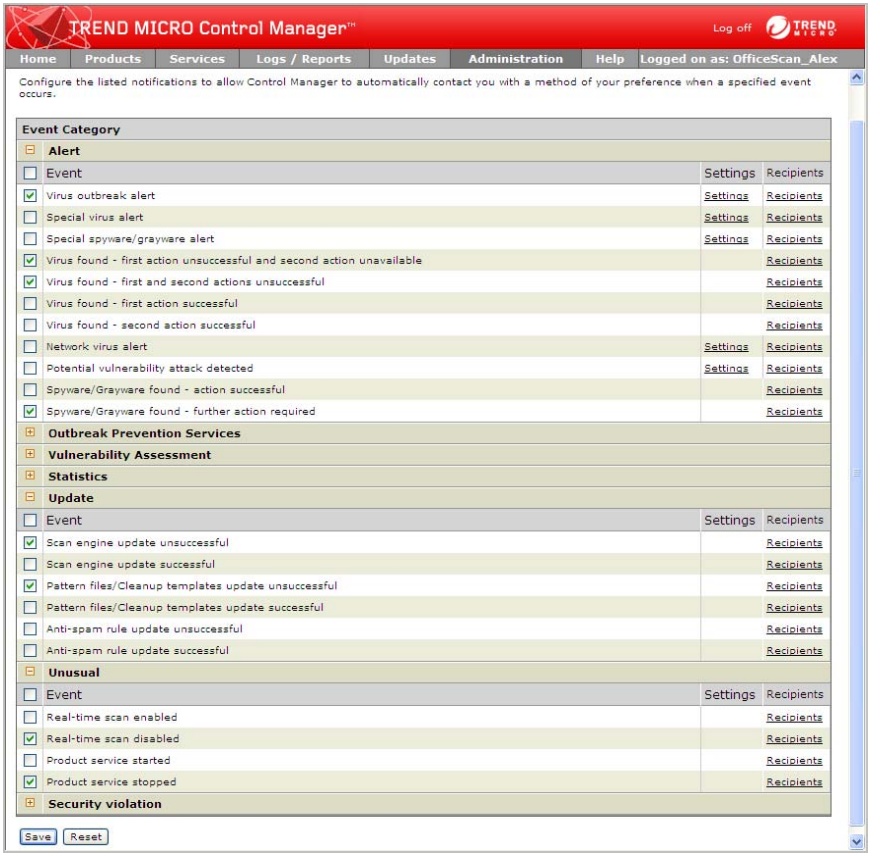
Once the notification methods for all notification types has been configured, Alex can now configure the notifications that are required for ACME CO.'s OfficeScan administrators.

To configure the notification recipients and test notification delivery:

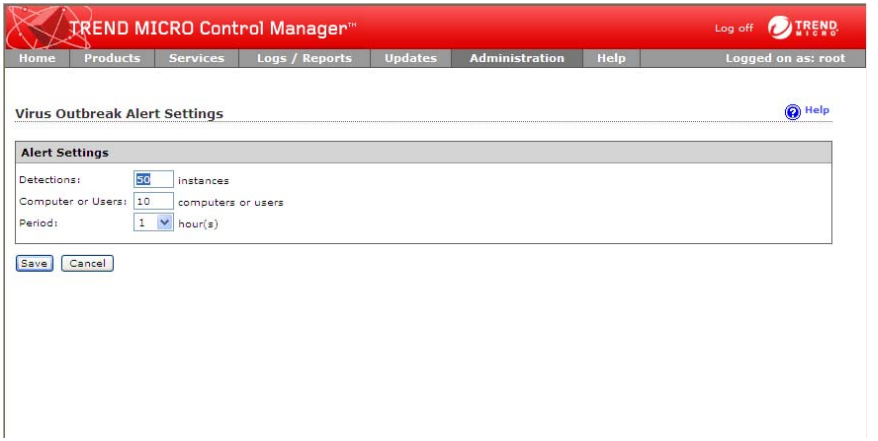
1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.

3. Click **Event Center** from the drop-down menu. The Event Center screen appears.

4. Expand the **Alert**, **Update**, and **Unusual** Event Categories. All available notifications for the categories display.



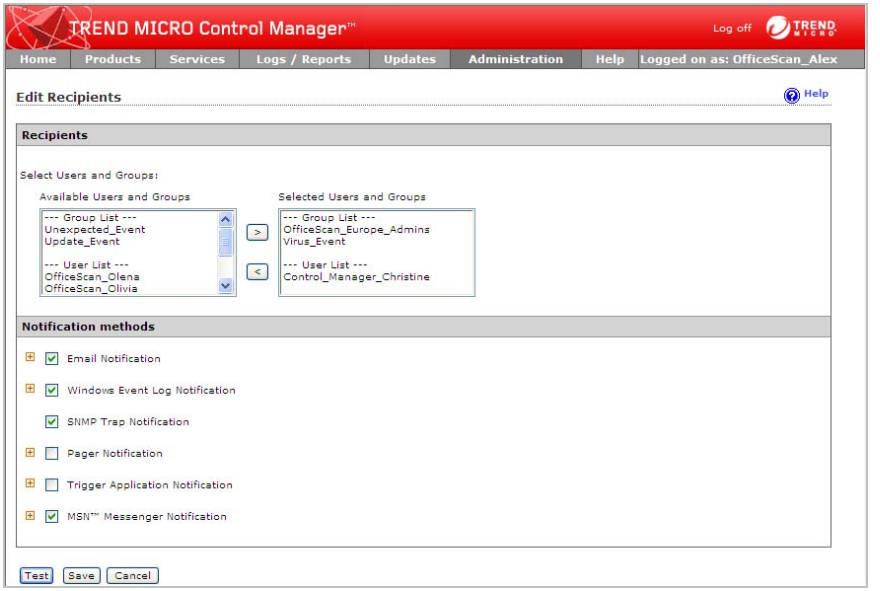
5. Click the **Settings** link for **Virus outbreak alert**. The Virus Outbreak Alert Settings screen appears.



6. Under Alert Settings, provide the following:
   - Detections: **50**
   - Computer or Users: **10**
   - Period: **1 hour**

   This means that if there are 50 or more detections across 10 computers over the course of an hour an alert is sent to all notification recipients.
7. Click **Save**. The Event Center screen appears.

8. Click the **Recipients** link for **Virus outbreak alert**. The Edit Recipients screen appears.



9. Under **Recipients**, add **OfficeScan_Europe_Admins** and **Control_Manager_Erin** to the **Selected Users and Groups** list.
10. Under **Notification methods**, select and expand **Email Notification**, **Windows Event Log Notification**, **SNMP Trap Notification**, and **MSN™ Messenger Notification**.
11. Add the following variables to the notification messages for **Email Notification** and **Windows Event Log Notification**:
    - **%pname%**: Managed product name
    - **%entity%**: Product Directory path of the managed product where an event occurred
    - **%computer%**: Network name of the client machine where an event was detected
12. Expand the notification method and provide a **notification message** in the corresponding message fields.

13. Click **Test** to verify delivery of the notifications.
14. Click **Save**. The Event Center screen appears.
15. Repeat steps 7 to 12 for the following:
    - **Virus found - first action unsuccessful and second action unavailable**
    - **Virus found - first and second actions unsuccessful**
    - **Spyware/Grayware found - further action required**
    - **Scan engine update unsuccessful**
    - **Pattern files/Cleanup templates update unsuccessful**
    - **Real-time scan disabled**
    - **Product service stopped**

Using Logs

Although Control Manager receives data from various log types, Control Manager now allows users to query the log data directly from the Control Manager database. The user can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

Configuring Log Aggregation

Control Manager log aggregation provides a way for administrators to decrease the impact that managed products have on network bandwidth. By configuring log aggregation administrators can choose which log information managed products send to Control Manager.

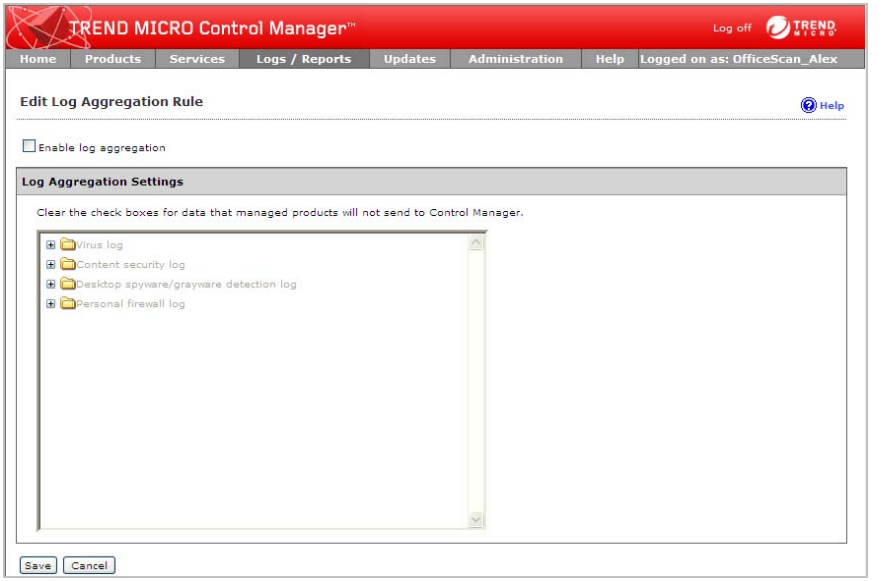
WARNING! Log aggregation comes at a cost. Information that managed products do not send to Control Manager is lost. Control Manager cannot create reports or queries for information the server does not have. This can raise issues if information that seems unimportant, and managed products drop, later becomes of critical importance with no way to recover the dropped data.

Alex wants to check the information that she could potentially stop OfficeScan servers from sending to Control Manager.

To configure log aggregation settings:

1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Mouseover **Settings** from the drop-down menu. A sub-menu appears.

4. Click **Log Aggregation** from the sub-menu. The Log Aggregation Settings screen appears.



5. Expand the **Virus log** list.

   After viewing the list Alex decides she does not want to enable log aggregation. She wants all information from OfficeScan sent to Control Manager.

6. Click **Cancel**.

Deleting Logs

Alex does not want to delete any logs for at least a year. By default, all logs are configured for deletion within 45 to 90 days, which means that Alex needs to disable automatic log deletion for all log types.

Configuring Automatic Log Deletion Settings

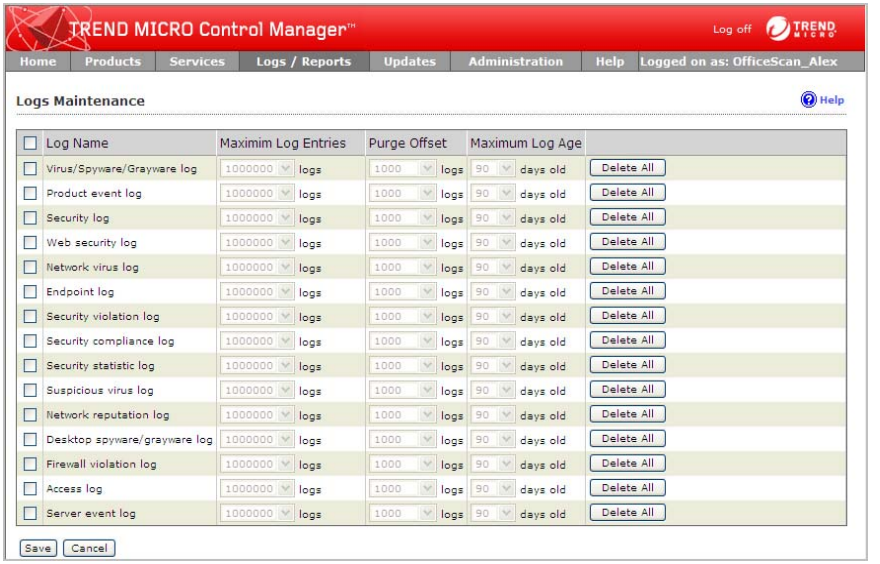
The Log Maintenance screen provides two methods for deleting logs automatically:

- By number of logs (minimum: 30,000, maximum: 1,000,000, default: 1,000,000)
- By the age of logs (minimum: 1 day, maximum: 90 days, default: 45 to 90 days)

Purge offset specifies the number of logs Control Manager deletes when the number of logs for a log type reaches the maximum. The default purge setting is 1000 for all log types.

To configure purge log settings:

1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.
3. Mouseover **Settings**. A sub-menu appears.
4. Click **Log Maintenance** from the submenu. The Log Maintenance screen appears.



5. Clear the corresponding checkbox for all log types.
6. Click **Save**.

Querying Log Data

Control Manager now supports gathering only the data an administrator needs from Control Manager and managed product logs. Control Manager supports this using Ad Hoc Queries. Ad Hoc Queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Using Ad Hoc Queries to pull data directly from the database provides a very powerful tool for administrators.

While 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 for further analysis, or save the query for future use. Control Manager also supports sharing Saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc Query consists of the following process:

Step 1: Select the managed product or current Control Manager server for the query

Step 2: Select the Data View to query

Step 3: Specify filtering criteria, and the specific information that displays

Step 4: Save and complete the query

Step 5: Export the data to CSV or XML

Note: Control Manager supports sharing saved Ad Hoc queries with other users. Saved and shared queries appear on the **Logs/Reports > Saved Ad Hoc Queries** screen.

Understanding Data Views

A Data View is a table consisting of cluster of related data cells. Data Views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Each heading in a data view acts as a column in a table. For example the Spyware/Grayware Action Result Summary has the following headings:

- Action Result
- Action Taken
- Infection Destination Count

- Infection Source Count
- Virus/Malware Detection Count

As a table, a data view takes the following form with potential sub-headings under each heading:

TABLE 4-5. Sample Data View Table

Action Result	Infection Source Count	Action Taken	Virus/Malware Detection Count	Infection Destination Count

This information is important to remember when specifying how data displays in a report template.

Control Manager separates Data Views into two major categories: Product Information and Security Threat Information. See *Appendix A: Understanding Data Views* on page A-1 for more information. The major categories separate further into several sub-categories, with the sub-categories separated into summary information and detailed information.

The Control Manager Web console displays the Data Views and the information available from each Data View.

TABLE 4-6. Control Manager Major Data View Categories

MAJOR DATA VIEW CATEGORY	DESCRIPTION
Product Information	Displays information about: • Control Manager • Managed products • Managed product components • Product license information

TABLE 4-6. Control Manager Major Data View Categories

MAJOR DATA VIEW CATEGORY	DESCRIPTION
Security Threat Information	Displays information about security threats that managed products detect: • Overall Security Risks • Malware/viruses • Spyware/grayware • Content violations • Spam • Web content violations • Policy/Rule violations • Suspicious threats

Note: For more information about the available data views Control Manager supports, see *Appendix A: Understanding Data Views* on page A-1.

Performing an Ad Hoc Query

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 whether to query the Control Manager server the user is currently logged on to, or to query the managed products the Control Manager manages. The managed products could include other Control Manager Child servers.

After selecting the managed products/directory from which the data originates, select a data view for the query. For more information on data views see *Understanding Data Views* on page 4-16.

After selecting the data view, specify the query filter criteria, the specific information the query displays, and the order in which the information displays.

Note: Control Manager supports specifying up to 20 criteria for filtering Ad Hoc Query data.

Finally specify whether to save the query for future use. Control Manager supports sharing of saved queries, so other users can benefit from useful queries.

Create a New Ad Hoc Query

Chris wants to search for detailed data about spyware/grayware instances on the network, but COOKIES are grouped in to this category. Chris wants to filter the query results so that it contains data about all spyware/grayware detected by the OfficeScan servers he is responsible for, without any data about COOKIES. Chris also only wants to see spyware/grayware that requires further action (OfficeScan was not able to clean) on his part.

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports** on the main menu. A drop-down menu appears.
3. Click **New Ad Hoc Query** from the drop-down menu. The Ad Hoc Query Step 1: Data Scope screen appears.

   From the Data Scope screen you select the network protection category, by selecting the managed product or directory from the Product Directory.

Step 1: Specify the origin of the information:

1. From the New Ad Hoc Query screen, select **Select Product Tree**.

   Chris has access to all managed products under the **OfficeScan Servers > Europe > England** folder (OfficeScan servers EN-OFFICESCAN_01, EN-OFFICESCAN_02, and EN-OFFICESCAN_03). He does not have access to information from any other sources.

   Chris can only choose **Select Product Tree** even though there are two choices available:

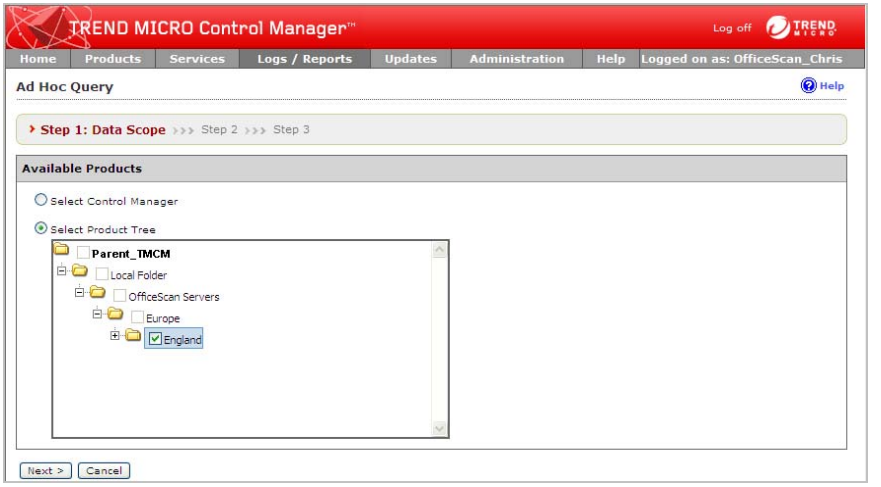
   - **Select Control Manager:** Specifies that information originates from the Control Manager server to which the user is currently logged on.

     Specifying this option disables the Product Tree, because the information only comes from the Control Manager server to which the user is logged on.

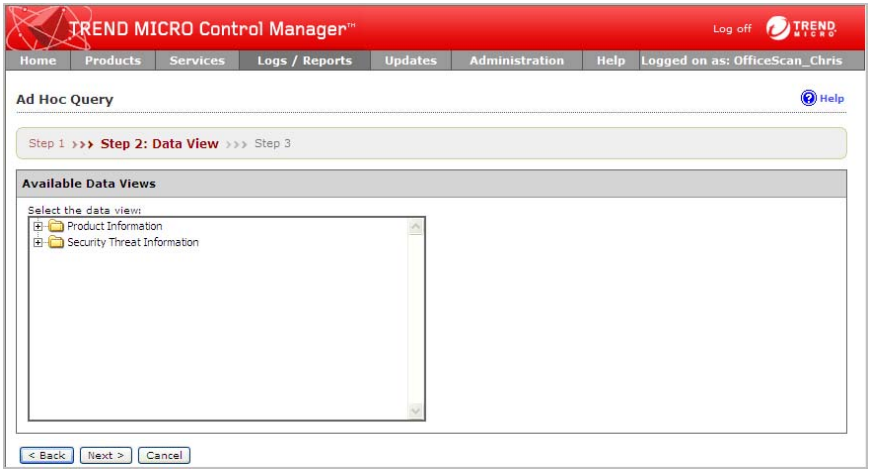
   - **Select Product Tree:** Specifies that information originates from the managed products the Control Manager server manages.

     After specifying this option, the user must then select the managed products/directories from Product Tree from which the information originates.

2. Expand the Product Directory and select **England**.



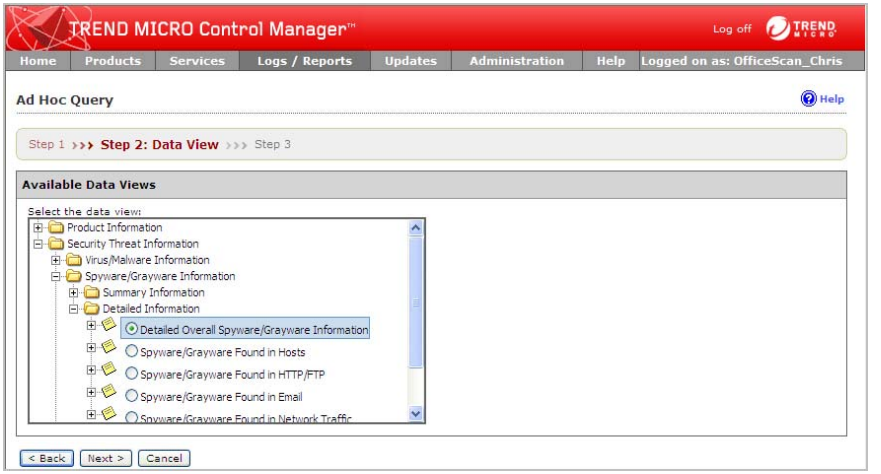
3. Click **Next**. The Select Data View screen appears.



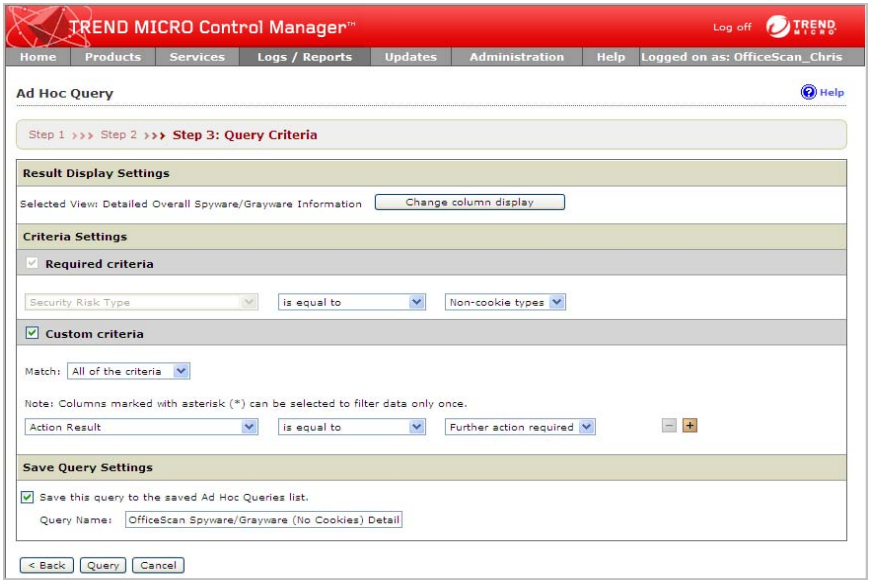
Step 2: Specify the data view for the query:

1. Expand the **Available Data Views** list to **Security Threat Information > Spyware/Grayware Information > Detailed Information** and select **Detailed**

Overall Spyware/Grayware Information. For more information on data views, see *Understanding Data Views* on page 4-16.



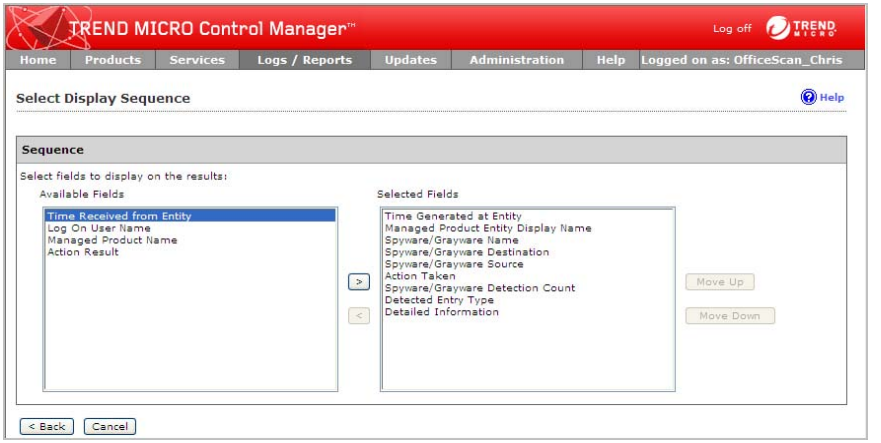
2. Click **Next**. The Query Criteria screen appears.



Step 3: Specify filtering criteria and the display sequence:

1. Specify the display and sequence for the information the query returns.

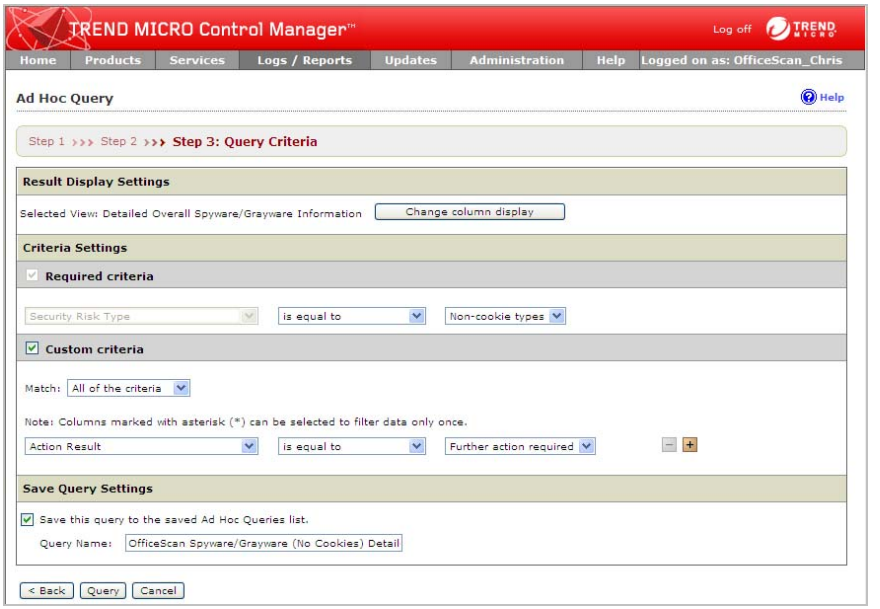
a. Click **Change column display**. The Select Display Sequence screen appears.



b. Remove the following from the **Selected Fields** list:

- **Time Received From Entity:** Chris only needs one value for time
- **Log On User Name:** The network uses the user name in the host name for the computer
- **Managed Product Name:** All products under the OfficeScan Server folder are OfficeScan servers
- **Action Result:** Chris will filter his results to only include entries that require further action

c. Click **Back**. The Query Criteria screen appears.



2. Specify the filtering criteria:

Required Criteria:

a. Specify the following filtering criteria:

- **Security Risk Type > is equal to > Non-cookie types**

Custom Criteria:

a. Select **Enable custom criteria** under Criteria Settings on the Query Criteria screen.

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 the analysis of the data that the query returns.

---

b. Chris wants to match all filter criteria for the query. He has two options

- **Any of the criteria:** Acts as a logical OR function for the criteria. That means data returns if it matches any of the specified filtering criteria.
- **All of the criteria:** Acts as a logical AND function for the criteria. That means data returns only if it matches all of the specified filtering criteria.

Select **All of the criteria** from the **Match** criteria from the drop-down list.

c. Specify the following filtering criteria:

- **Action Result > is equal to > Further action required**

Note: You can add up to 20 filter criteria for each data view.

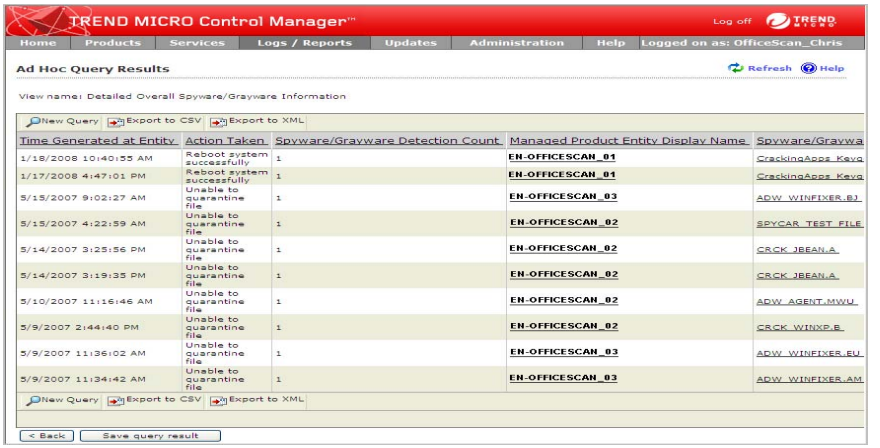
Step 4: Save and complete the query:

1. Click **Save this query to the saved Ad Hoc Queries list** under Save Query Settings to save the Ad Hoc query.
2. Specify an the following name in the **Query Name** field:
   - **OfficeScan Spyware/Grayware (No Cookies) Detailed Information**

Note: Control Manager supports sharing saved Ad Hoc Queries with other users. Saved Queries appear on the **Logs/Reports > My Reports** screen.

---

3. Click **Query**. The Results screen appears displaying the results of the query.



For more detailed information about a given item, click the underlined link for the item.

Step 5: Export the query results to CSV or XML:

1. A File Download dialog box appears after clicking one of the following:
   - **Export to CSV:** Exports the query results to CSV format.
   - **Export to XML:** Exports the query results to XML format.
2. Complete one of the following:
   - Click **Open** to view the query results immediately in CSV or XML format.
   - Click **Save**. A Save As dialog box appears. Specify the location to save the file.

Working With Saved and Shared Ad Hoc Queries

Control Manager supports saving an Ad Hoc query a user creates. Saved Ad Hoc queries appear on the **Logs/Reports > Saved Ad Hoc Queries** screen. The Saved Ad Hoc Queries screen contains two tabs: My Queries and Available Queries.

The My Queries section of the Saved Ad Hoc Queries screen displays all Ad Hoc Queries the logged on user created. From the My Queries screen, the user can add, edit,

view, delete, export, and share/unshare queries. Sharing saved queries makes the queries available to other users.

Note: Control Manager access control, provided by the user account and user type, restricts the information to which a user has access. This means that even though all users can view shared queries, access control limits the effectiveness of the query.

Editing Saved Ad Hoc Queries

Control Manager supports modifying saved Ad Hoc queries from the My Queries tab of the Saved Ad Hoc Queries screen. Modifying a saved Ad Hoc query requires the following steps:

Step 1: Select the managed product or current Control Manager server for the query

Step 2: Select the Data View to query

Step 3: Specify filtering criteria, and the specific information that displays

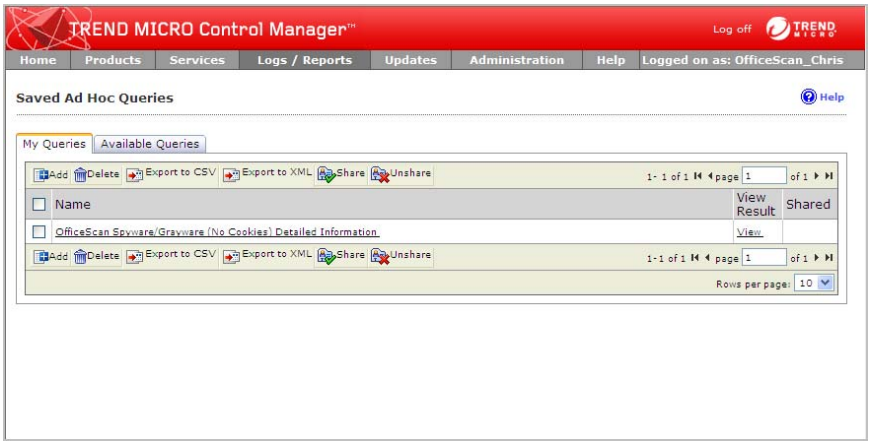
Step 4: Save and complete the query

Step 5: Export the data to CSV or XML

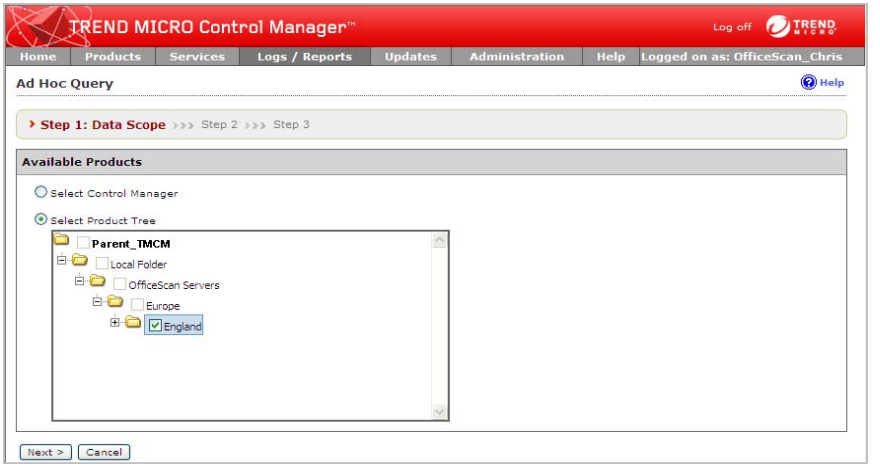
Chris decides that the original Ad Hoc Query still has too much information displaying when a query returns. He decides to further reduce the number of columns in the query and the order that information displays in the returned query.

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports** on the main menu. A drop-down menu appears.

3. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.



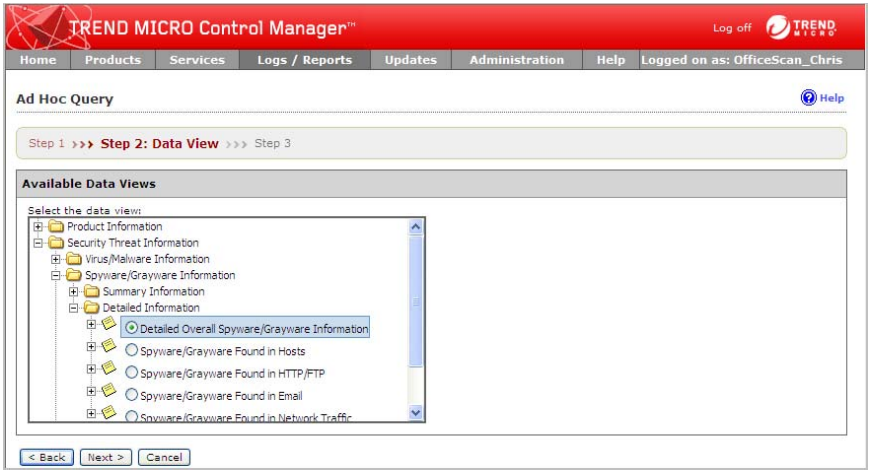
4. Click **OfficeScan Spyware/Grayware (No Cookies) Detailed Information**. The Select Product Tree screen appears.



Step 1: Specify the origin of the information:

Chris does not need to change the source of the information

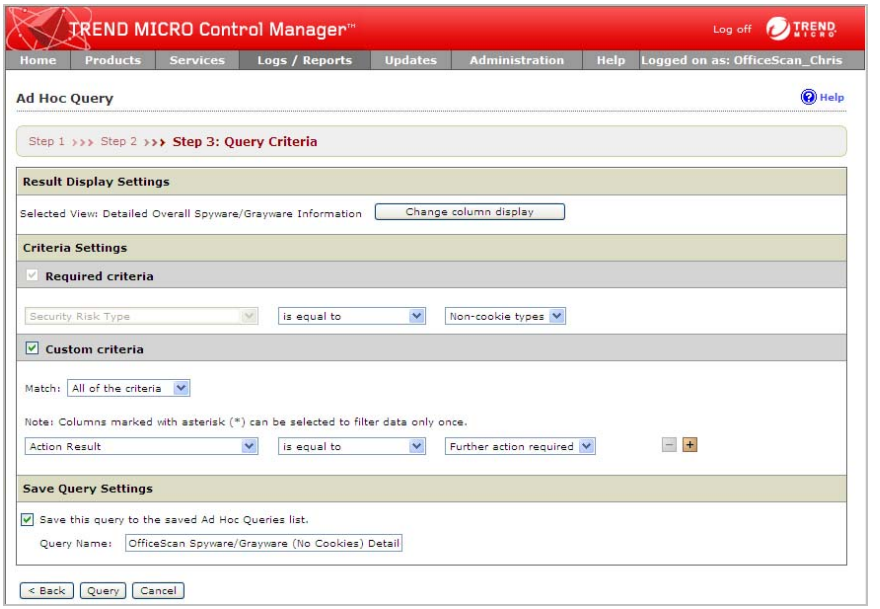
1. Click **Next**. The Select Data View screen appears.



Step 2: Specify a data view for the query:

Chris does not need to change the data view for the query.

1. Click **Next**. The Query criteria screen appears.

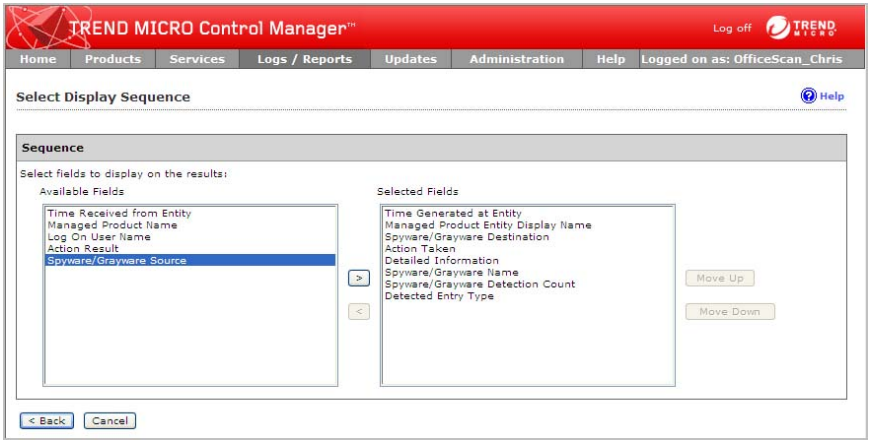


Step 3: Specify filtering criteria and the display sequence:

Chris wants to display less information from the returned query and to change the sequence that the information displays.

1. Specify the display and sequence for the information the query returns:

a. Click **Change column display**. The Select Display Sequence screen appears.



b. Remove the following from the **Selected Fields** list:

- **Spyware/Grayware Source**

c. Change the order of the columns to the following:

- **Time Generated at Entity**
- **Managed Product Entity Display Name**
- **Spyware/Grayware Destination**
- **Action Taken**
- **Detailed Information**
- **Spyware/Grayware Name**
- **Spyware/Grayware Detection Count**
- **Detected Entry Type**

d. Click **Back**. The Query Criteria screen appears.

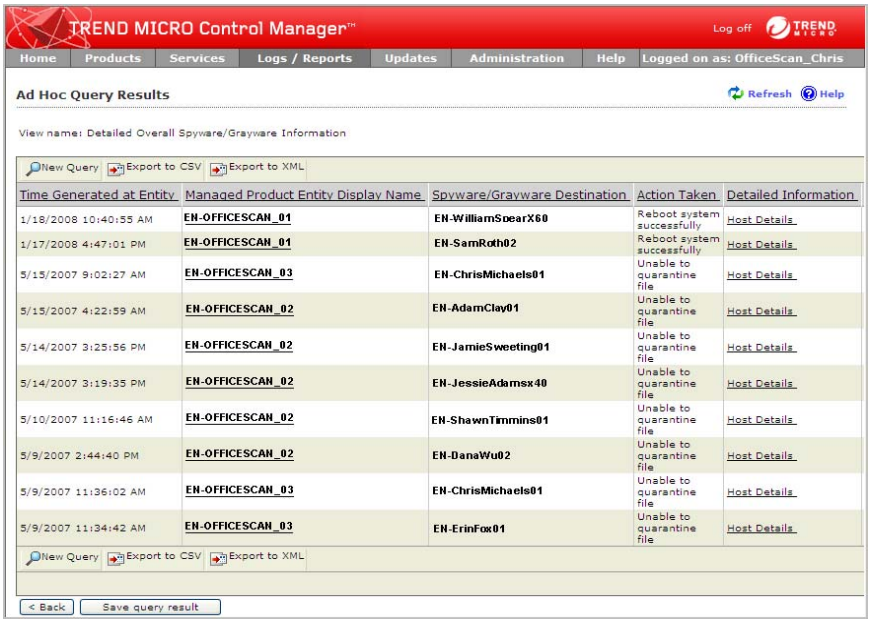
2. Chris does not want to change the filtering criteria for the query.

Step 4: Save and complete the query:

Chris does not need to change the save settings.

> **Note:** Control Manager supports sharing saved Ad Hoc Queries with other users. Saved Queries appear on the **Logs/Reports > My Reports** screen.

1. Click **Query**. The Results screen appears displaying the results of the query.



Step 5: Export the query results to CSV or XML:

1. A File Download dialog box appears after clicking one of the following:
   - **Export to CSV:** Exports the query results to CSV format.
   - **Export to XML:** Exports the query results to XML format.

2. Complete one of the following:
   - Click **Open** to view the query results immediately in CSV or XML format.
   - Click **Save**. A Save As dialog box appears. Specify the location to save the file.

Sharing Saved Ad Hoc Queries

After modifying the Ad Hoc Query, Chris thinks that this query might be useful to other people, so he decides to share the query.

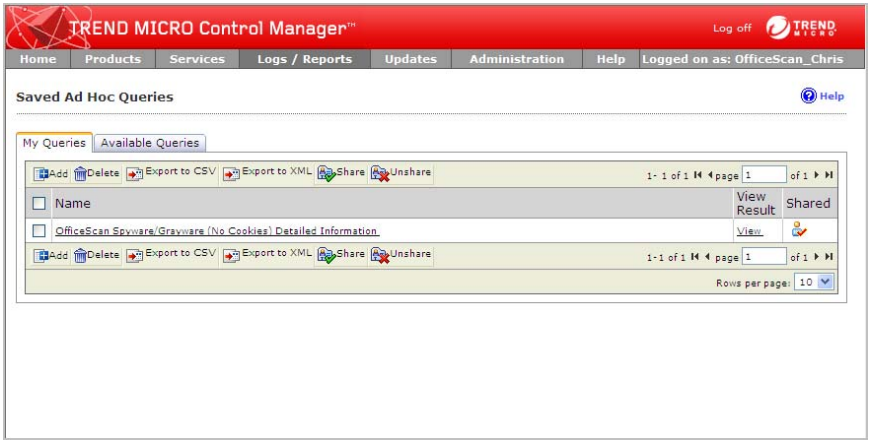
Note: Shared queries allow everyone with access to Control Manager to use the query. However, a user's access privileges prevent the user from using a saved query to gather information on parts of the Control Manager network that they do not have rights to access.

To share a saved Ad Hoc query:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.

4. Click the check box beside **OfficeScan Spyware/Grayware (No COOKIES) Detailed Information**.

5. Click **Share**. An icon appears in the Shared column for the saved Ad Hoc query.



Working With Shared Ad Hoc Queries

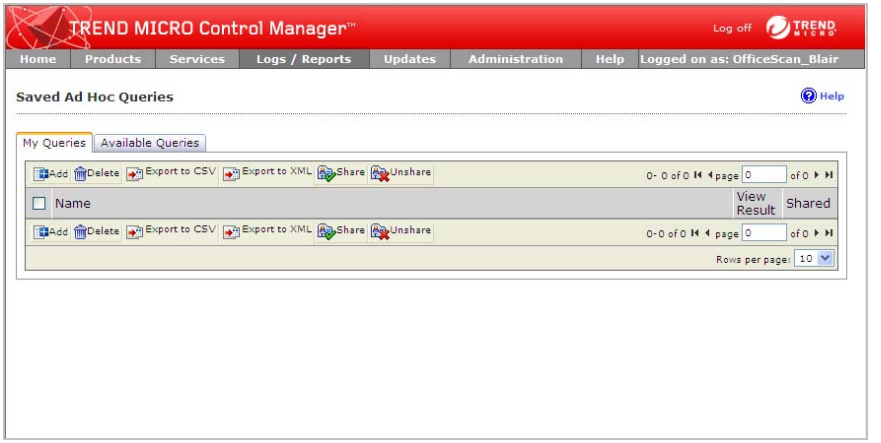
After creating an Ad Hoc query, a user can share the query with other users. All shared queries from all users appear on the Available Queries tab of the Saved Ad Hoc Queries screen. Users can view, and export shared queries.

Blair receives an email from Chris about a new query that Blair may be able to use. Blair decides to have a look at the query Chris created.

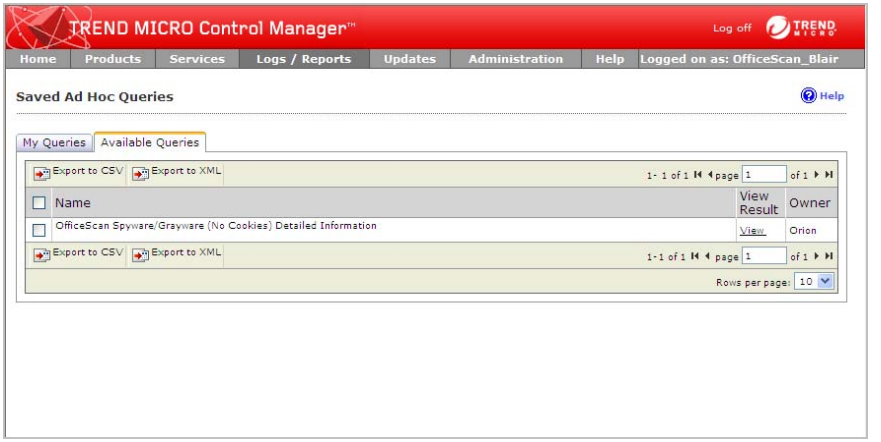
To access Available Queries:

1. Log on to the Control Manager Web console as **Blair**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.

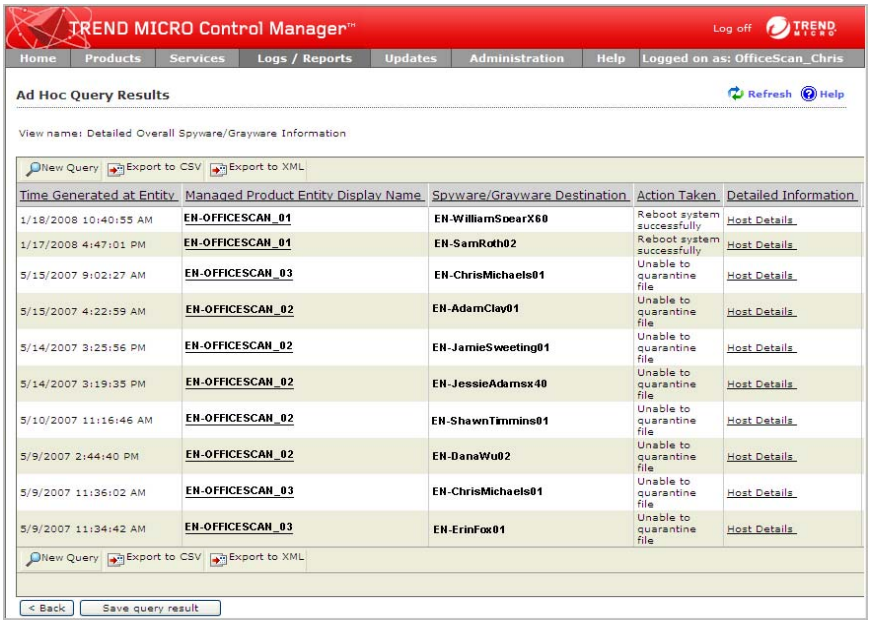
3. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.



4. Click **Available Queries**. The Available Queries tab appears.



5. Click **View** to look at the query.



Working With Reports

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduces radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 5.0 continues to support report templates from previous Control Manager versions, however Control Manager 5.0 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager 5.0 categorizes report templates according to the following types:

- **Control Manager 5.0 templates:** User-defined customized report templates that use direct database queries (database views) and report template elements (charts/graphs/tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions. For more information on Control Manager 5.0 templates, see the *Control Manager Administrator's Guide.*
- **Control Manager 3.0 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3.0 templates, see the *Control Manager Administrator's Guide.*.

Adding Control Manager 5.0 Report Templates

Control Manager 5.0 templates allow greater flexibility for report generation than previous versions of Control Manager templates. Control Manager 5.0 templates directly access the Control Manager database, providing users the opportunity to create reports based on any information the Control Manager database contains.

Adding a Control Manager 5.0 custom template requires the following steps:

1. Access the Add Report Template screen and name the template.
2. Specify the template component to add to the report template.

3. Specify the data view for the template.
4. Specify the query criteria for the template.
5. Specify the data to appear in the report and the order in which the data appears.
6. Complete report template creation.

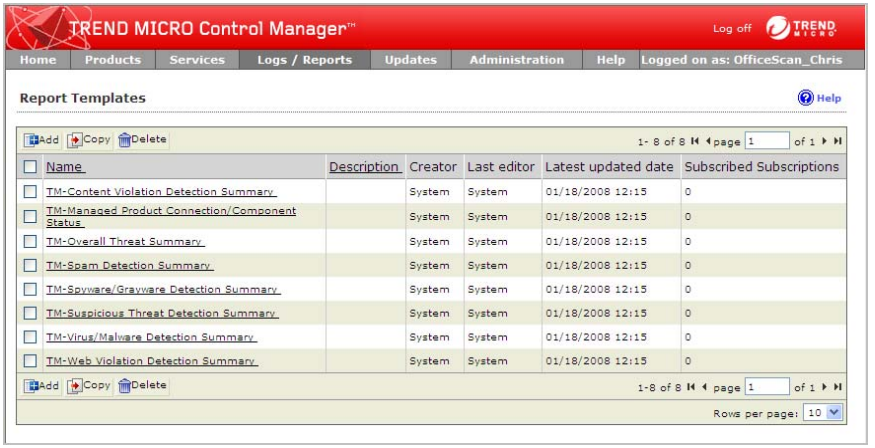
Modifying an Existing Template

Chris wants to create a report for spyware/grayware detected by his OfficeScan servers. He does not want COOIKES included in the report. Instead of creating a new report, he would like to modify one of the existing reports Control Manager has available.

To add a Control Manager 5.0 report template from an existing template:

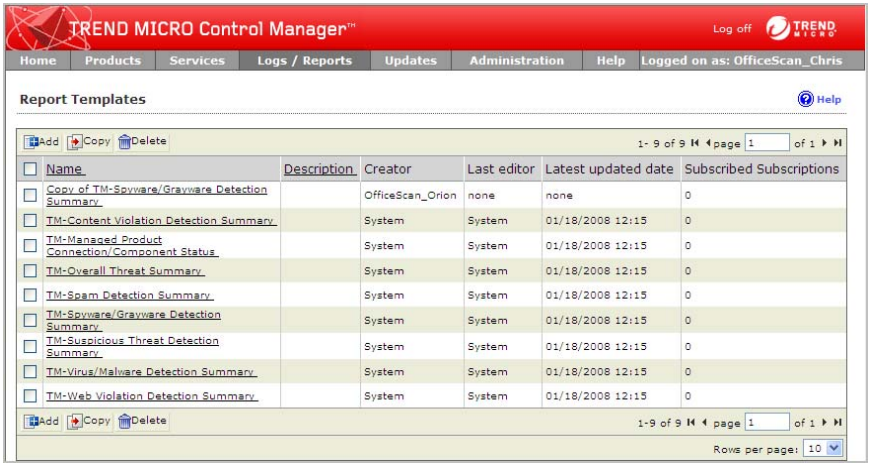
Step 1: Access the Add Report Template screen and name the template:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Report Templates** from the menu. The Report Templates screen appears.

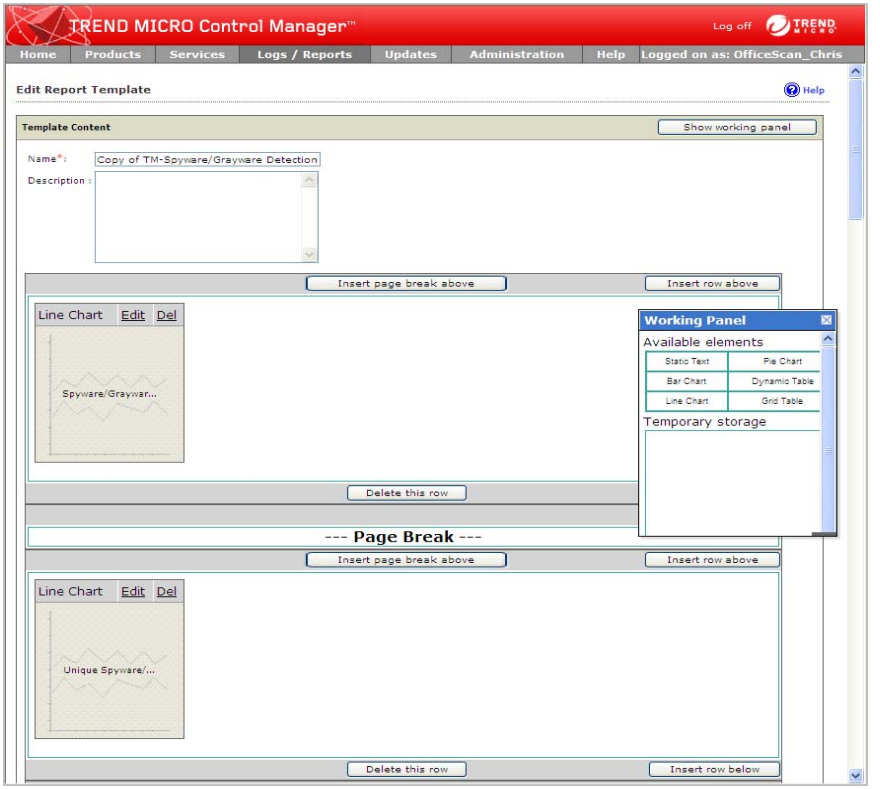


4. Select **TM-Spyware/Grayware Detection Summary**.

5. Click **Copy**. **Copy of TM-Spyware/Grayware Detection Summary** appears in the Report Templates list.



6. Click **Copy of TM-Spyware/Grayware Detection Summary**. The Edit Report Template screen appears.



7. Type the following in the **Name** field:

   OfficeScan Spyware/Grayware Detection Summary

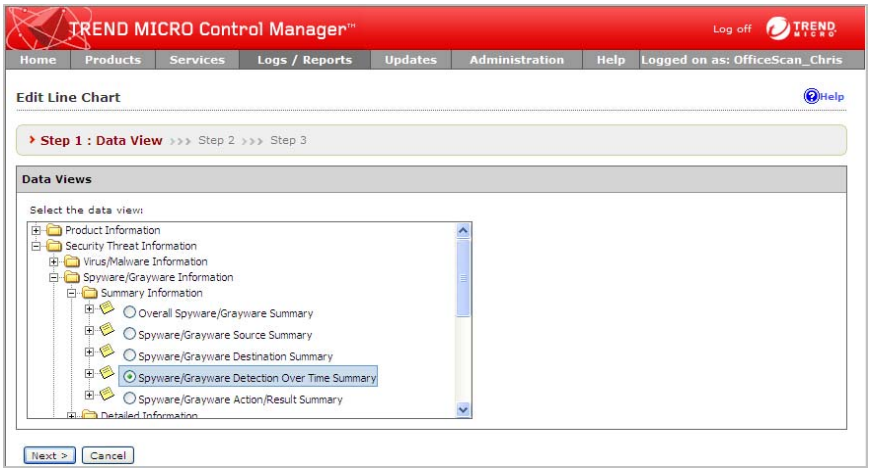
8. Type the following in the **Description** field:

   This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.

Edit the Report Template Element

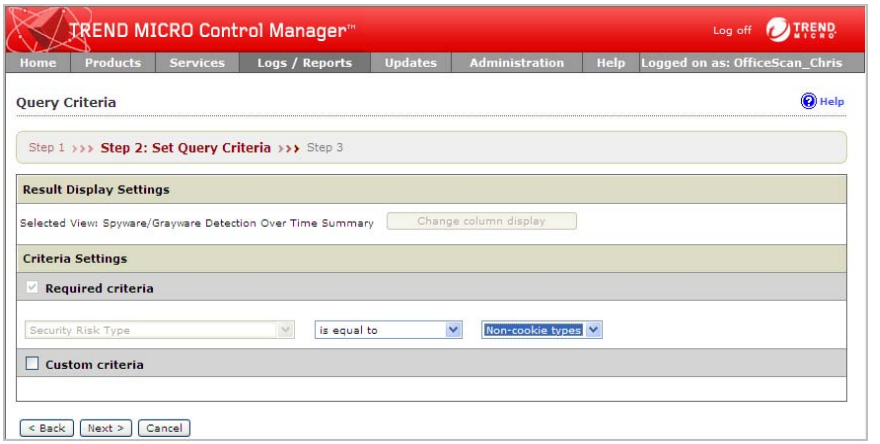
Step 1: Edit the Spyware/Grayware Detection Grouped by Day line chart:

1. Click **Edit** on the Spyware/Grayware Detection Grouped by Day line chart. The Edit Line Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

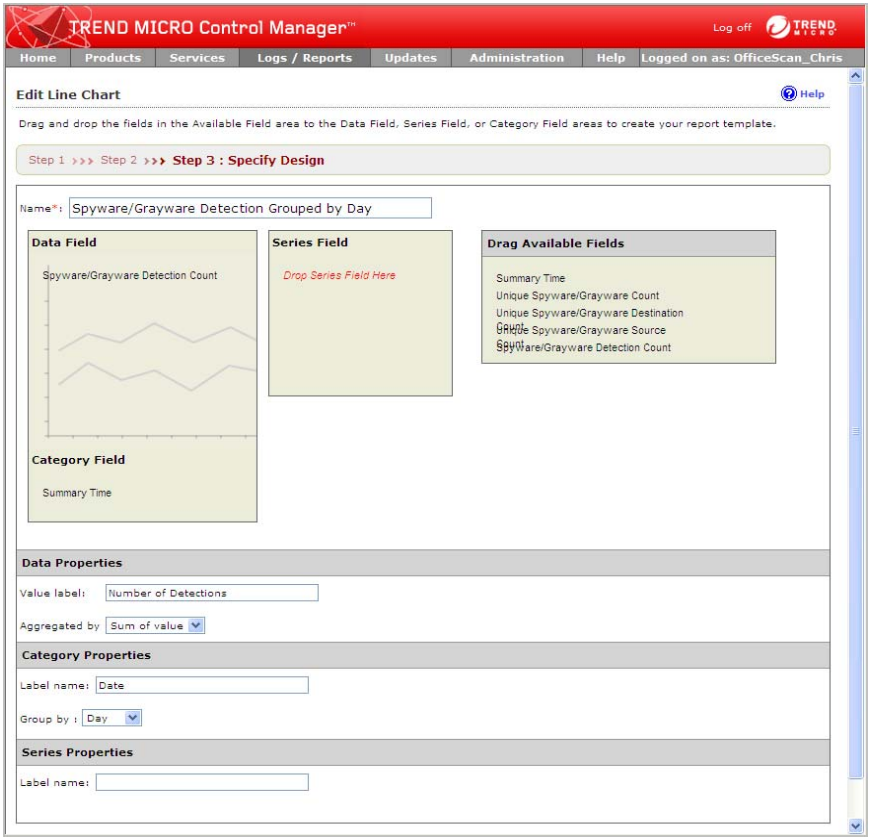
Chris does not want cookies to appear in his line chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

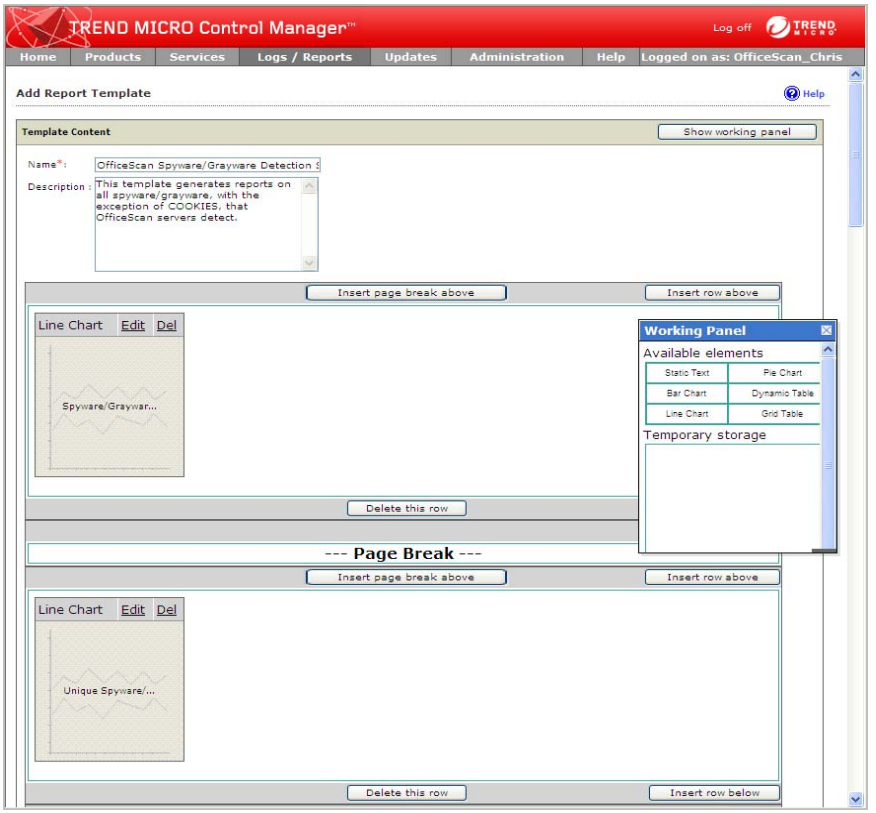
Step 3: Configure settings for the Spyware/Grayware Detection Grouped by Day line chart settings:

1. Click **Next**. The Edit Line Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Spyware/Grayware Detection Grouped by Day line chart.

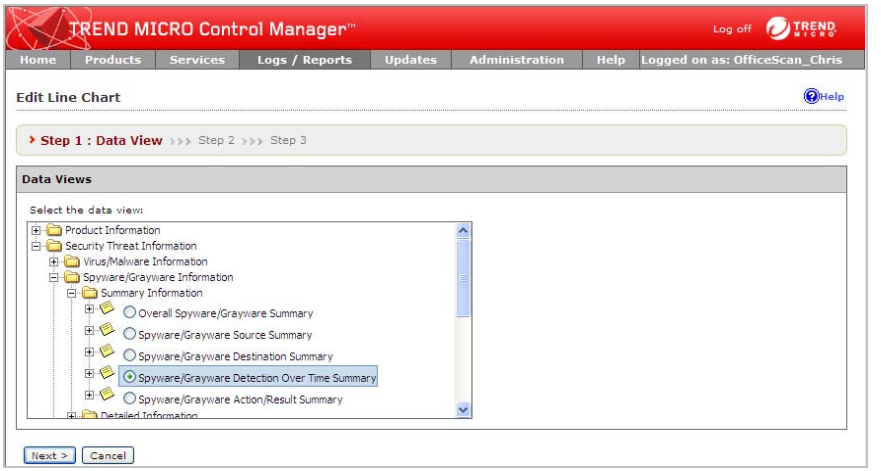
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

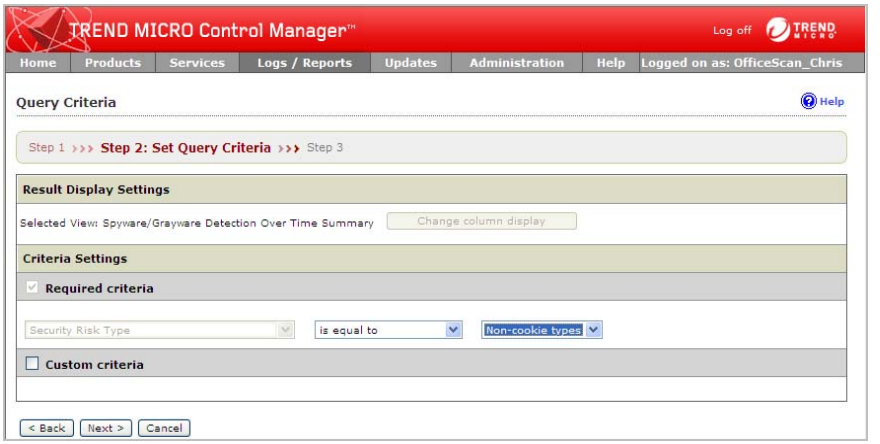
Step 1: Edit the Unique Spyware/Grayware Count Grouped by Day line chart:

1. Click **Edit** on the Unique Spyware/Grayware Count Grouped by Day line chart. The Edit Line Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

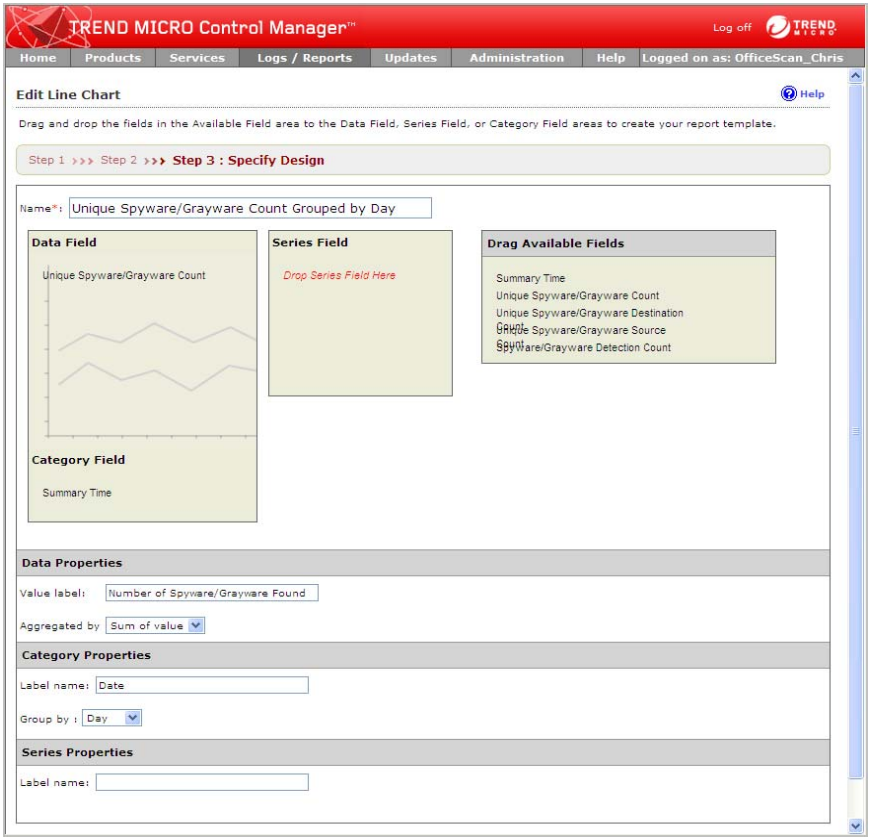
Chris does not want cookies to appear in his line chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

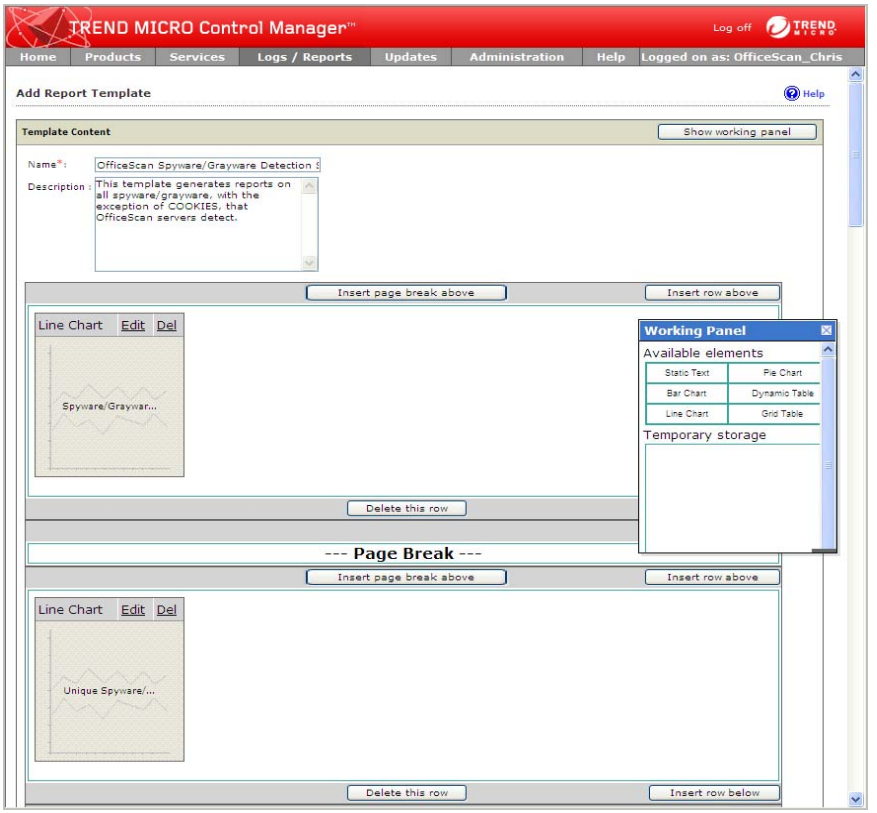
Step 3: Configure settings for the Unique Spyware/Grayware Count Grouped by Day line chart settings:

1. Click **Next**. The Edit Line Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Unique Spyware/Grayware Count Grouped by Day line chart.

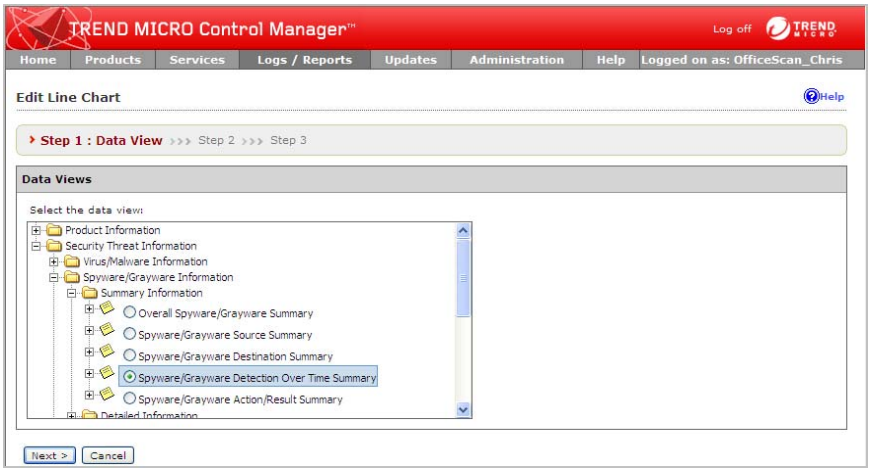
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

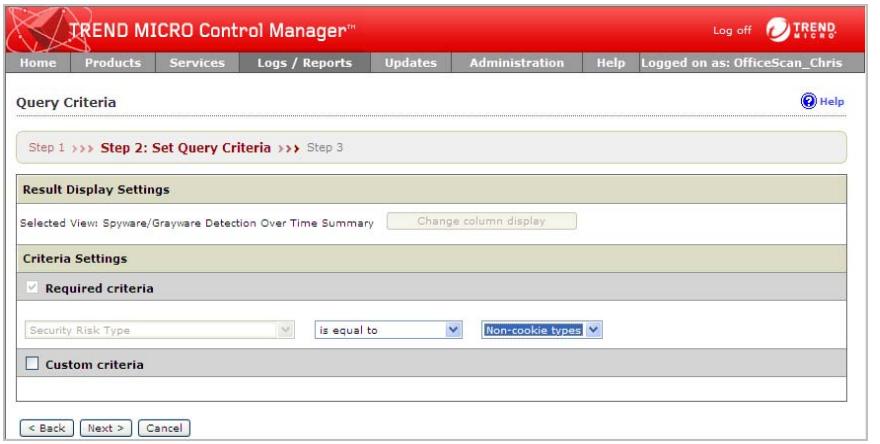
Step 1: Edit the Spyware/Grayware Source Count Grouped by Day line chart:

1. Click **Edit** on the Spyware/Grayware Source Count Grouped by Day line chart. The Edit Line Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

> **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 the analysis of the data that the query returns.

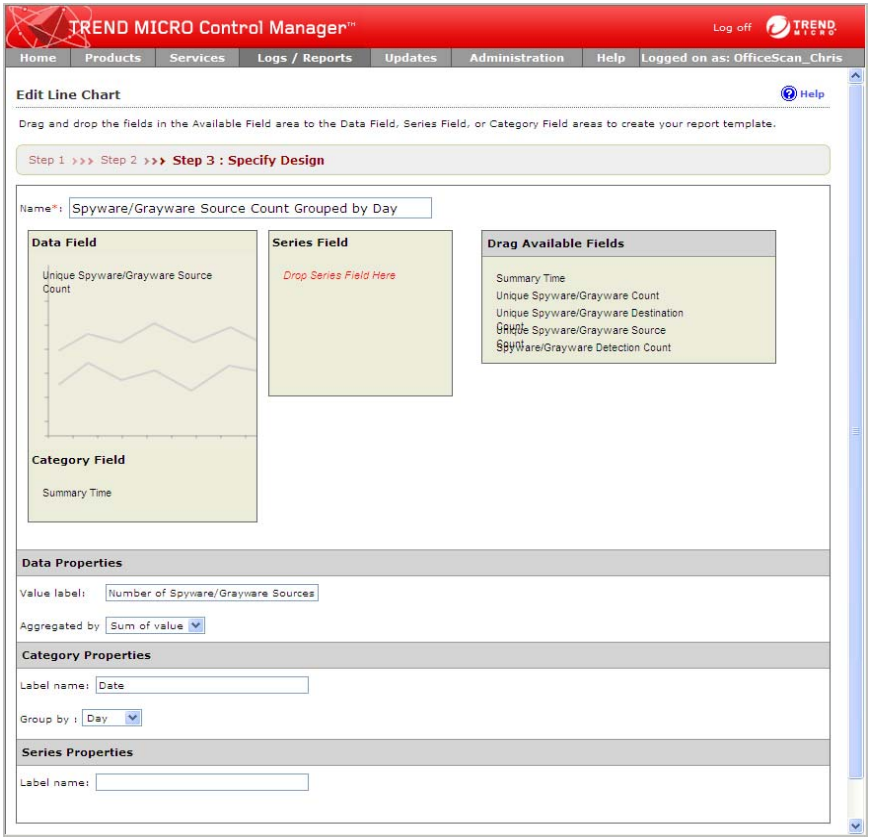
Chris does not want cookies to appear in his line chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

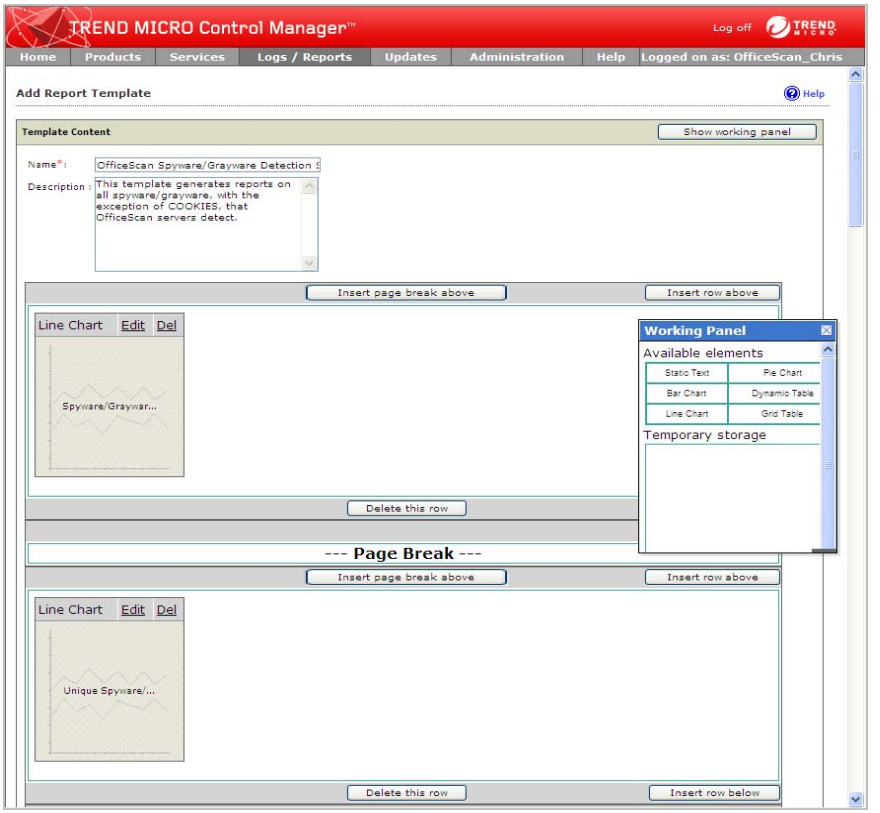
Step 3: Configure settings for the Spyware/Grayware Source Count Grouped by Day line chart settings:

1. Click **Next**. The Edit Line Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Spyware/Grayware Source Count Grouped by Day line chart.

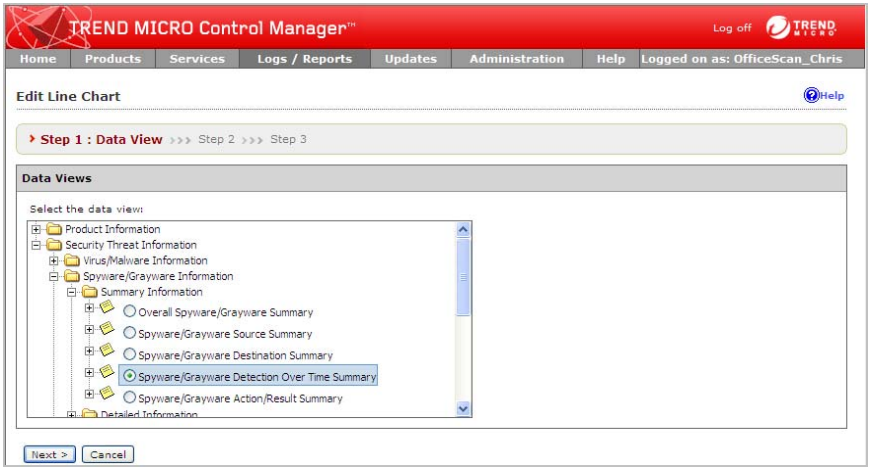
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

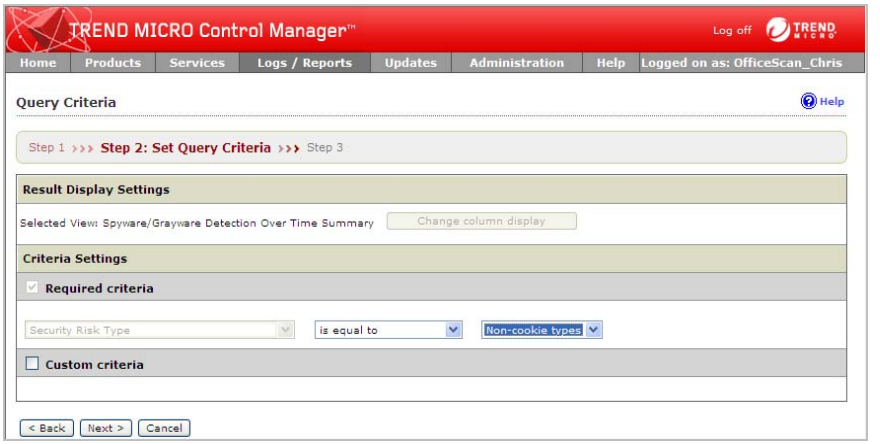
Step 1: Edit the Spyware/Grayware Destination Count Grouped by Day line chart:

1. Click **Edit** on the Spyware/Grayware Destination Count Grouped by Day line chart. The Edit Line Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

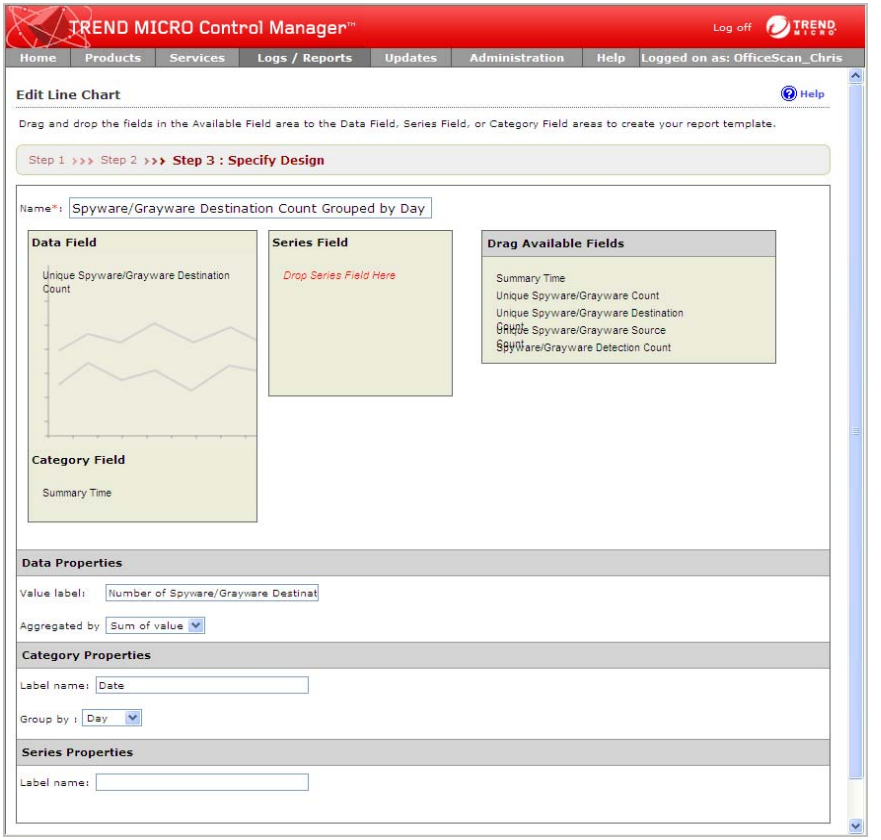
Chris does not want cookies to appear in his line chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

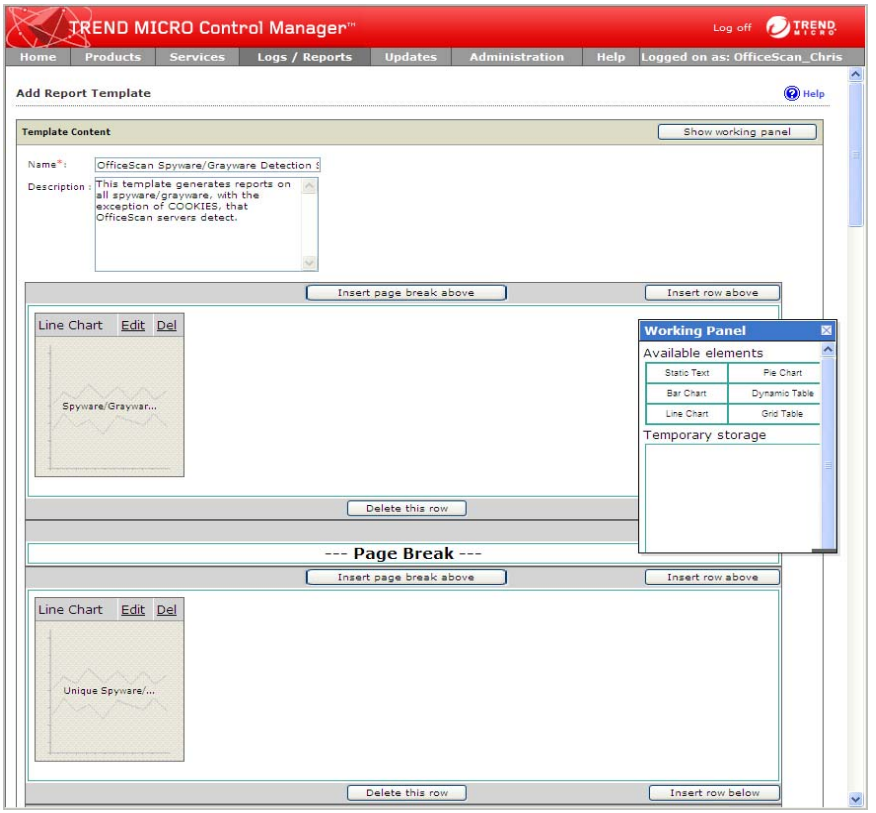
Step 3: Configure settings for the Spyware/Grayware Destination Count Grouped by Day line chart settings:

1. Click **Next**. The Edit Line Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Spyware/Grayware Destination Count Grouped by Day line chart.

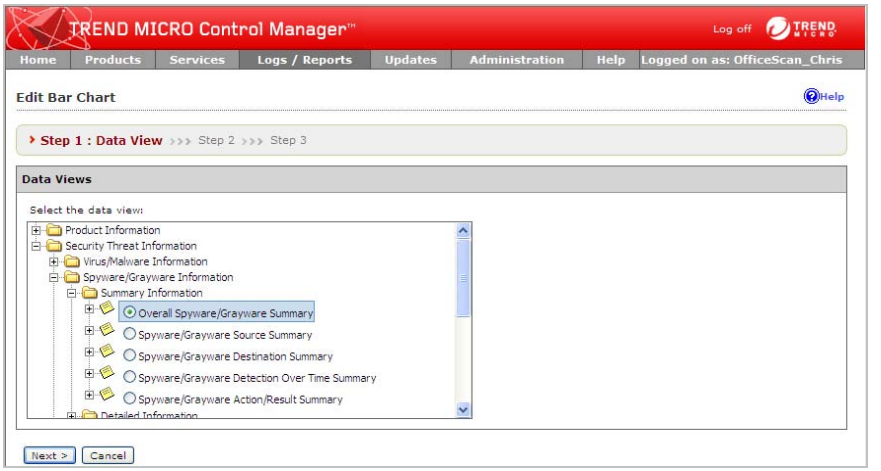
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

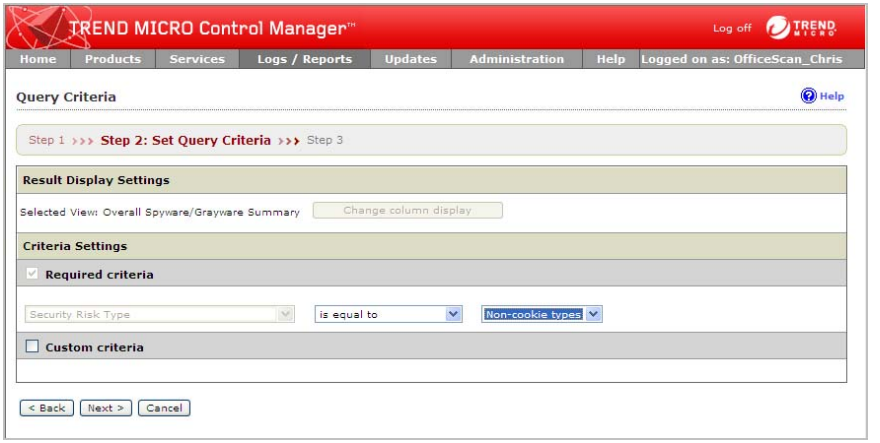
Step 1: Edit the Top 25 Spyware/Grayware bar chart:

1. Click **Edit** on the Top 25 Spyware/Grayware bar chart. The Edit Bar Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

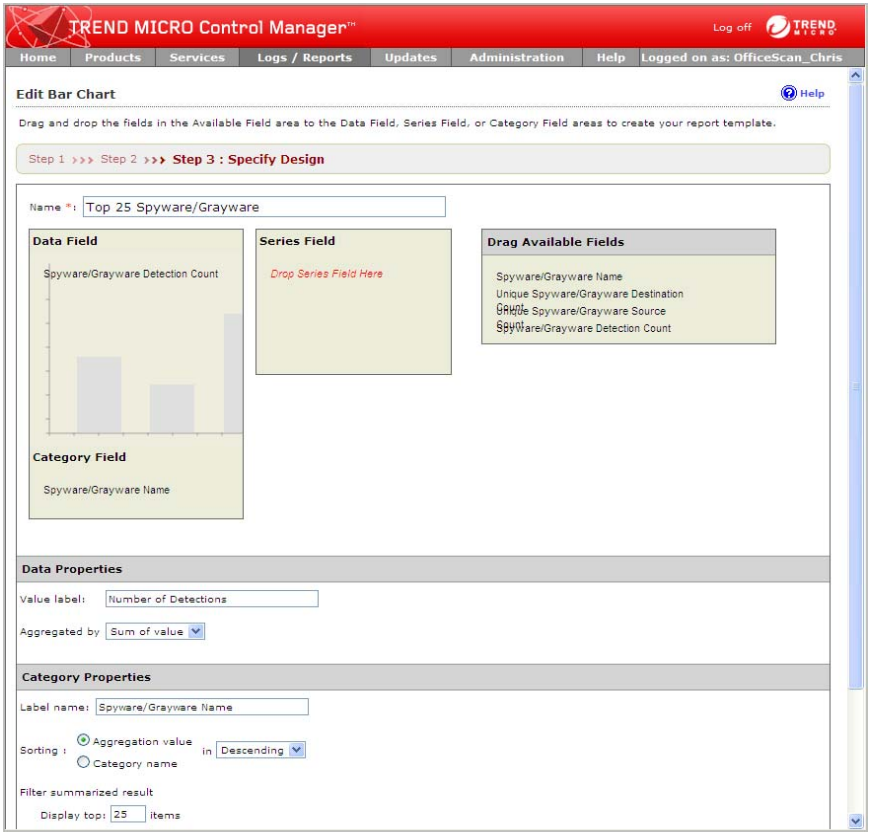
Chris does not want cookies to appear in his bar chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

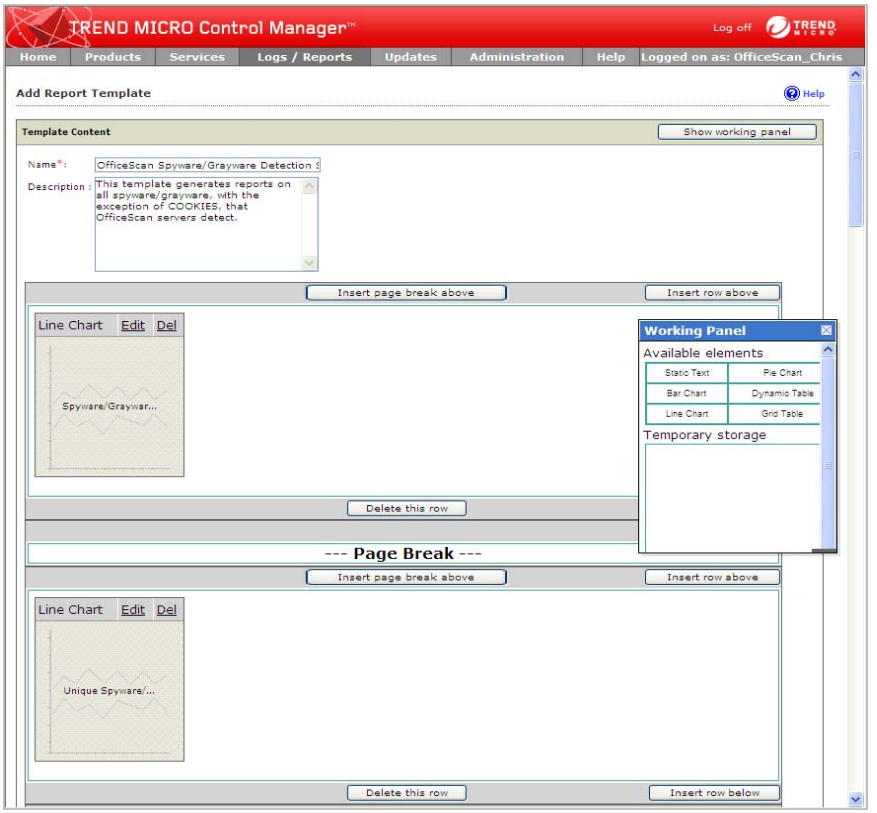
Step 3: Configure bar chart settings:

1. Click **Next**. The Edit Bar Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Top 25 Spyware/Grayware bar chart.

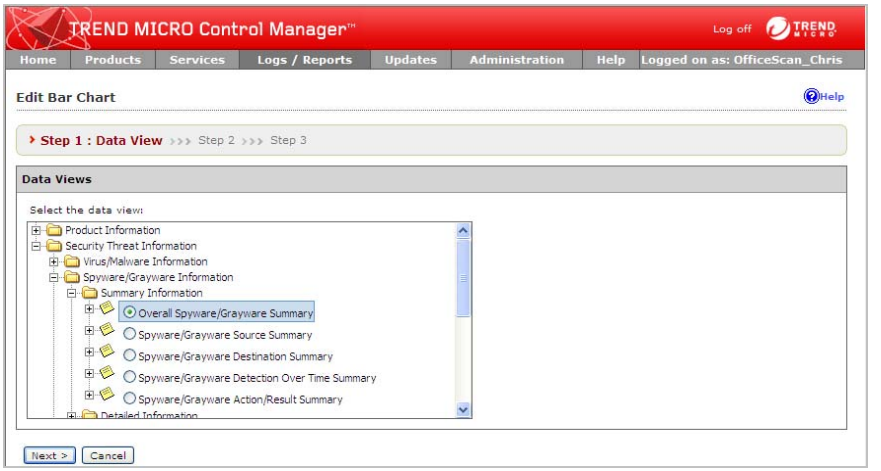
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

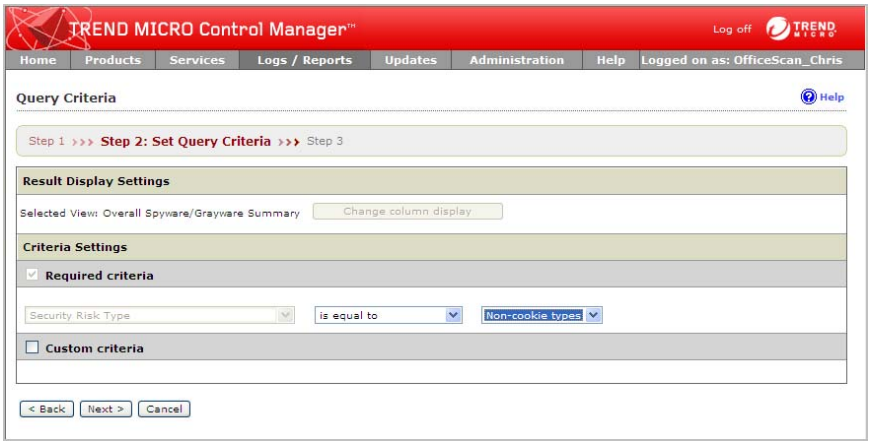
Step 1: Edit the Overall Spyware/Grayware Summary grid table:

1. Click **Edit** on the Overall Spyware/Grayware Summary grid table. The Edit Grid Table screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

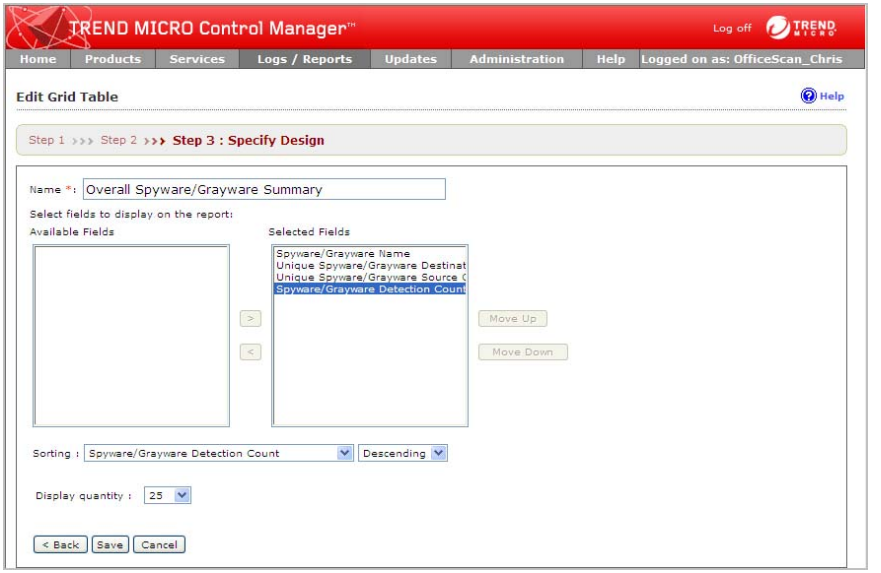
Chris does not want cookies to appear in his grid table for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

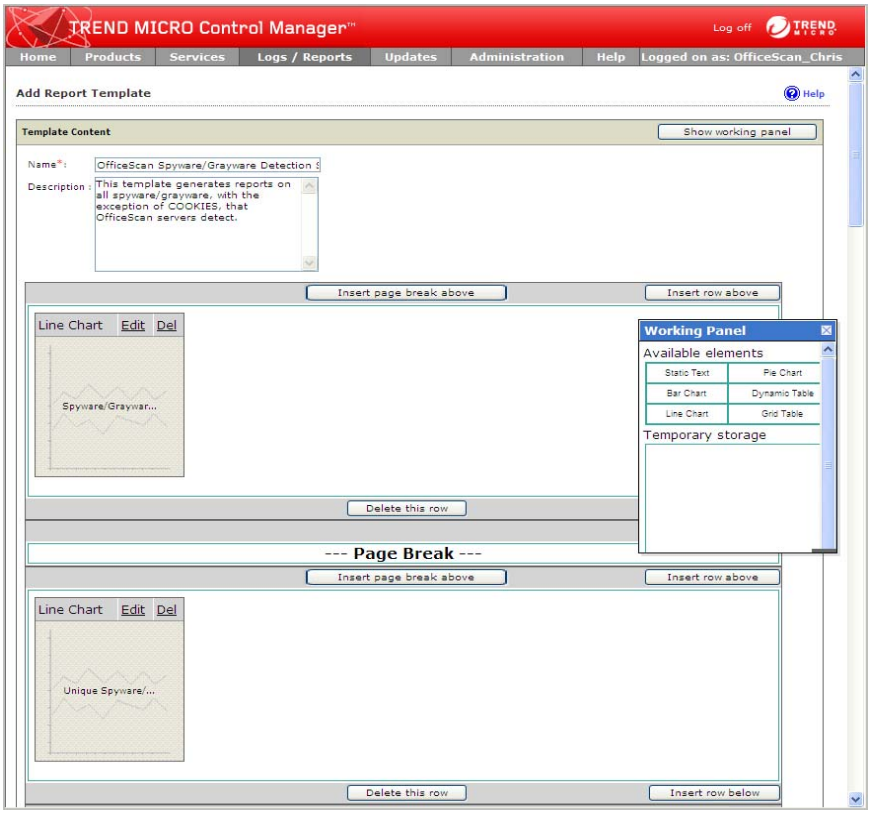
Step 3: Configure Overall Spyware/Grayware Summary grid table settings:

1. Click **Next**. The Edit Grid Table > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Overall Spyware/Grayware Summary grid table.

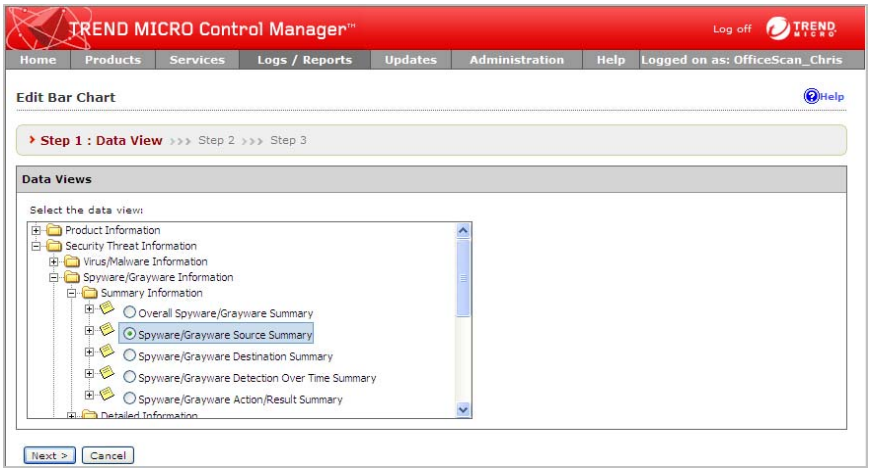
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

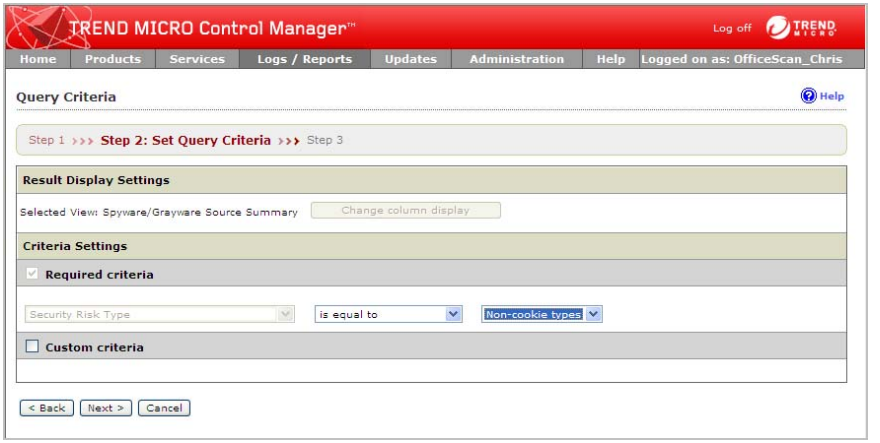
Step 1: Edit the Top 25 Spyware/Grayware Sources bar chart:

1. Click **Edit** on the Top 25 Spyware/Grayware Sources bar chart. The Edit Bar Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

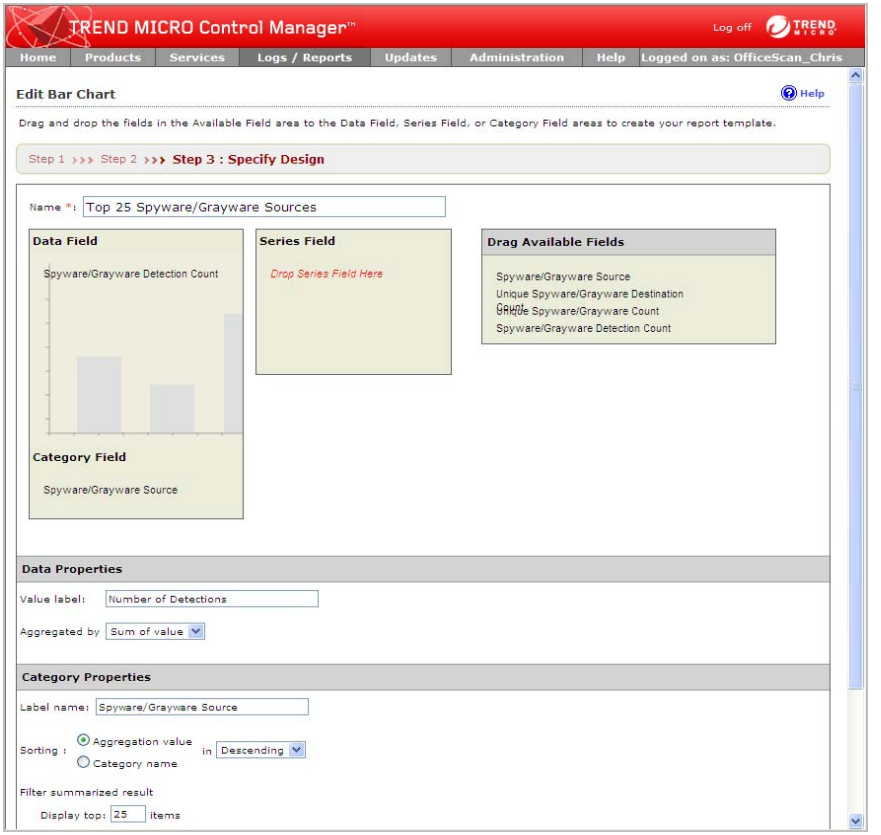
Chris does not want cookies to appear in his bar chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

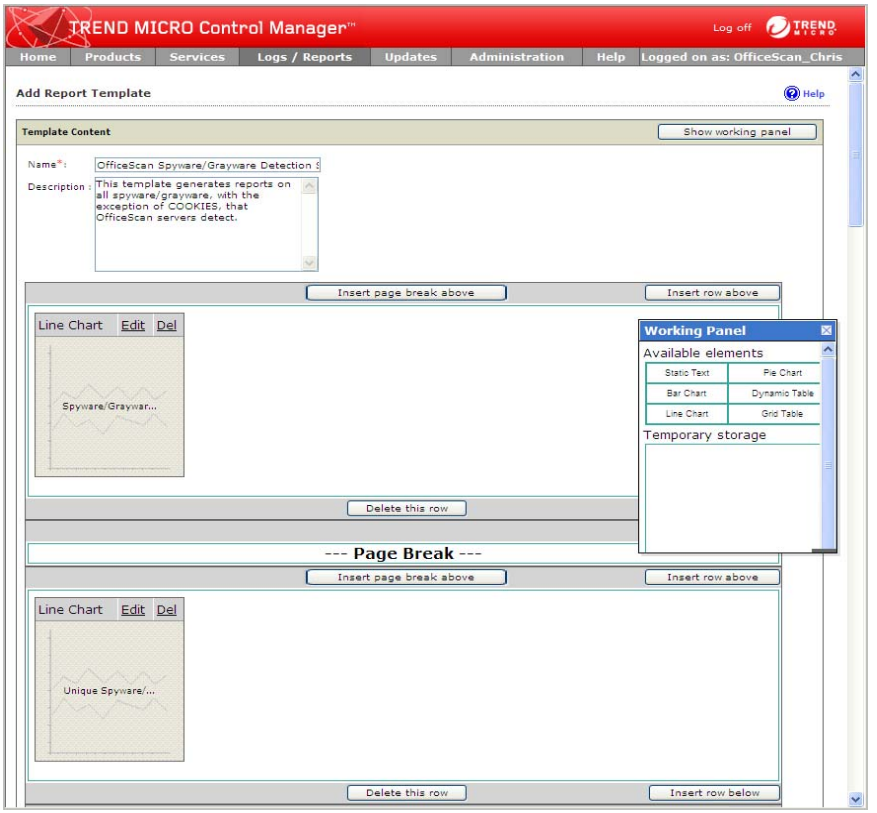
Step 3: Configure bar chart settings:

1. Click **Next**. The Edit Bar Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Top 25 Spyware/Grayware Sources bar chart.

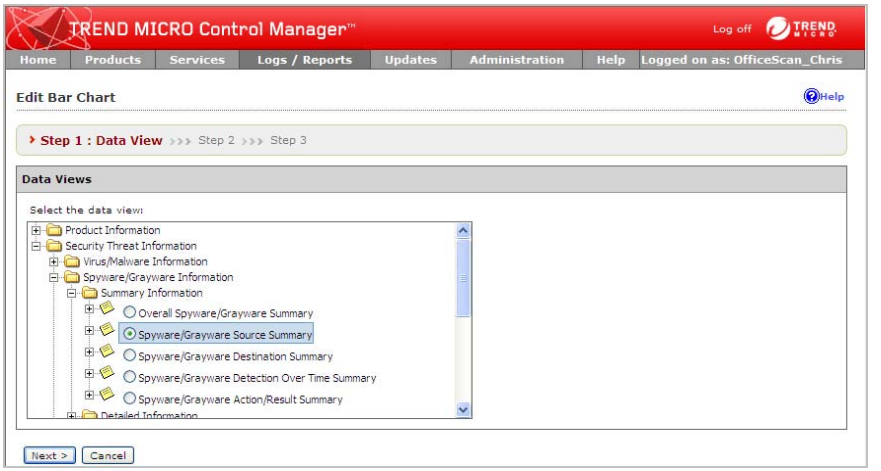
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

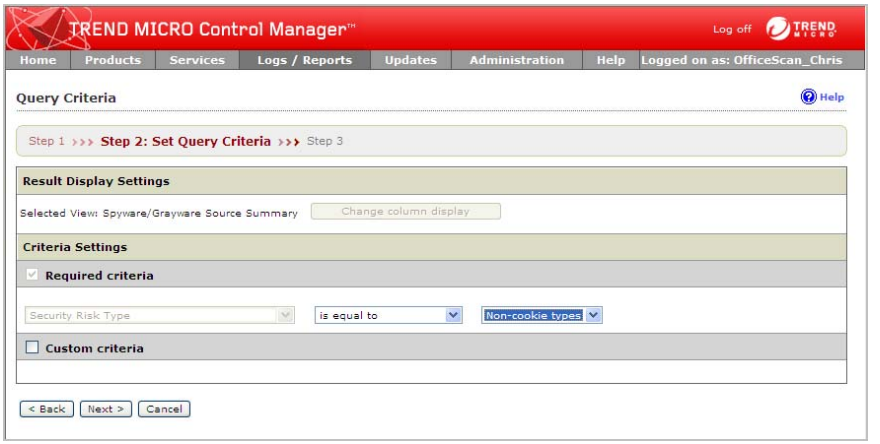
Step 1: Edit the Spyware/Grayware Source Summary grid table:

1. Click **Edit** on the Spyware/Grayware Source Summary grid table. The Edit Grid Table screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

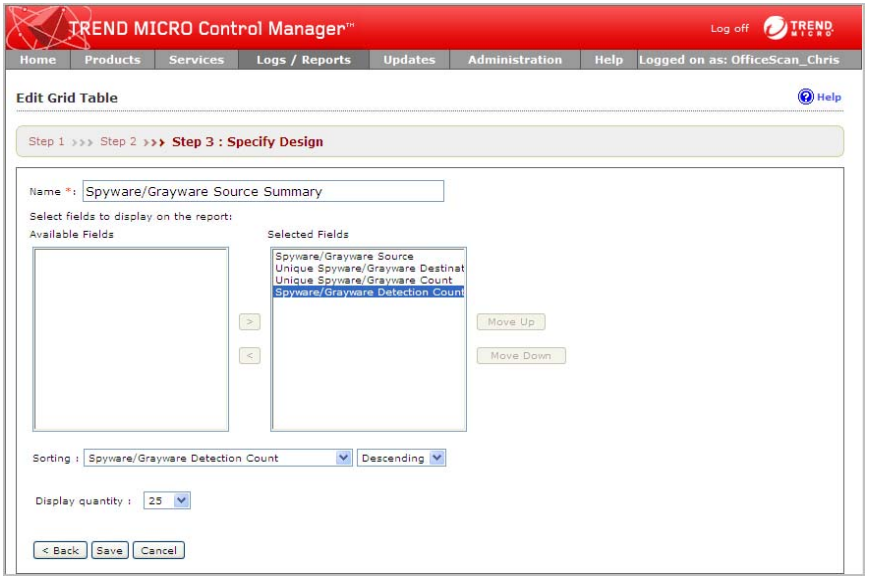
Chris does not want cookies to appear in his grid table for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

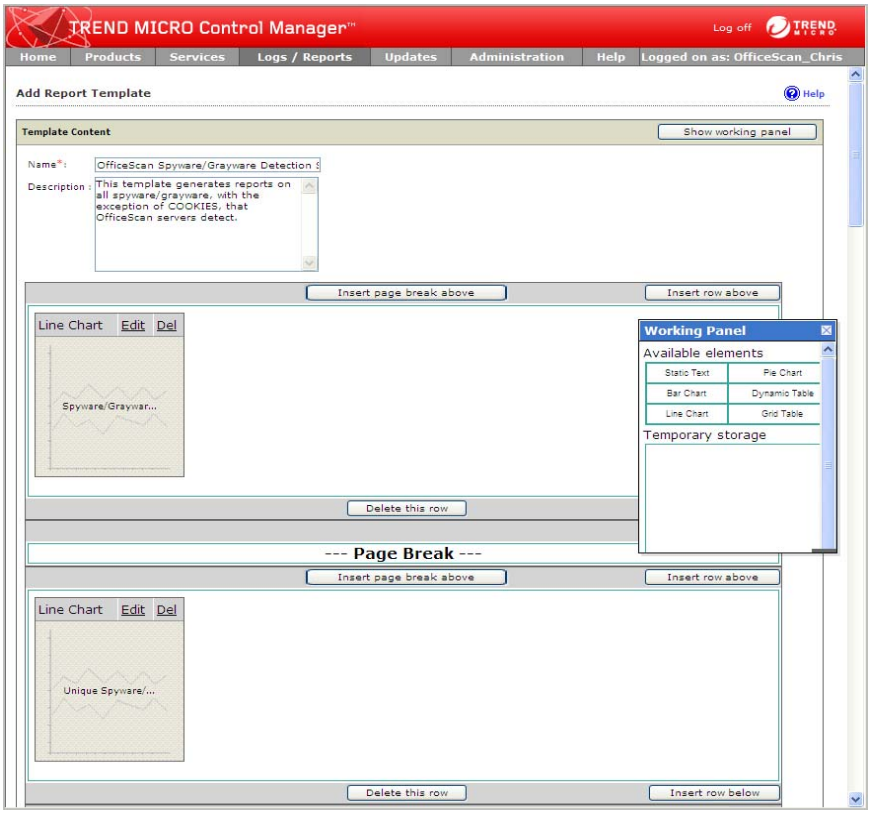
Step 3: Configure Spyware/Grayware Source Summary grid table settings:

1. Click **Next**. The Edit Grid Table > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Spyware/Grayware Source Summary grid table.

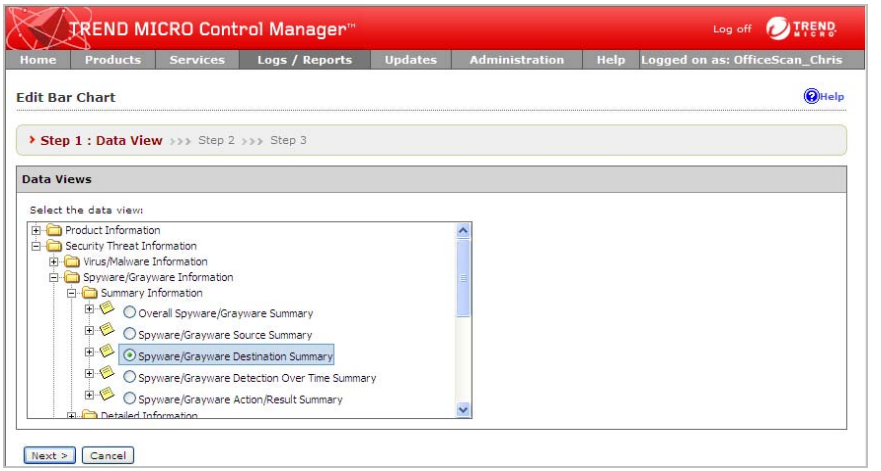
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

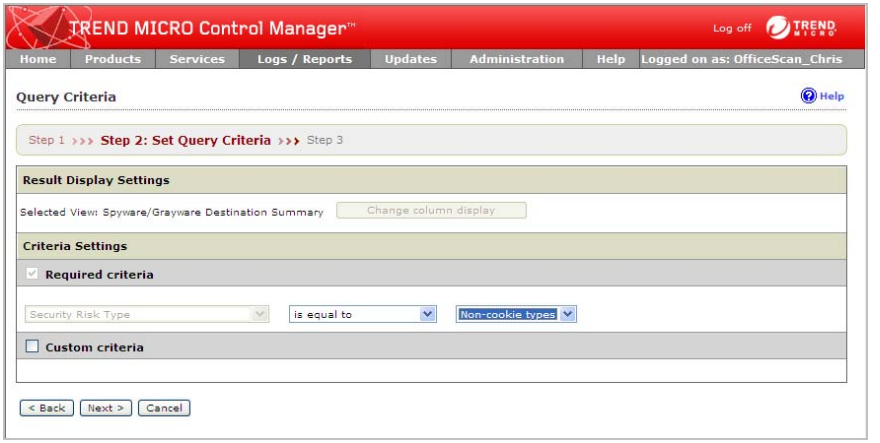
Step 1: Edit the Top 25 Spyware/Grayware Destinations bar chart:

1. Click **Edit** on the Top 25 Spyware/Grayware Destinations bar chart. The Edit Bar Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

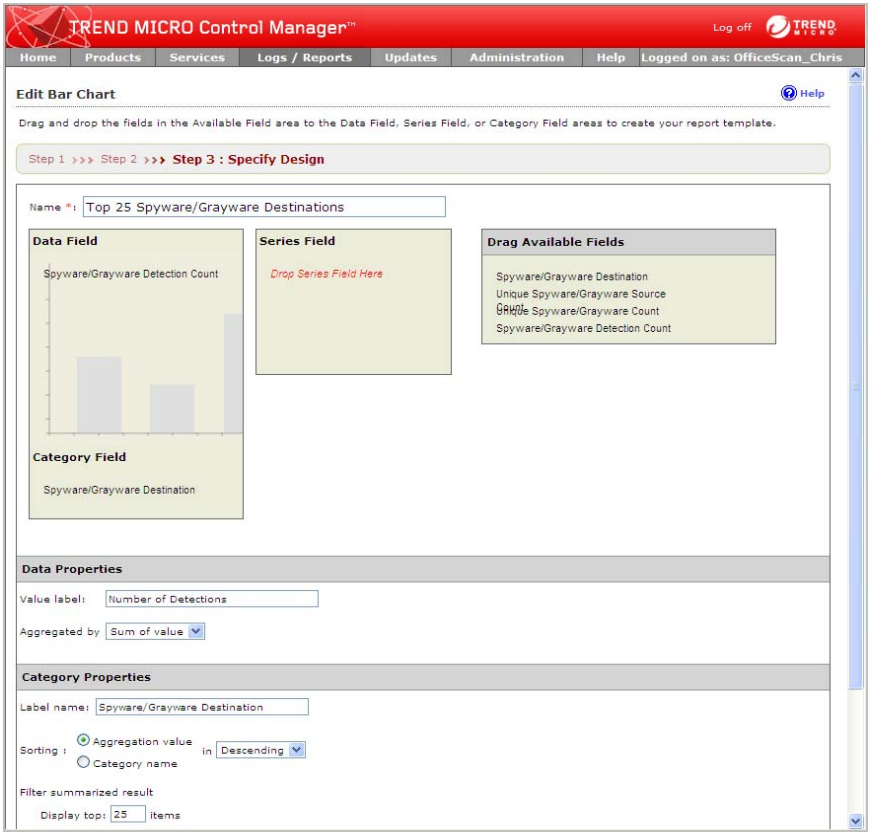
Chris does not want cookies to appear in his bar chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

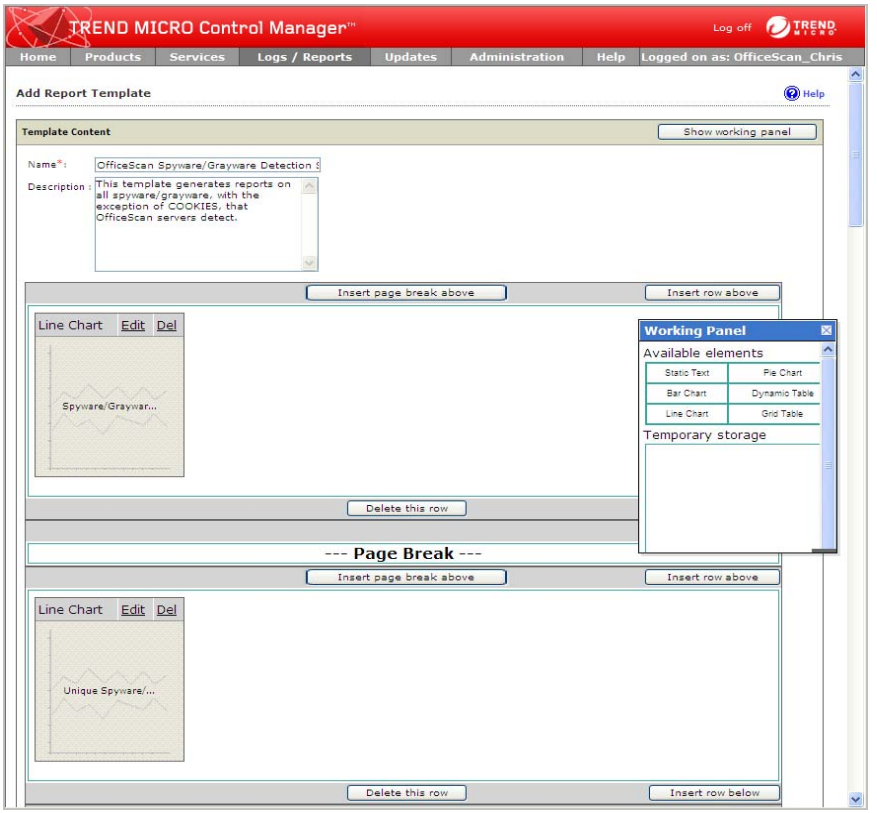
Step 3: Configure bar chart settings:

1. Click **Next**. The Edit Bar Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Top 25 Spyware/Grayware Destinations bar chart.

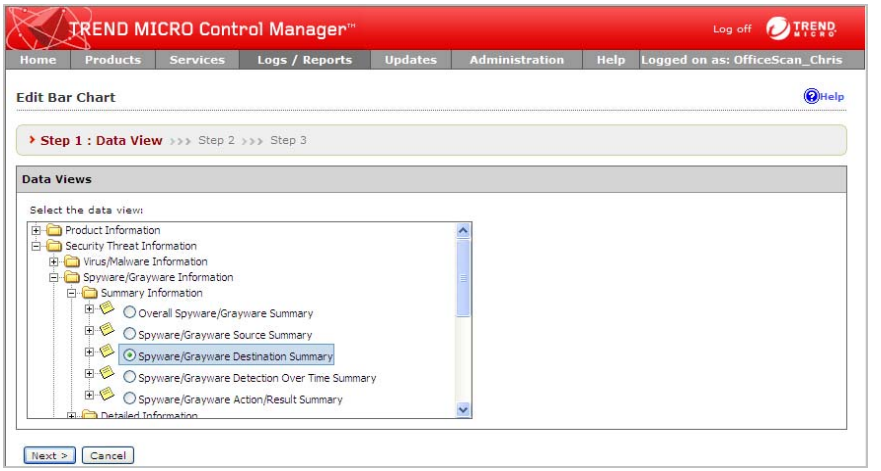
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

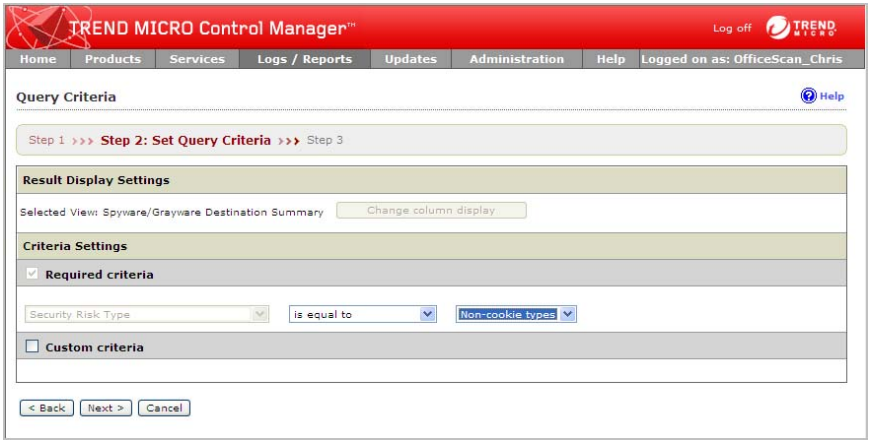
Step 1: Edit the Spyware/Grayware Destination Summary grid table:

1. Click **Edit** on the Spyware/Grayware Destination Summary grid table. The Edit Grid Table screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

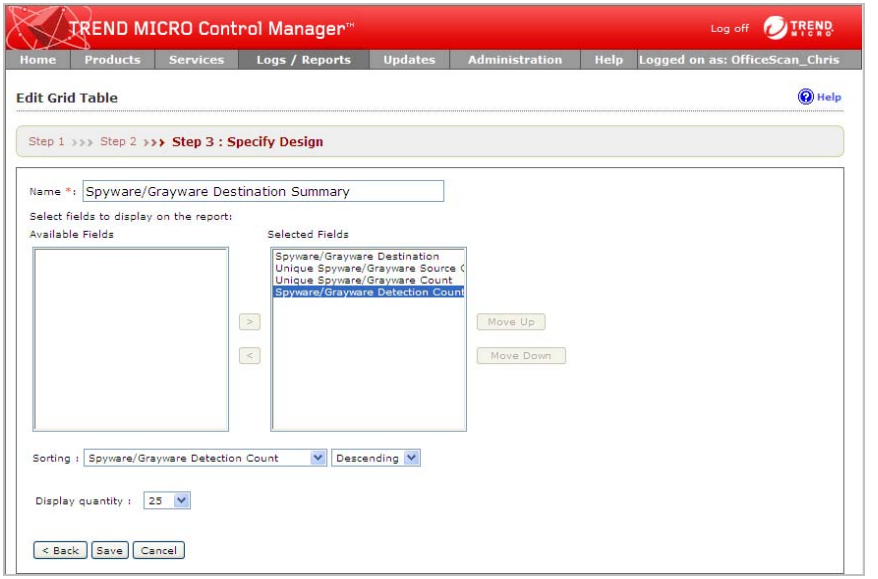
Chris does not want cookies to appear in his grid table for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

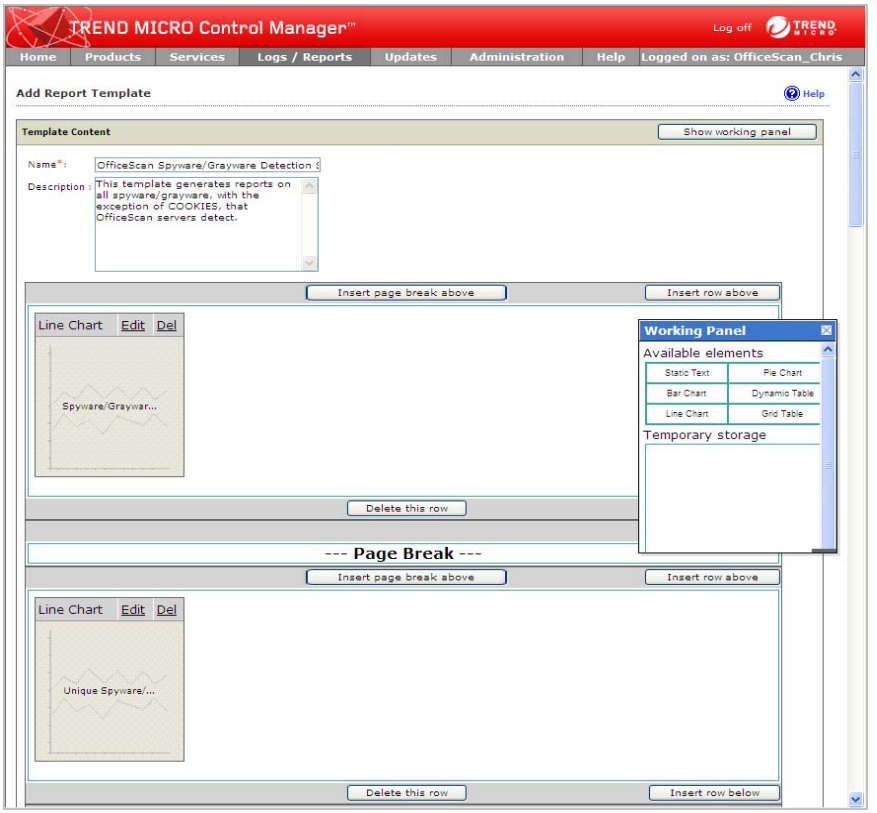
Step 3: Configure Spyware/Grayware Destination Summary grid table settings:

1. Click **Next**. The Edit Grid Table > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Spyware/Grayware Destination Summary grid table.

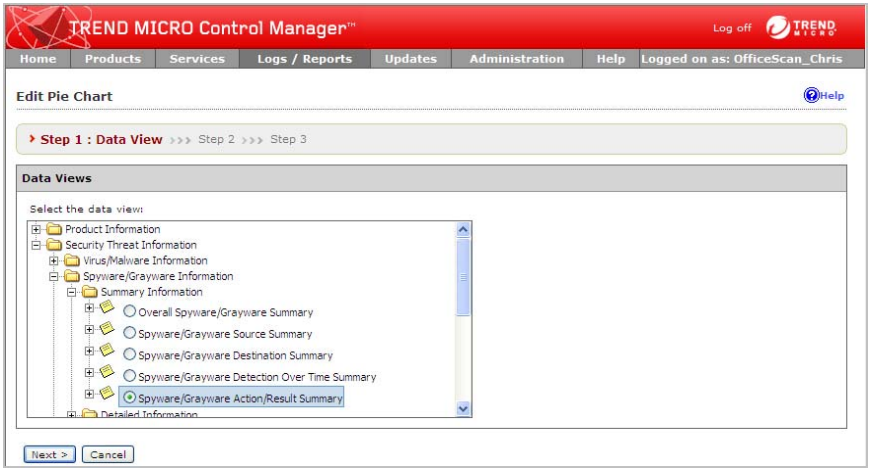
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

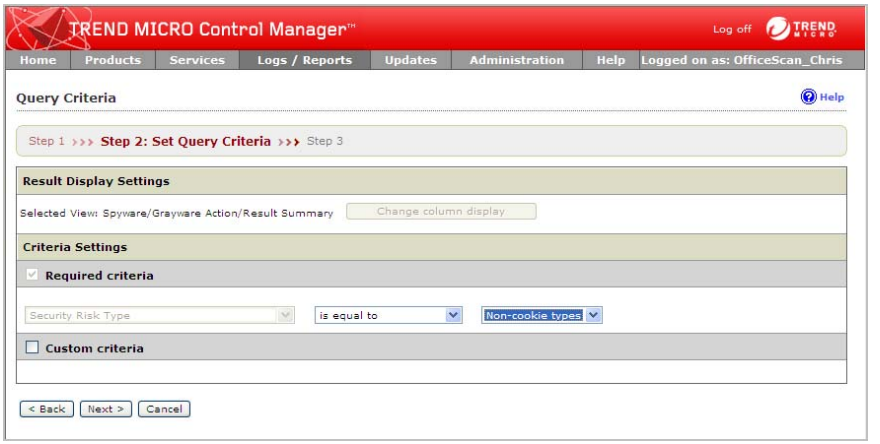
Step 1: Edit the Action Result Summary pie chart:

1. Click **Edit** on the Action Result Summary pie chart. The Edit Pie Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

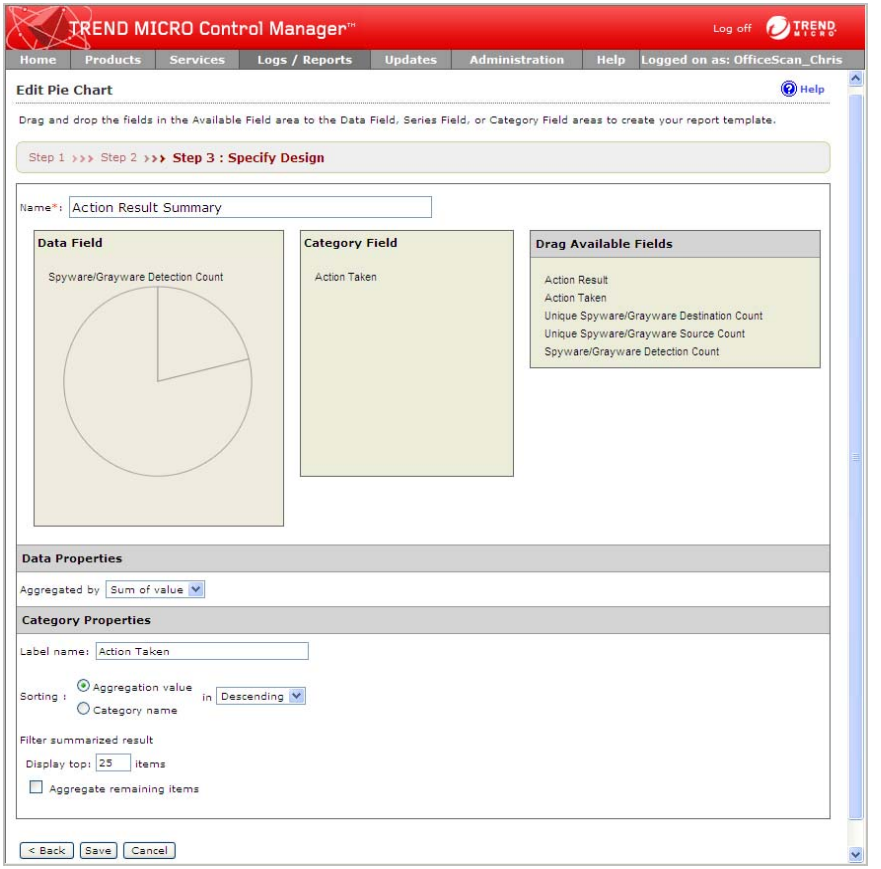
Chris does not want cookies to appear in his pie chart for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

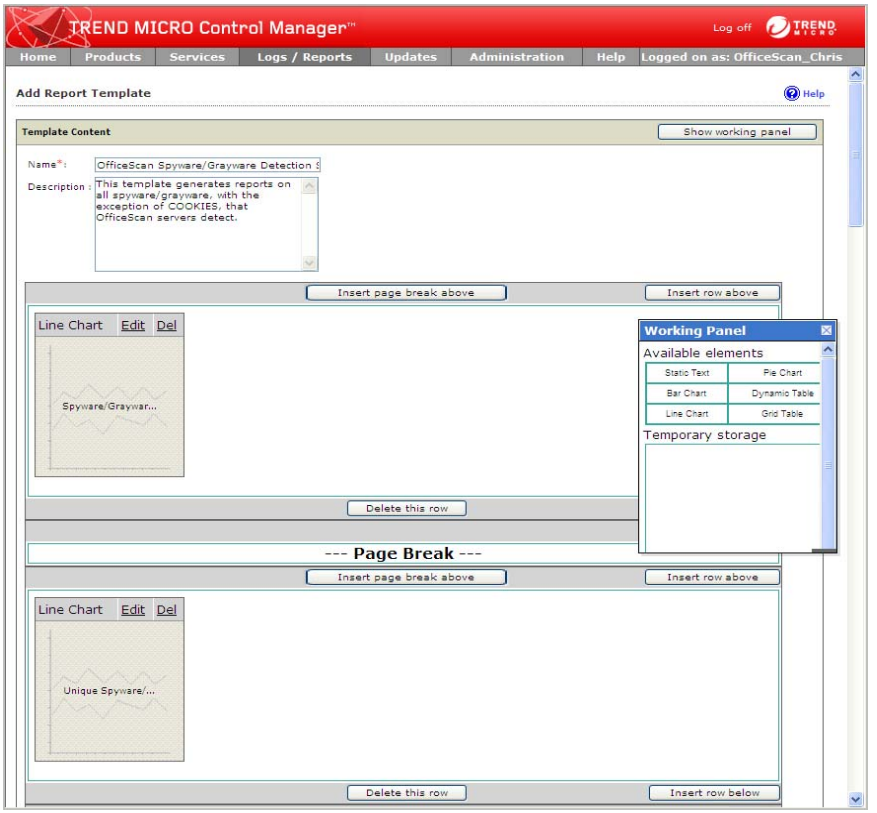
Step 3: Configure pie chart settings:

1. Click **Next**. The Edit Pie Chart > Step 3 Specify Design screen appears.



Chris does not want to modify any of the settings for the Action Result Summary pie chart.

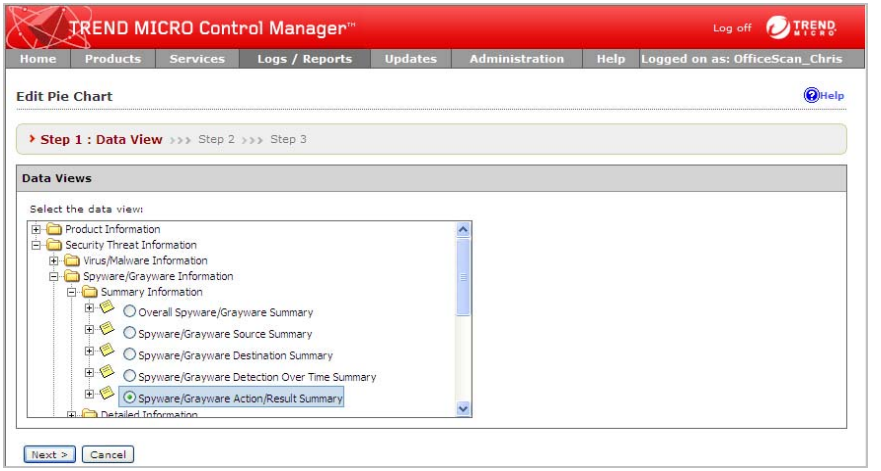
2. Click **Save**. The Add Report Template screen appears.



Edit the Report Template Element

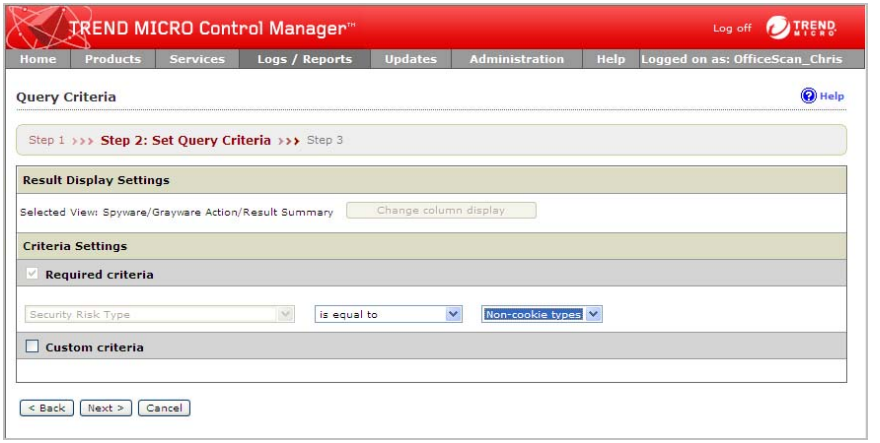
Step 1: Edit the Spyware/Grayware Action/Result Summary grid table:

1. Click **Edit** on the Spyware/Grayware Action/Result Summary grid table. The Edit Grid Table screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

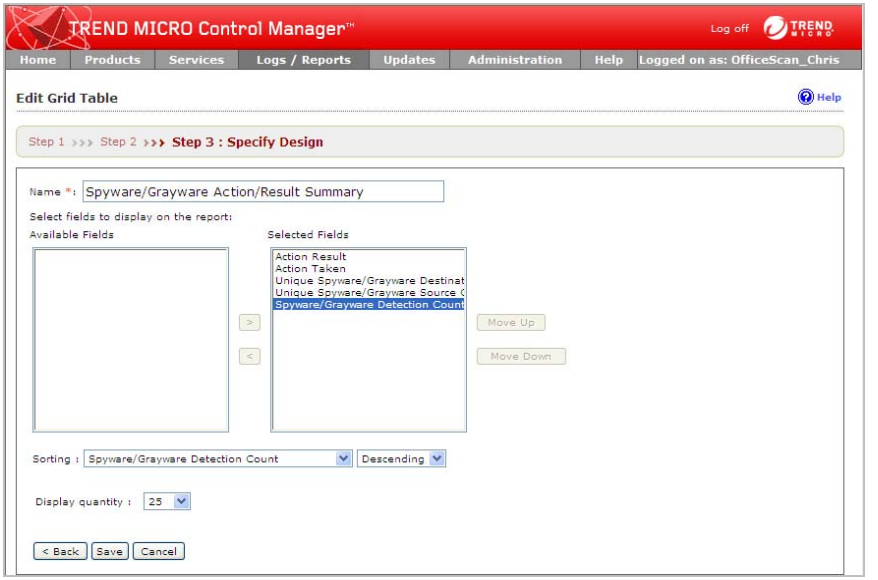
Chris does not want cookies to appear in his grid table for spyware/grayware.

1. Specify the following for **Required criteria**:

   Security Risk Type > is equal to > Non-cookie types

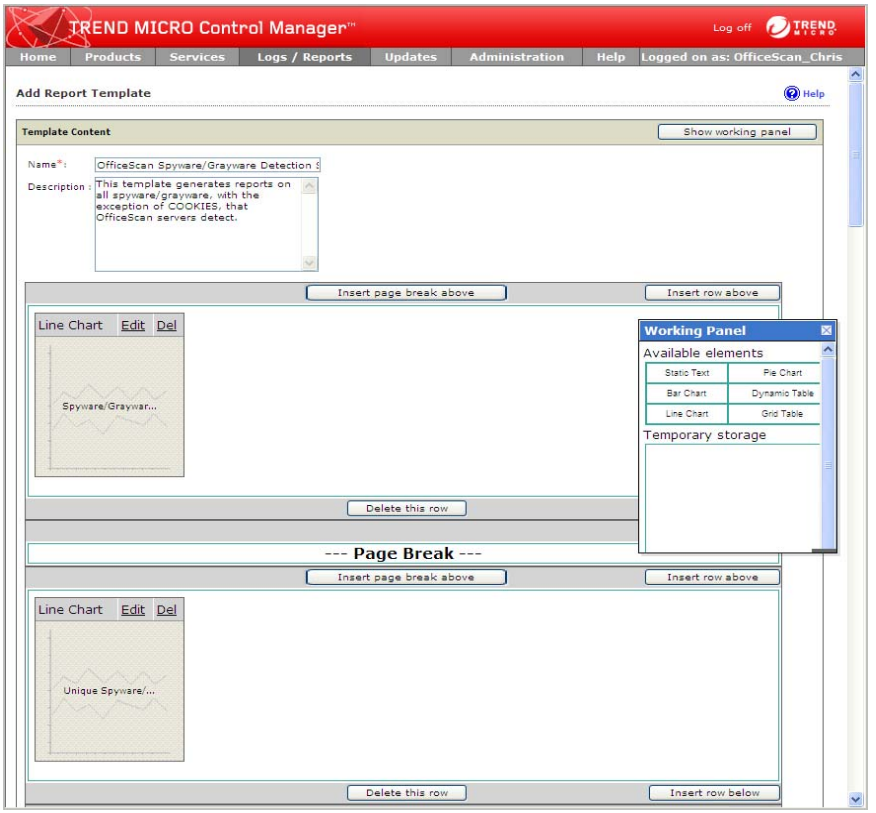
Step 3: Configure Spyware/Grayware Action/Result Summary grid table settings:

1. Click **Next**. The Edit Grid Table > Step 3 Specify Design screen appears.

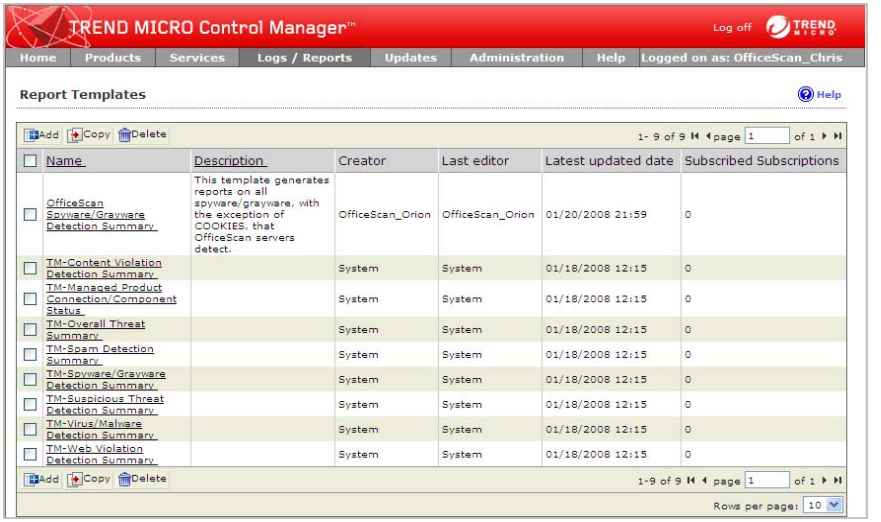


Chris does not want to modify any of the settings for the Spyware/Grayware Action/Result Summary grid table.

2. Click **Save**. The Add Report Template screen appears.



3. Click **Save**. The Report Templates screen appears with the modified template appearing at the top of the Report Template list.



Viewing a Generated Report Using the Template

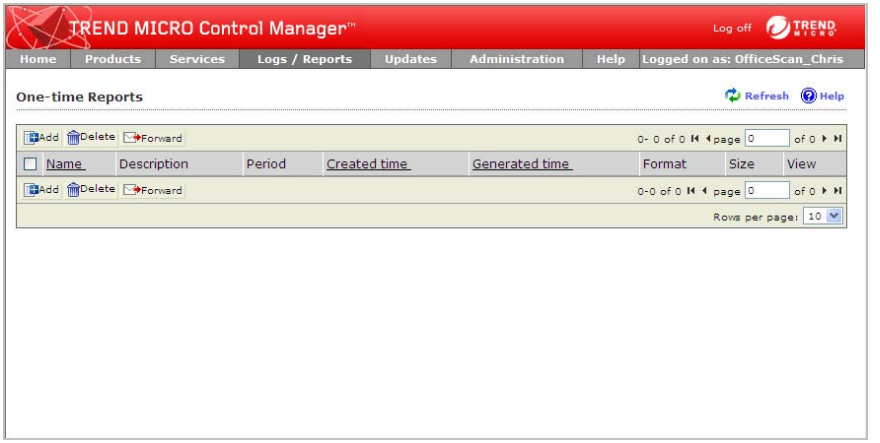
After modifying the template, Chris wants to see how the report would look. To quickly view a report using this template Chris needs to create a one-time report. Chris would also like to gather feedback from other OfficeScan administrators and his boss on the layout of the report. He will email the report, when the report completes generation, to his boss and the other OfficeScan administrators.

To add a one-time report:

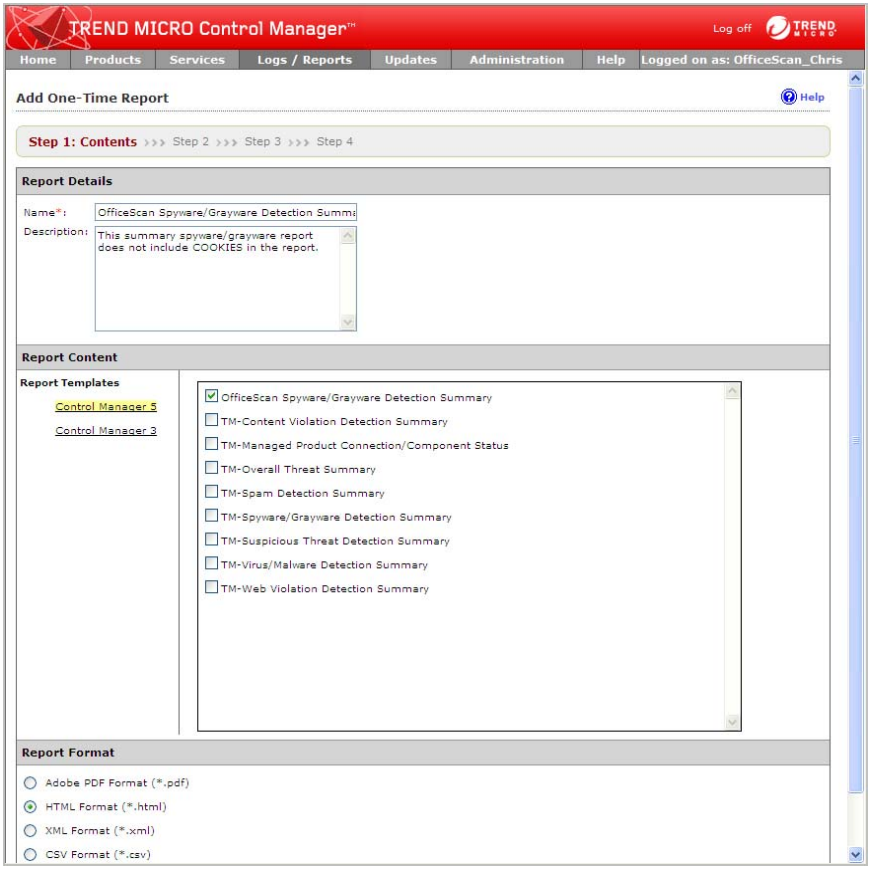
Step 1: Access the Add One-time Report screen and select the report type:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.

3. Click **One-time Reports** from the menu. The One-time Reports screen appears.



4. Click **Add**. The Add One-time Report > Step 1: Contents screen appears.



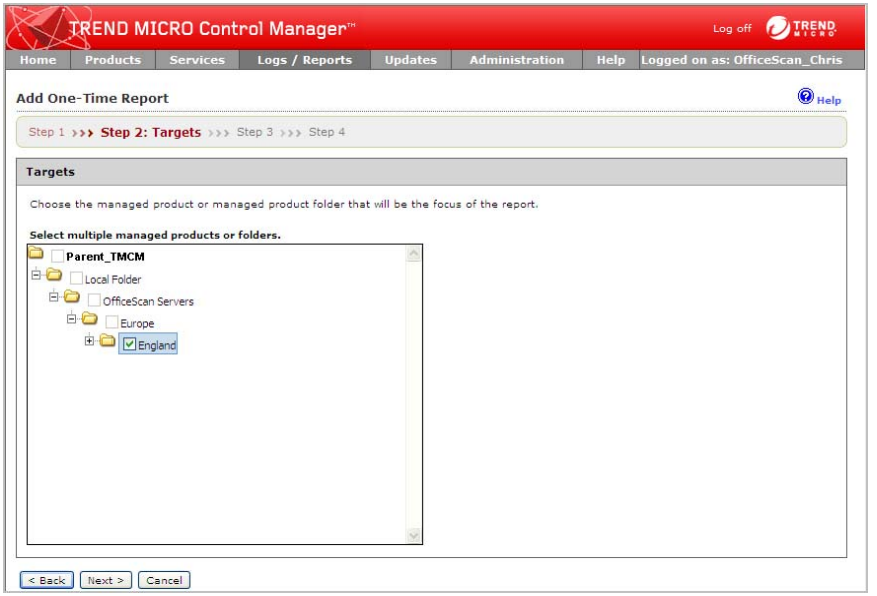
5. Type the following in the **Name** field, under Report Details:

   OfficeScan Spyware/Grayware Detection Summary

6. Type the following in the **Description** field, under Report Details:

   This summary spyware/grayware report does not include COOKIES in the report.

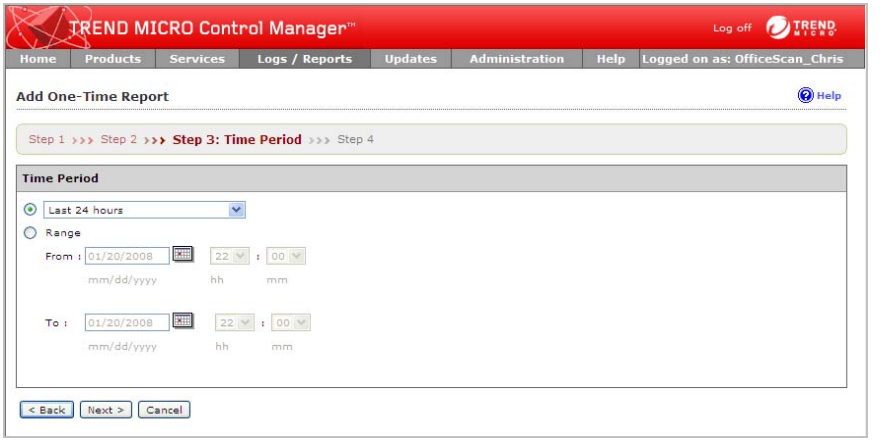
7. Select the **OfficeScan Spyware/Grayware Detection Summary** Control Manager template to generate the report:
8. Select **HTML Format (*.html)** for the report generation format:
9. Click **Next**. The Add One-Time Report > Step 2: Targets screen appears.



Step 2: Specify the product/products from which the report data generates:

1. Select **England** from the Product Directory.

2. Click **Next**. The Add One-Time Report > Step 3: Time Period screen appears.



Step 3: Specify the date that the product/products produced the data:

1. Specify the data generation date:

   From the drop-down list select one of the following:

   - All dates
   - Last 24 hours
   - Today
   - Last 7 days
   - Last 14 days
   - Last 30 days

   Specify a date range:

   a. Type a date in the **From** field.

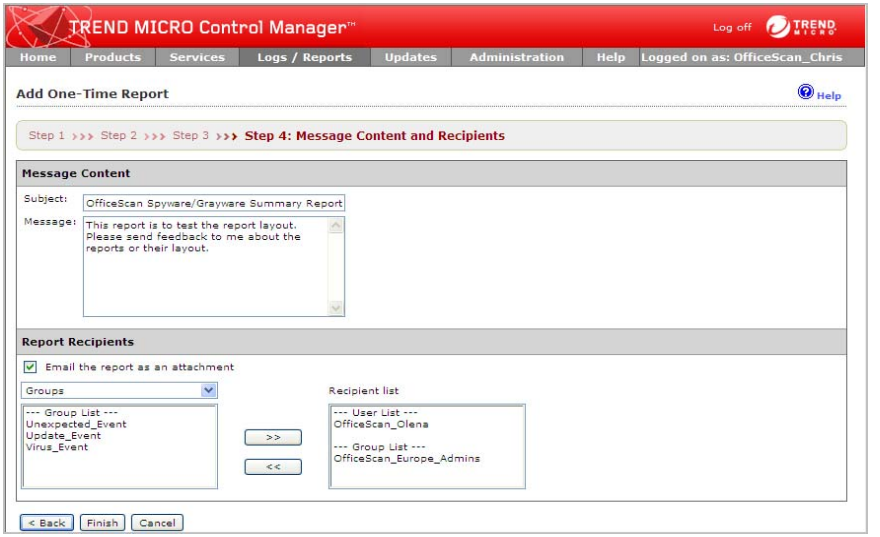
   b. Specify a time in the accompanying **hh** and **mm** fields.

   c. Type a date in the **To** field.

   d. Specify a time in the accompanying **hh** and **mm** fields.

Tip: Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**. The Add One-time Report > Step 4: Message Content and Recipients screen appears.



Step 4: Specify the email content and recipients of the report:

1. Type the following in the **Message** field:

   OfficeScan Spyware/Grayware Summary Report Test

2. Type the following in the **Message** field:

   This report is to test the report layout. Please send feedback to me about the reports or their layout.

3. Select **Email the report as an attachment**.

4. Add the following users to the **Report Recipients** list:

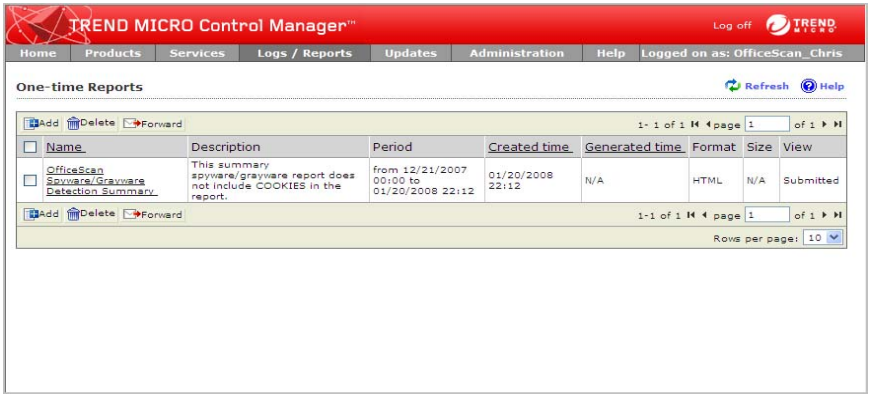
   Groups:

   - **OfficeScan_Europe_Admins**

Users:

- **OfficeScan_Dana**

5. Click **Finish**. The One-time Reports screen appears with the report in the One-time Reports list.



After report generation completes successfully **View** appears under the View column.

6. Click **View.** The Internet browser on your computer opens to display the HTML report.

TREND MICRO™
Control Manager™ 5

Consolidated Report

Period : 4/1/2007 12:00:00 AM - 12/19/2007 11:45:00 PM

Issuer : OfficeScan_Orion

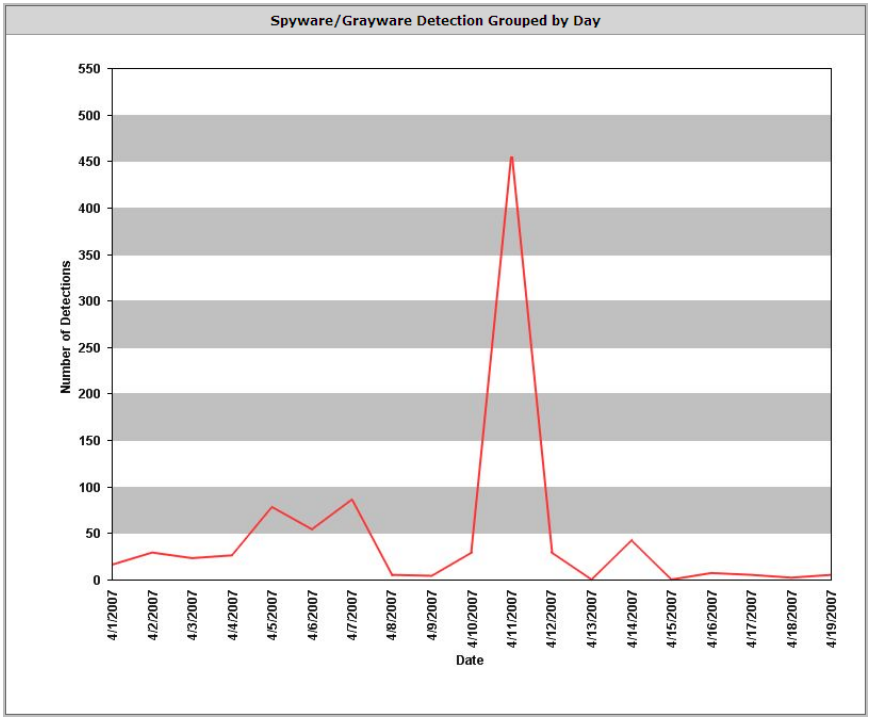
OfficeScan Spyware/Grayware Summary Report

List of templates:

1. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Detection Grouped by Day
2. OfficeScan Spyware/Grayware Detection Summary - Unique Spyware/Grayware Count Grouped by Day
3. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Source Count Grouped by Day
4. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Destination Count Grouped by Day
5. OfficeScan Spyware/Grayware Detection Summary - Top 25 Spyware/Grayware
6. OfficeScan Spyware/Grayware Detection Summary - Overall Spyware/Grayware Summary
7. OfficeScan Spyware/Grayware Detection Summary - Top 25 Spyware/Grayware Sources
8. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Source Summary
9. OfficeScan Spyware/Grayware Detection Summary - Top 25 Spyware/Grayware Destinations
10. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Destination Summary
11. OfficeScan Spyware/Grayware Detection Summary - Action Result Summary
12. OfficeScan Spyware/Grayware Detection Summary - Spyware/Grayware Action/Result Summary

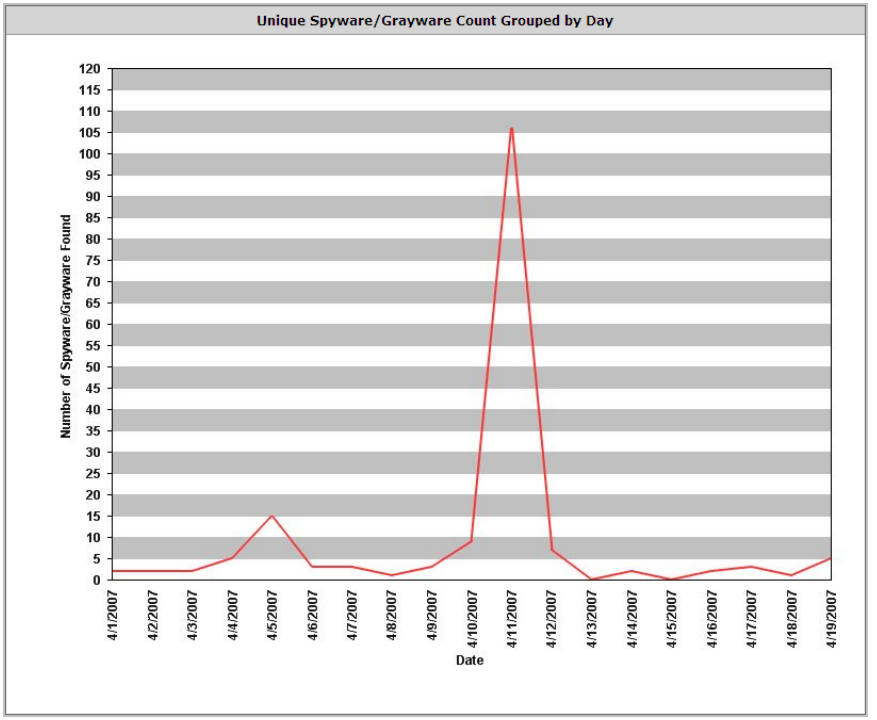
Each of the following figures corresponds to one of the report template elements. The settings for each template element are provided so you will have a better idea about how reports generate.

TABLE 4-7. Spyware/Grayware Detection Grouped by Day Line Chart



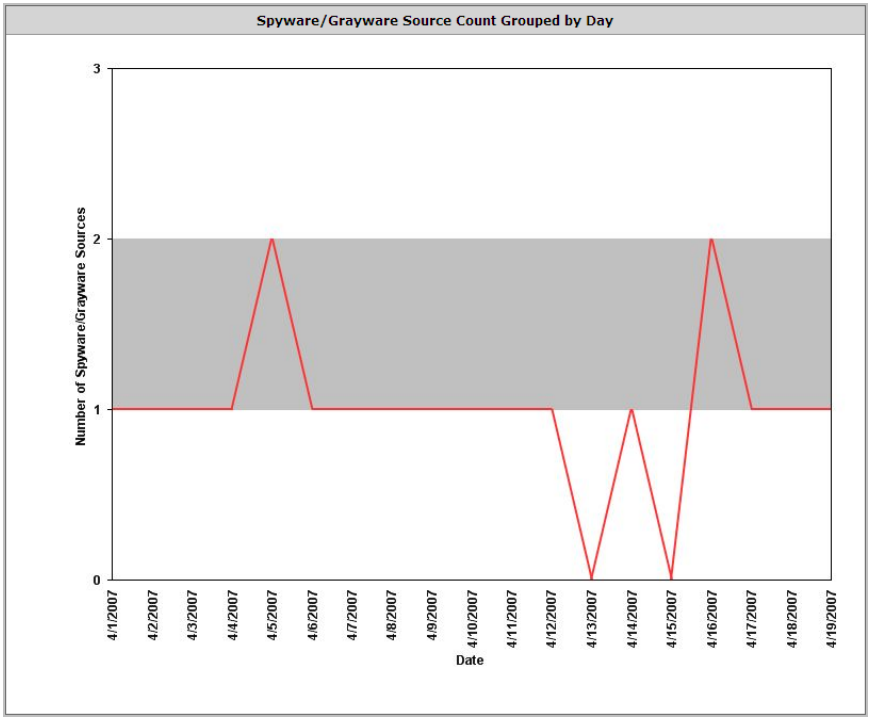
Data view: • Spyware/Grayware Detection Over Time Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Detection Count • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date • Group by: Day

TABLE 4-8. Unique Spyware/Grayware Count Grouped by Day Line Chart



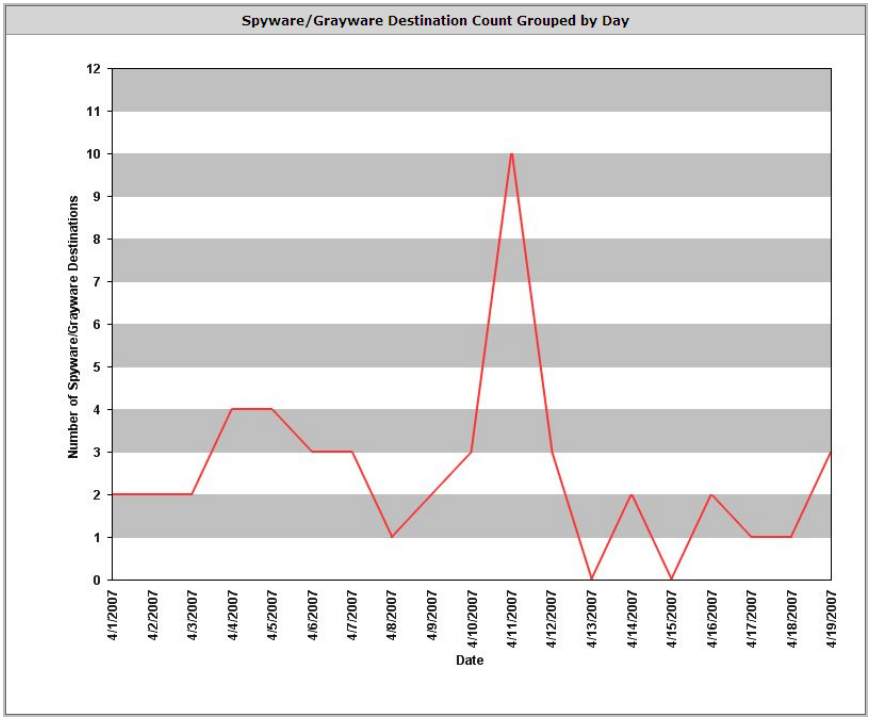
Data view: • **Spyware/Grayware Detection Over Time Summary** Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Unique Spyware/Grayware Count • Value label: Number of Spyware/Grayware Found • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date • Group by: Day

TABLE 4-9. Spyware/Grayware Source Count Grouped by Day Line Chart



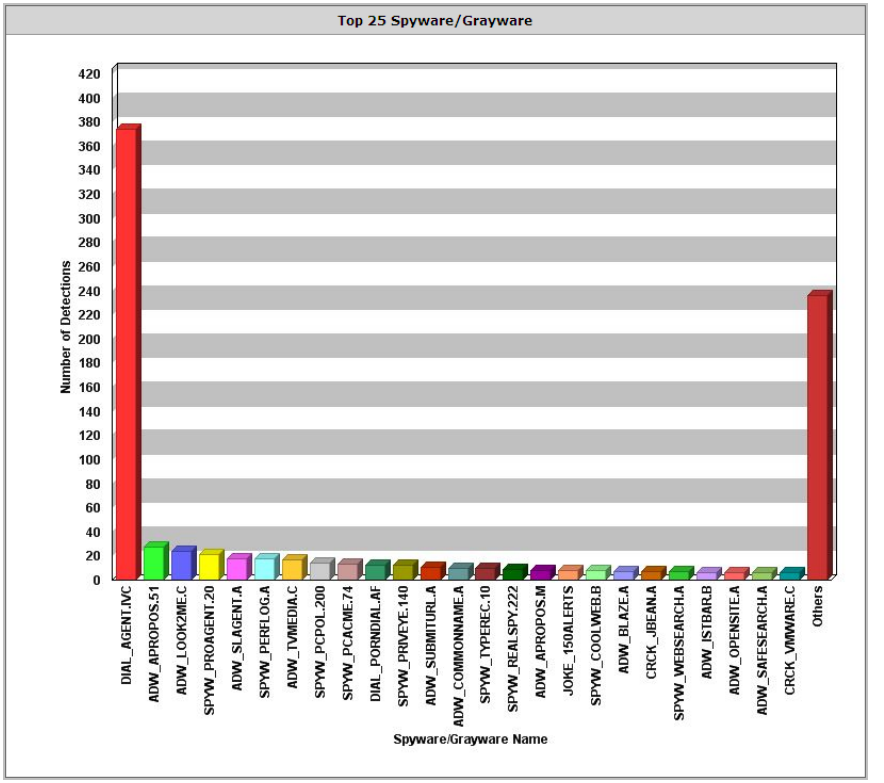
Data view: • Spyware/Grayware Detection Over Time Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Source Count • Value label: Number of Spyware/Grayware Sources • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date • Group by: Day

TABLE 4-10. Spyware/Grayware Destination Count Grouped by Day Line Chart



Data view: • Spyware/Grayware Detection Over Time Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Destination Count • Value label: Number of Spyware/Grayware Destinations • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date • Group by: Day

TABLE 4-11. Top 25 Spyware/Grayware Bar Chart



Data view: • Overall Spyware/Grayware Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Detection Count • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Spyware/Grayware Name • Label name: Spyware/Grayware Name • Sorting: Aggregation value > Descending • Filter summarized result: Display top 25 > Aggregate remaining items

TABLE 4-12. Overall Spyware/Grayware Summary Grid Table

Overall Spyware/Grayware Summary			
Spyware/Grayware Name	Unique Spyware/Grayware Destination Count	Unique Spyware/Grayware Source Count	Spyware/Grayware Detection Count
DIAL_AGENT.IVC	1	1	378
ADW_APROPOS.51	1	1	27
ADW_LOOK2ME.C	2	1	24
SPYW_PROAGENT.20	1	1	21
ADW_SLAGENT.A	1	1	18
SPYW_PERFLOG.A	1	1	18
ADW_TVMEDIA.C	1	1	17
SPYW_PCPOL.200	1	1	14
SPYW_PCACME.74	1	1	13
DIAL_PORNDIAL.AF	1	1	12
SPYW_PRIVEYE.140	1	1	12
ADW_SUBMITURL.A	1	1	11
ADW_COMMONNAME.A	1	1	10
SPYW_TYPEREC.10	1	1	10
SPYW_REALSPY.222	1	1	9
ADW_APROPOS.M	1	1	8
JOKE_150ALERTS	1	1	8
SPYW_COOLWEB.B	1	1	8
ADW_BLAZE.A	1	1	7
CRCK_JBEAN.A	1	2	7
SPYW_WEBSEARCH.A	1	1	7
ADW_ISTBAR.B	1	1	6
ADW_OPENSITE.A	1	1	6
ADW_SAFESEARCH.A	1	1	6
SPYW_COOLWEB.A	1	1	6

Data view:

- Overall Spyware/Grayware Summary

Query Criteria:

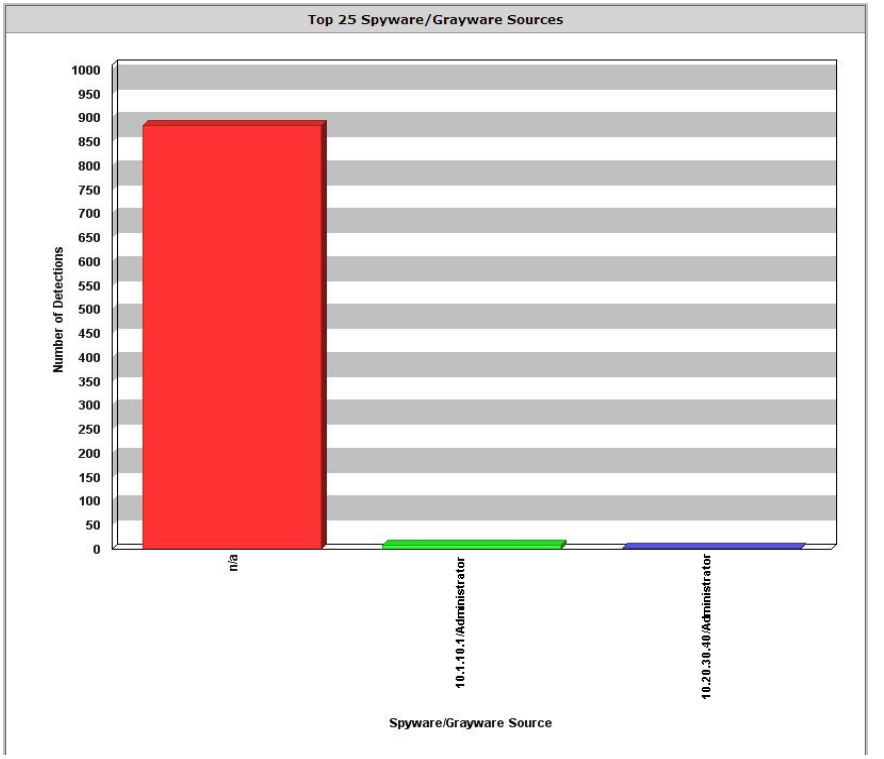
- Security Risk Type > is equal to > Non-cookie types

Table Columns:

- Spyware/Grayware Name
- Spyware/Grayware Destination Count
- Spyware/Grayware Source Count
- Spyware/Grayware Detection Count

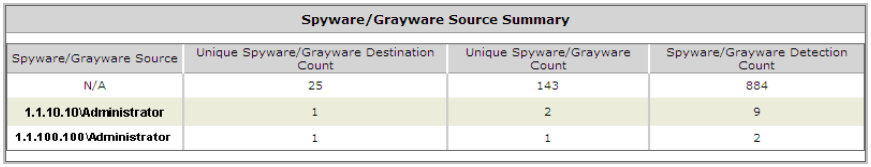
Sorting: Spyware/Grayware Detection Count > Descending
Display quantity: 25

TABLE 4-13. Top 25 Spyware/Grayware Sources Bar Chart



Data view: • Spyware/Grayware Source Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Detection Count • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Spyware/Grayware Source • Label name: Spyware/Grayware Source • Sorting: Aggregation value > Descending • Filter summarized result: Display top 25

TABLE 4-14. Spyware/Grayware Source Summary Grid Table

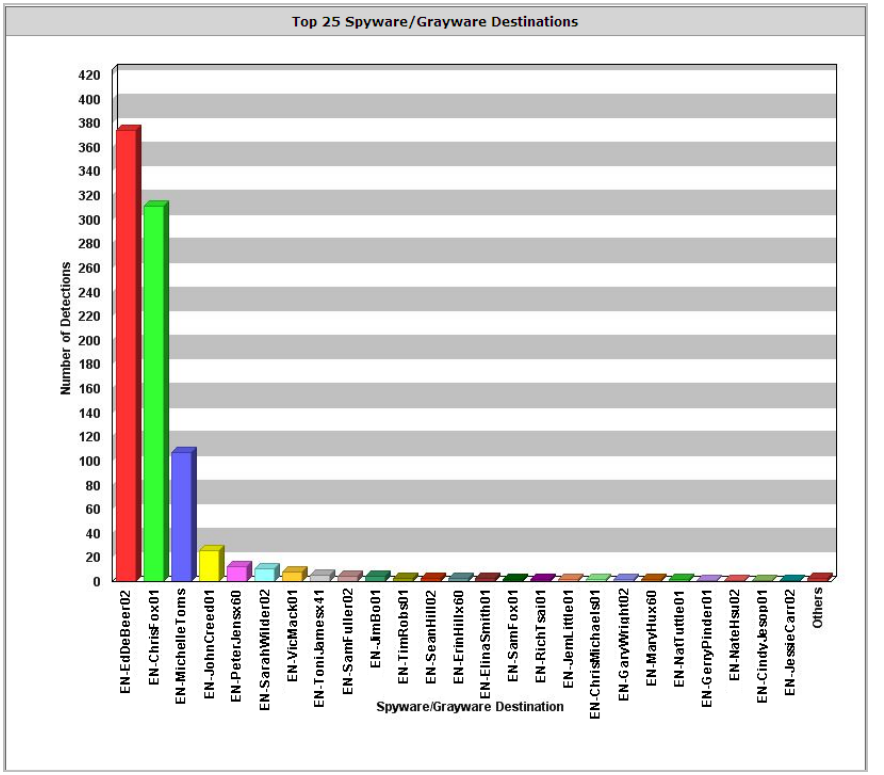


Spyware/Grayware Source Summary

Spyware/Grayware Source	Unique Spyware/Grayware Destination Count	Unique Spyware/Grayware Count	Spyware/Grayware Detection Count
N/A	25	143	884
1.1.10.10\Administrator	1	2	9
1.1.100.100\Administrator	1	1	2

Data view: • Spyware/Grayware Source Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Table Columns: • Spyware/Grayware Source • Spyware/Grayware Destination Count • Unique Spyware/Grayware Count • Spyware/Grayware Detection Count Sorting: Spyware/Grayware Detection Count > Descending Display quantity: 25

TABLE 4-15. Top 25 Spyware/Grayware Destinations Bar Chart



Data view: • Spyware/Grayware Destination Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Detection Count • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Spyware/Grayware Destination • Label name: Spyware/Grayware Destination • Sorting: Aggregation value > Descending • Filter summarized result:: Display top 25

TABLE 4-16. Spyware/Grayware Destination Summary Grid Table

Spyware/Grayware Destination Summary			
Spyware/Grayware Destination	Unique Spyware/Grayware Source Count	Unique Spyware/Grayware Count	Spyware/Grayware Detection Count
EN-EdDeBeer02	1	1	378
EN-ChrisFox01	1	72	311
EN-MichelleToms	1	13	107
EN-JohnCreed01	1	19	26
EN-PeterJensx60	1	6	12
EN-SarahWilder02	2	2	11
EN-VicMack01	1	8	8
EN-ToniJamesx41	1	3	5
EN-SamFuller02	1	1	4
EN-JimBo01	1	1	4
EN-TimRobs01	1	2	3
EN-SeanHill02	1	2	3
EN-ErinHillx60	1	3	3
EN-ElinaSmith01	1	1	2
EN-SamFox01	1	2	2
EN-RichTsai01	1	1	2
EN-JemLittle01	1	1	2
EN-ChrisMichaels01	1	1	2
EN-GaryWright02	1	1	2
EN-MaryHux60	1	2	2
EN-NatTuttle01	1	1	1
EN-GerryPinder01	1	1	1
EN-NateHsu02	1	1	1
EN-CindyJesop01	1	1	1
EN-JessieCarr02	1	1	1

Data view:

- Spyware/Grayware Destination Summary

Query Criteria:

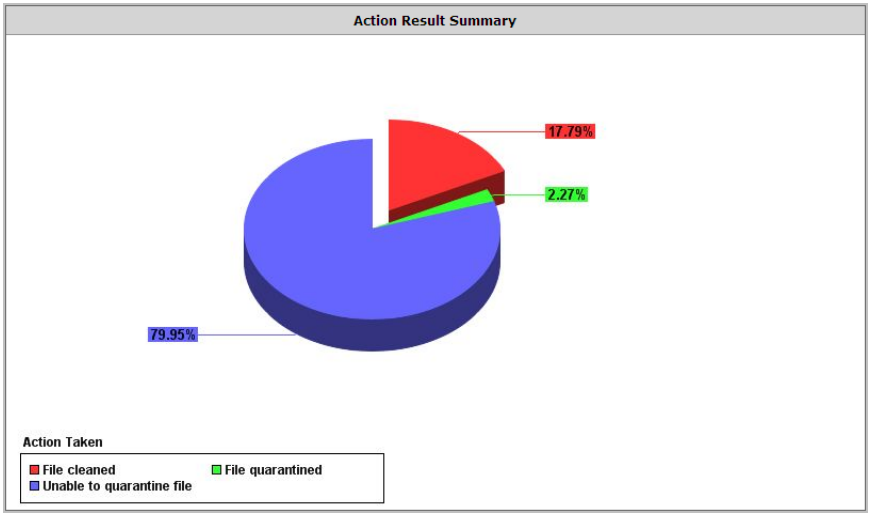
- Security Risk Type > is equal to > Non-cookie types

Table Columns:

- Spyware/Grayware Destination
- Spyware/Grayware Source Count
- Unique Spyware/Grayware Count
- Spyware/Grayware Detection Count

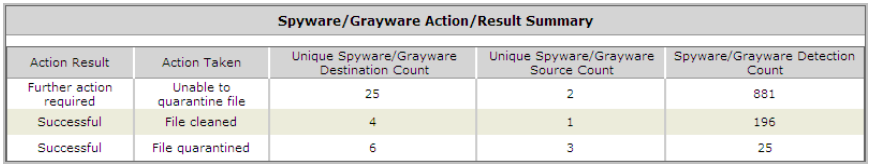
Sorting: Spyware/Grayware Detection Count > Descending
Display quantity: 25

TABLE 4-17. Action Result Summary Pie Chart



Data view: • Spyware/Grayware Action/Result Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Data Properties: • Spyware/Grayware Detection Count • Aggregated by: Sum of Value Category Properties: • Action Taken • Label name: Action Taken • Sorting: Category name > Ascending

TABLE 4-18. Spyware/Grayware Action/Result Summary Grid Table



Spyware/Grayware Action/Result Summary				
Action Result	Action Taken	Unique Spyware/Grayware Destination Count	Unique Spyware/Grayware Source Count	Spyware/Grayware Detection Count
Further action required	Unable to quarantine file	25	2	881
Successful	File cleaned	4	1	196
Successful	File quarantined	6	3	25

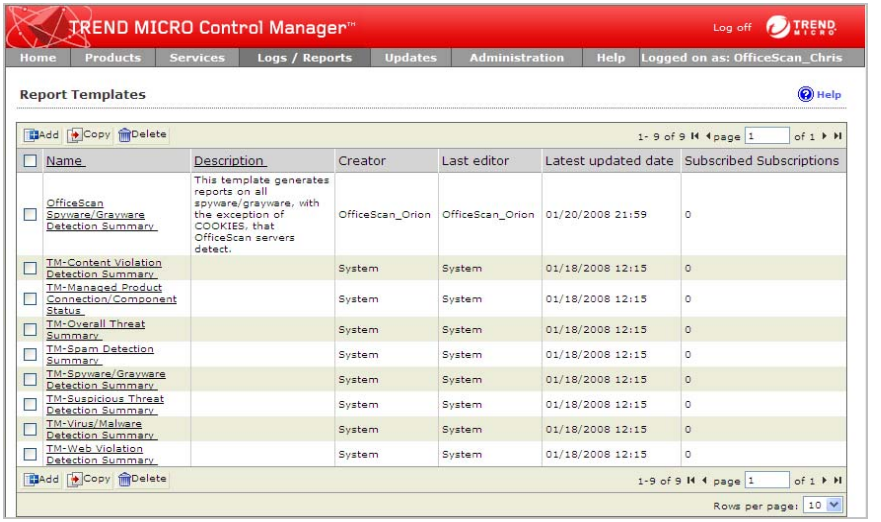
Data View: • Spyware/Grayware Action/Result Summary Query Criteria: • Security Risk Type > is equal to > Non-cookie types	Table Columns: • Action Result • Action Taken • Spyware/Grayware Destination Count • Spyware/Grayware Source Count • Spyware/Grayware Detection Count Sorting: Spyware/Grayware Detection Count > Descending Display quantity: 25

After looking over the reports and gathering feedback from his manager and other OfficeScan administrator's, Chris decides he needs to modify the report template. Chris does not want to see the bar for **Others** in the table 4-11, "Top 25 Spyware/Grayware Bar Chart," on page 4-102. He needs to modify the template to remove these items or change how they display.

To edit the report template:

1. Mouseover **Logs/Reports**. A drop-down menu appears.

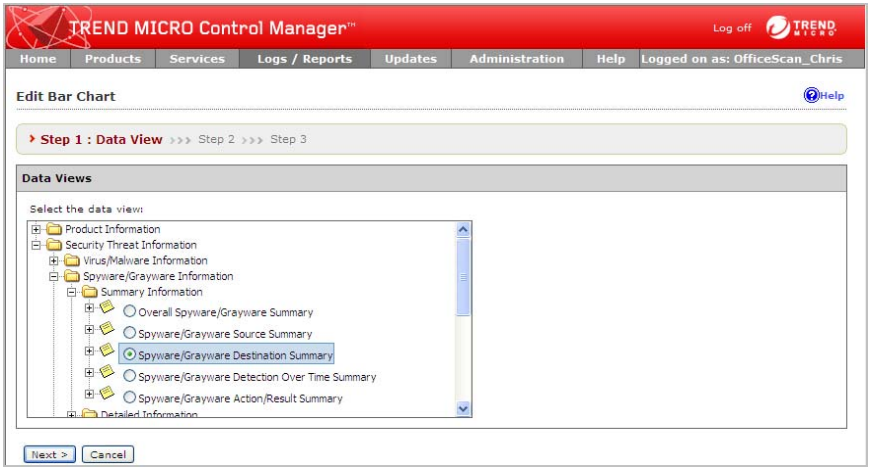
2. Click **Report Templates** from the drop-down menu. The Report Templates screen appears.



3. Click **OfficeScan Spyware/Grayware Detection Summary** from the Report Templates list. The Edit Report Template screen appears.

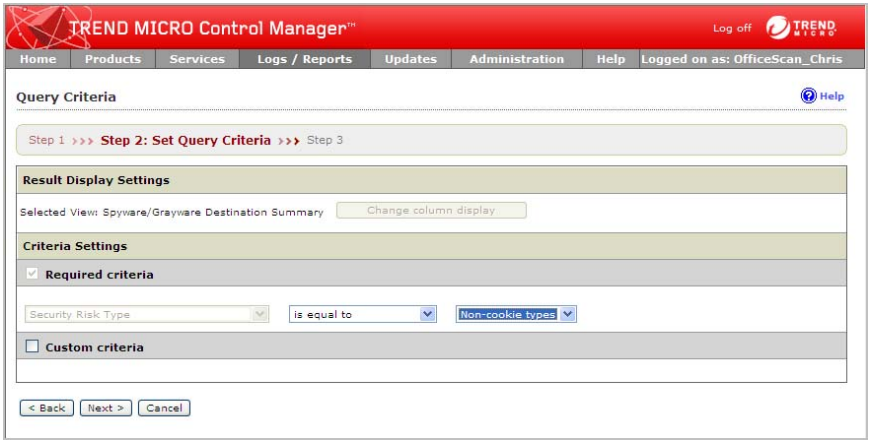
Step 1: Edit the Top 25 Spyware/Grayware bar chart:

1. Click **Edit** on the Top 25 Spyware/Grayware bar chart. The Edit Bar Chart screen appears.



Chris does not want to change the settings on this screen.

2. Click **Next**. The Query Criteria screen appears.



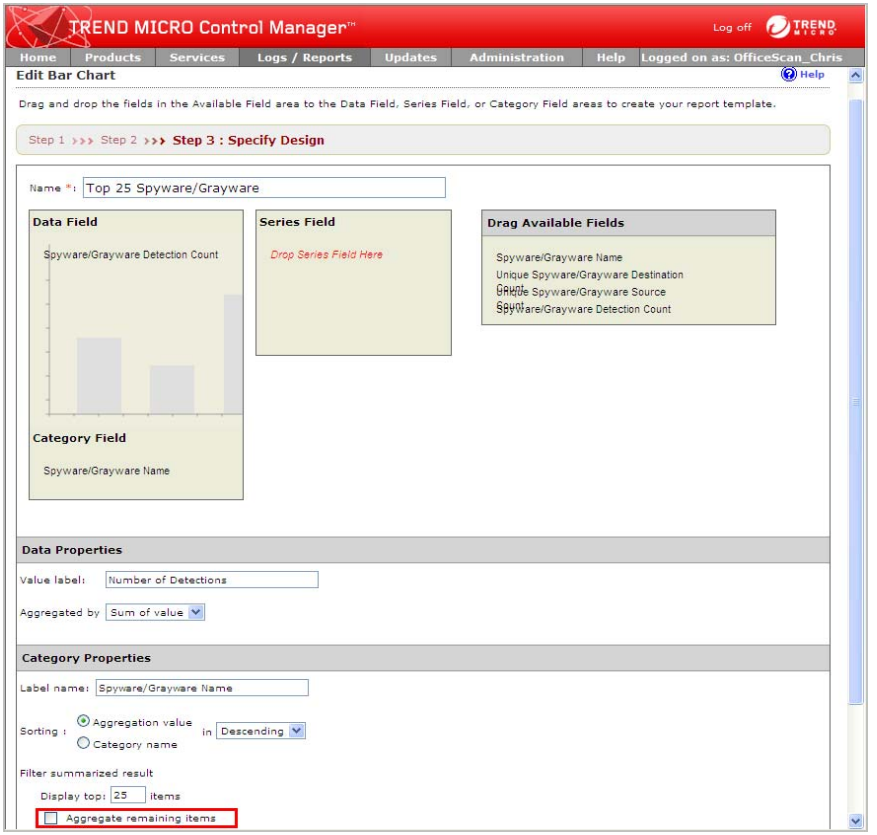
Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

Chris does not want cookies to appear in his bar chart for spyware/grayware and he has already specified that when he modified the report template.

Step 3: Configure bar chart settings:

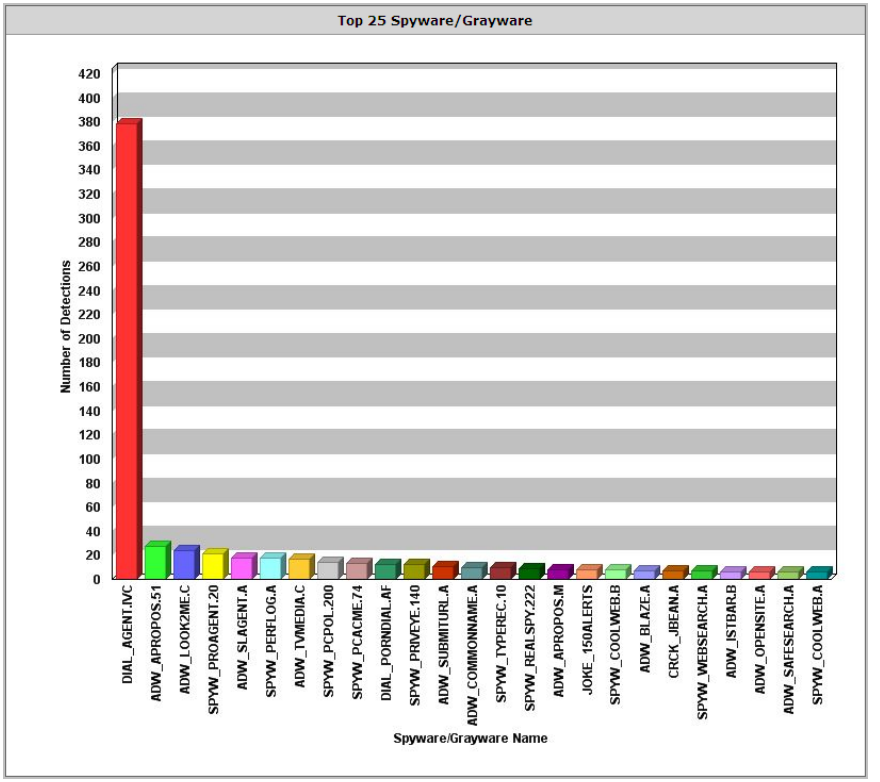
1. Click **Next**. The Edit Bar Chart > Step 3 Specify Design screen appears.



2. Clear the **Aggregate remaining items** check box under Category Properties, to stop the bar **Others** from appearing in the bar chart.
3. Click **Save**. The Add Report Template screen appears.

After modifying the report template Chris regenerates the report to check the results.

TABLE 4-19. Top 25 Spyware/Grayware Bar Chart



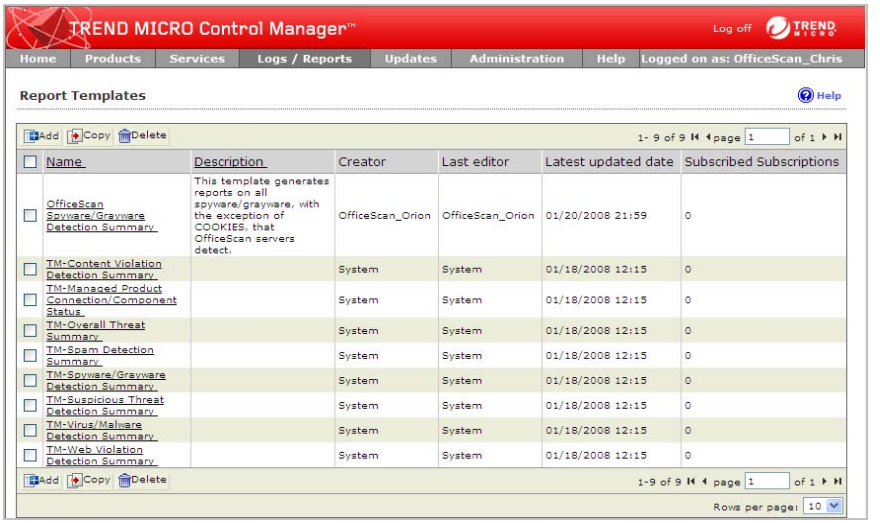
Data view: • Overall Spyware/Grayware Summary Query Criteria: • Security Risk Type is > not equal to > COOKIES	Data Properties: • Spyware/Grayware Detection Count • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Spyware/Grayware Name • Label name: Spyware/Grayware Name • Sorting: Aggregation value > Descending • Filter summarized result: Display top 25

Creating a New Report Template

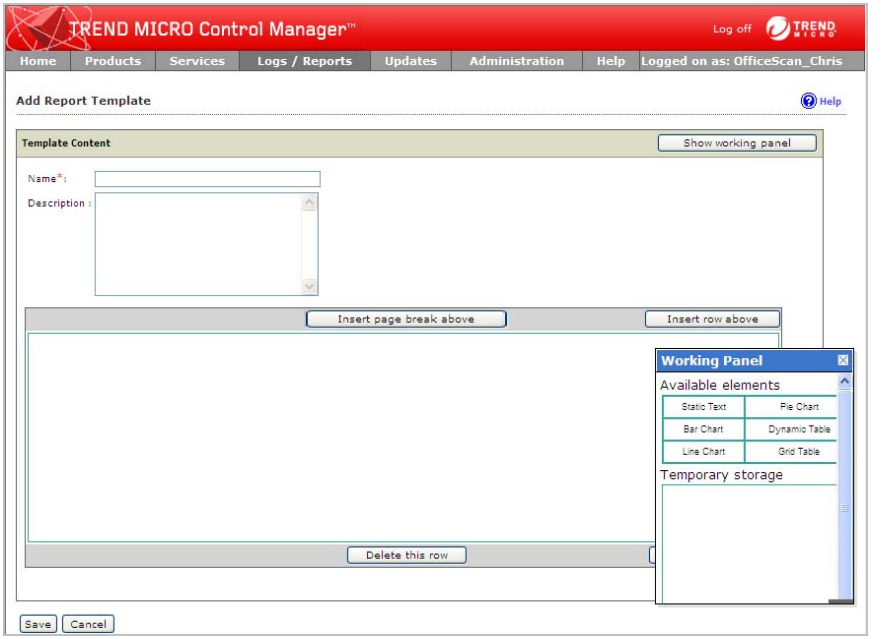
Chris has modified an existing template for spyware/grayware detected by his OfficeScan servers. Chris would like to create a report template, but he does not want to make another high-level report. Chris now wants to create a detailed report that displays information that will require him to take action on his network. Specifically he wants to focus on computers that require action on his part.

To create a new report template:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Report Templates** from the menu. The Report Templates screen appears.



4. Click **Add**. The Add Report Template screen appears.



5. Type the following in the **Name** field:

   OfficeScan Client Requires Further Action Report

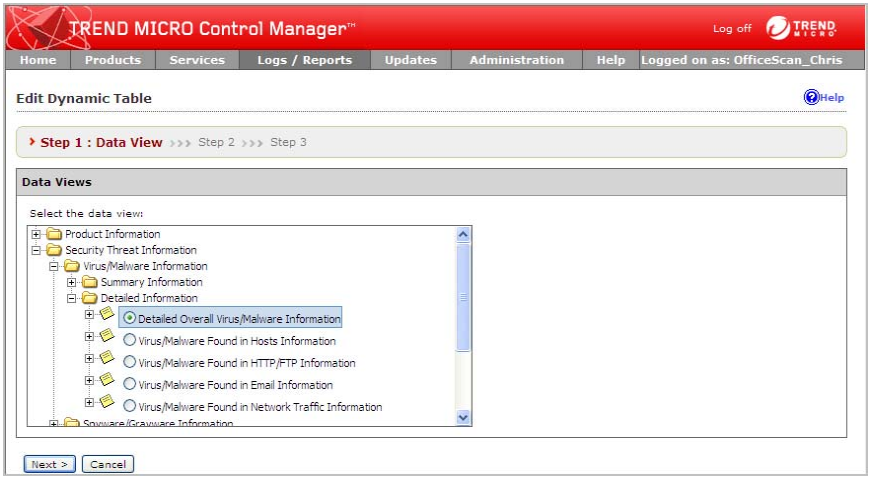
6. Type the following in the **Description** field:

   This report provides information on OfficeScan clients that require further action by administrators.

7. Drag-and-drop **Dynamic Table** to the work area.

Step 1: Select the data view for the report element:

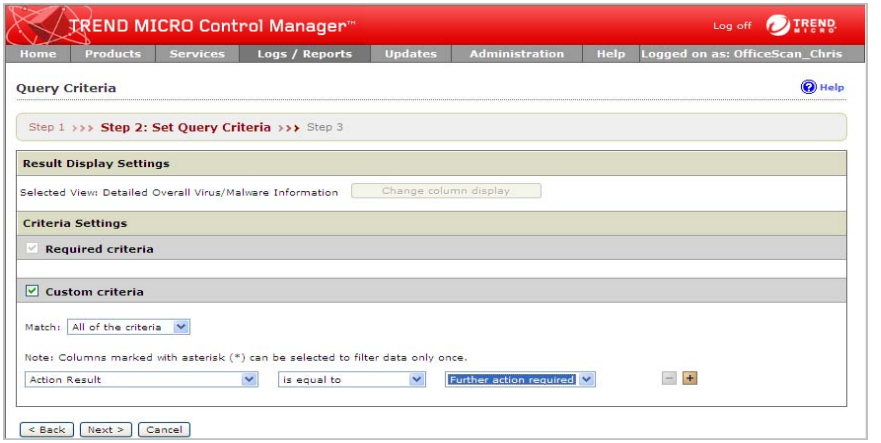
1. Click **Edit** on the dynamic table. The Edit Dynamic Table screen appears.



2. Expand the data view tree to the following: **Security Threat Information > Virus/Malware Information > Detailed Information**.
3. Select **Detailed Overall Virus/Malware Information**.

Step 2: Specify the query criteria for the template:

4. Click **Next**. The Query Criteria screen appears.



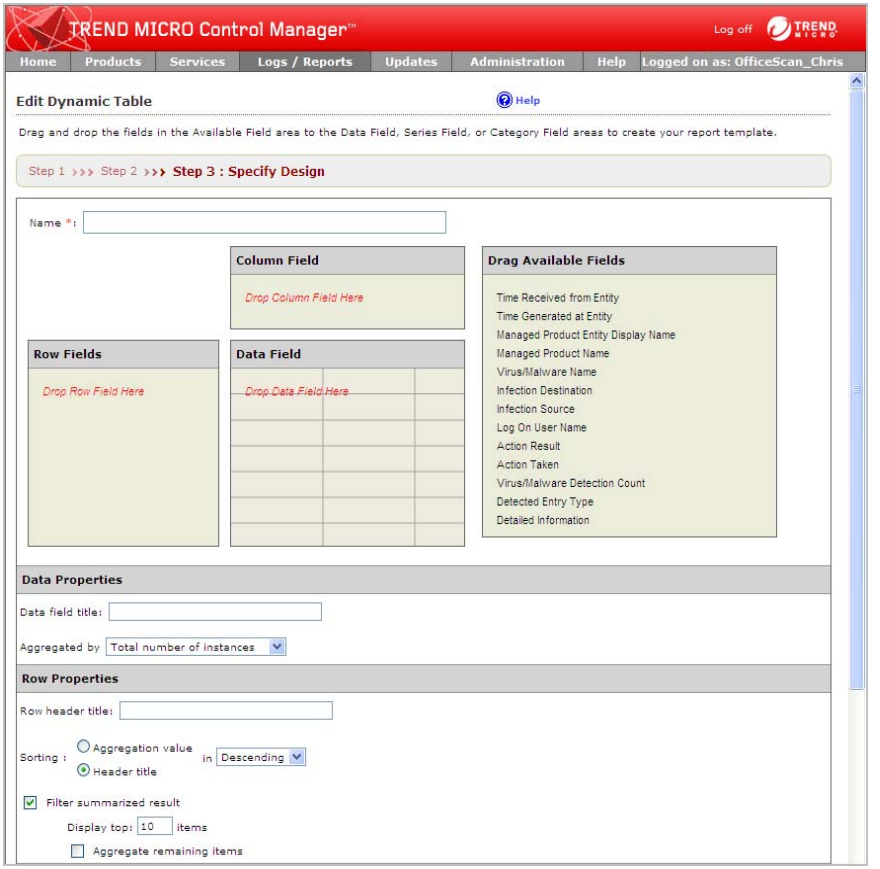
> **Tip:** If you do not specify any filtering criteria, the Ad Hoc query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify the analysis of the data that the query returns.

Chris only wants to see computers that require further action (OfficeScan was not able to clean, delete, or quarantine the virus).

1. Specify the following:
   - **Action Result > is equal to > Further action required**

Step 3: Specify the design for the template:

2. Click **Next**. The Edit Dynamic Table > Step 3 Specify Design screen appears.



Chris wants this table to display only the items that he will have to investigate. He is not concerned with clients that have successfully cleaned or quarantined viruses. Chris also wants to see the name of clients upon which he has to take action.

1. Type the following in the **Name** field:

   OfficeScan Clients Requiring Further Action: Virus/Malware

2. Drag-and-drop **Action Taken** to **Drop Column Field Here.**

   This will display all the actions OfficeScan takes against virus/malware as columns for the table.

3. Drag-and-drop **Managed Product Entity Display Name** and then **Infection Destination** to **Drop Row Field Here.**

   The order which the fields are dropped is important. Chris wants the OfficeScan clients to display as secondary to the OfficeScan server that manages the clients. The OfficeScan server and clients display in the row fields.

4. Drag-and-drop **Virus/Malware Detection Count** to **Drop Data Field Here.**

   Chris wants to know the number of incidents he needs to take action against.

5. Specify the display settings for the Data Properties:

   Chris does not want to change the Data Properties settings.

   a. Specify how data displays for Data Fields from the **Aggregated by** drop-down list:

      - **Sum of value:** Specifies that the total number of virus/malware incidents are included

6. Specify the display settings for the Row Properties.

   a. Type the following in the **Label name** field:

      OfficeScan Server > Client

   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

   c. Clear the **Filter summarized result** check box.

7. Specify the display settings for the Column Properties.

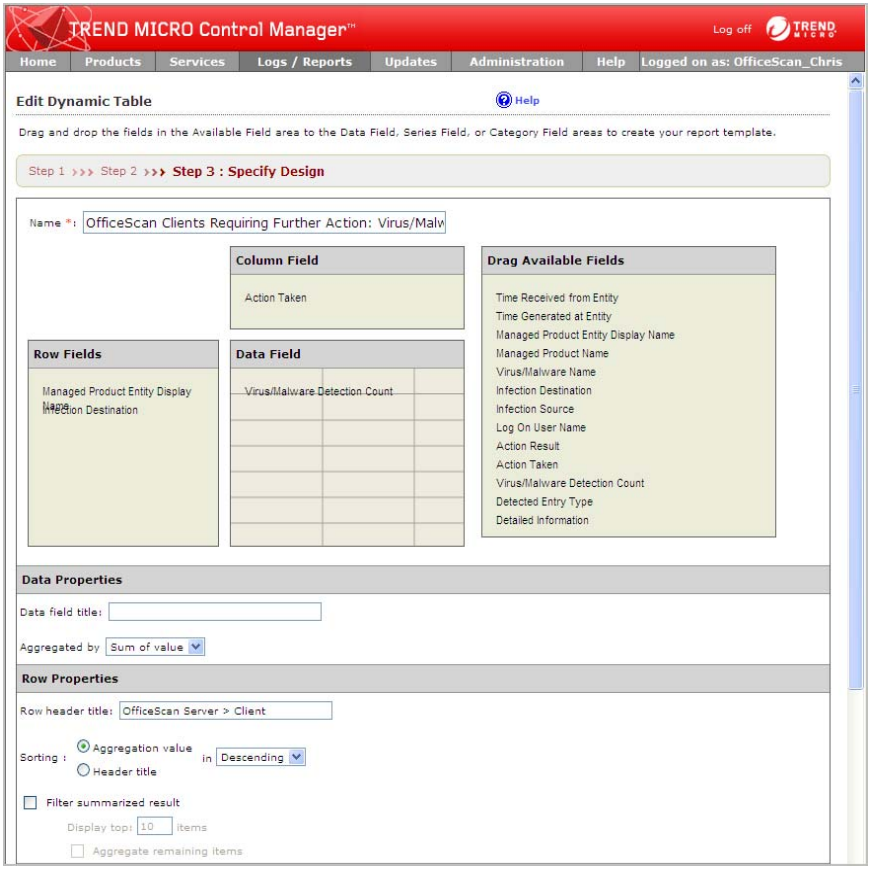
   a. Type the following in the **Label name** field:

      Further Action Required

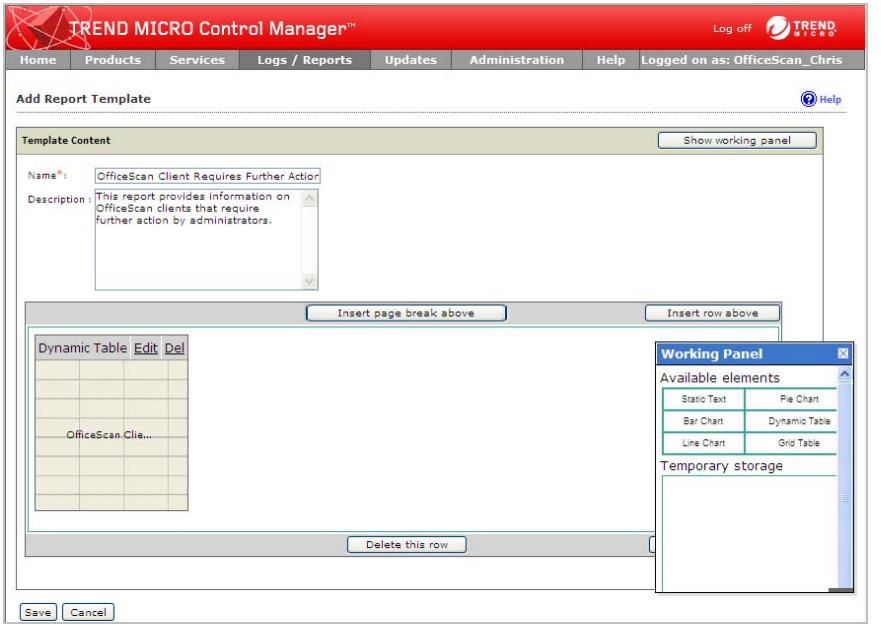
   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

The Edit Dynamic Table screen appears as follows after completing the steps for the screen.



8. Click **Save**. The Add Report Template screen appears.

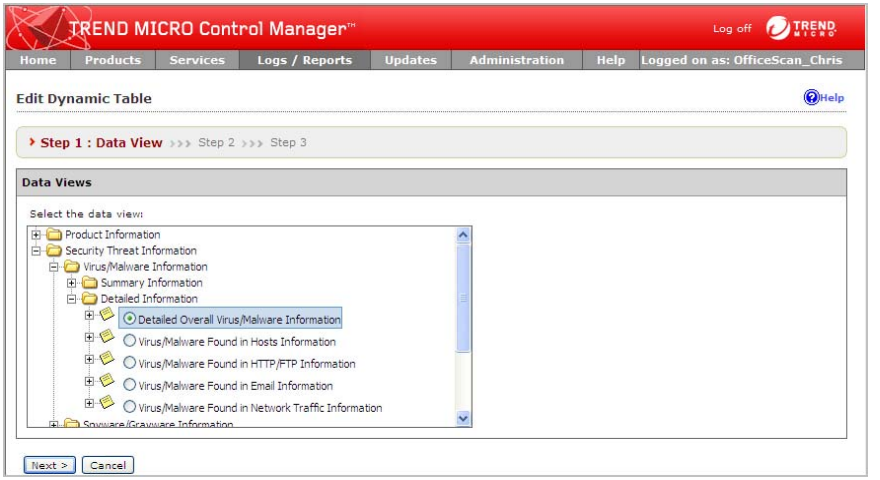


9. Click **Insert Row Below**. A row appears below the first row.
10. Drag-and-drop **Dynamic Table** to the work area in the second row.

Add a Report Element

Step 1: Select the data view for the report element:

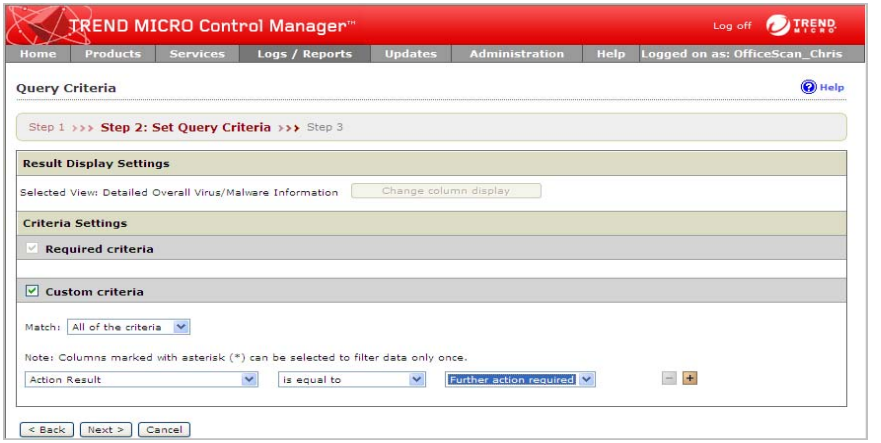
1. Click **Edit** on the dynamic table. The Edit Dynamic Table screen appears.



2. Expand the data view tree to the following: **Security Threat Information > Virus/Malware Information > Detailed Information**.
3. Select **Detailed Overall Virus/Malware Information**.

Step 2: Specify the query criteria for the template:

4. Click **Next**. The Query Criteria screen appears.

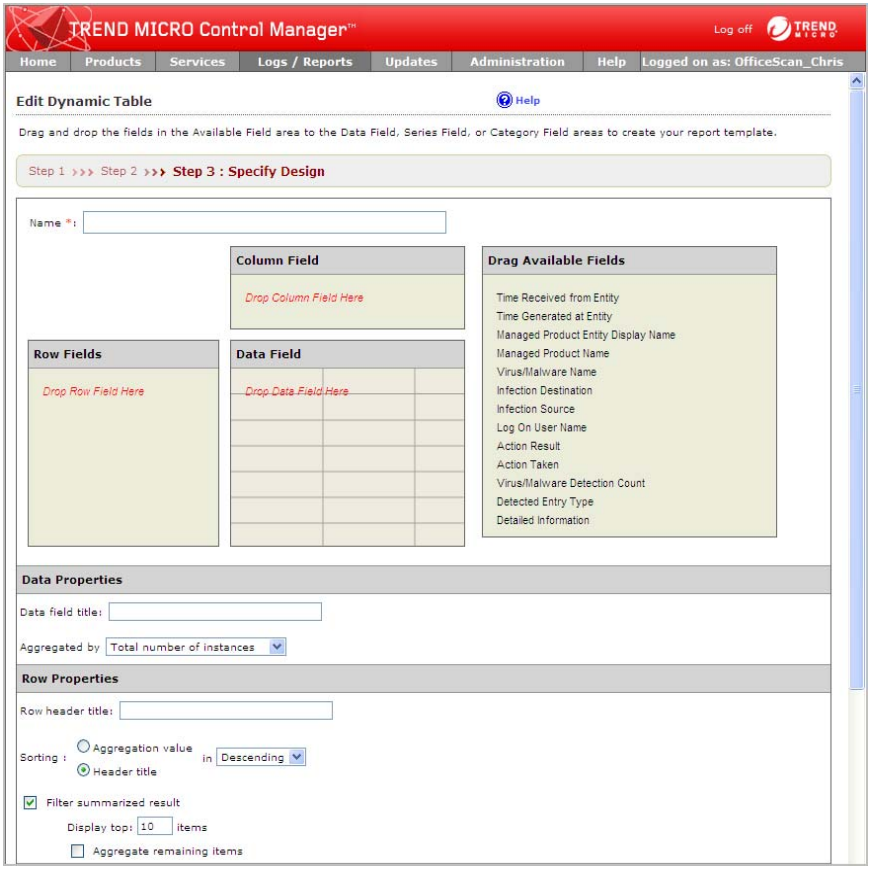


> **Tip:** If you do not specify any filtering criteria, the Ad Hoc query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify the analysis of the data that the query returns.

Chris only wants to see clients that require further action (OfficeScan was not able to clean, delete, or quarantine the virus).

1. Specify the following:
   - **Action Result > is equal to > Further action required**

2. Click **Next**. The Edit Dynamic Table > Step 3 Specify Design screen appears.



Step 3: Specify the design for the template:

Chris wants this table to display only the items that he will have to investigate. He is not concerned with clients that have successfully cleaned or quarantined viruses. Chris also wants to see the name of clients upon which he has to take action.

1. Type the following in the **Name** field:

   OfficeScan Network Requiring Further Action: Virus/Malware

2. Drag-and-drop **Virus/Malware Name** to **Drop Column Field Here.**

   This will display all the viruses/malware OfficeScan detects as columns for the table.

3. Drag-and-drop **Managed Product Entity Display Name** and then **Infection Destination** to **Drop Row Field Here.**

   The order which the fields are dropped is important. Chris wants the OfficeScan clients to display as secondary to the OfficeScan server that manages the clients. The OfficeScan server and clients display in the row fields.

4. Drag-and-drop **Virus/Malware Detection Count** to **Drop Data Field Here.**

   Chris wants to know the number of incidents he needs to take action against.

5. Specify the display settings for the Data Properties:

   Chris does not want to change the Data Properties settings.

   a. Specify how data displays for Data Fields from the **Aggregated by** drop-down list:

      - **Sum of value:** Specifies that the total number of virus/malware incidents are included

6. Specify the display settings for the Row Properties.

   a. Type the following in the **Label name** field:

      OfficeScan Server > Client

   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

   c. Clear the **Filter summarized result** check box.

7. Specify the display settings for the Column Properties.

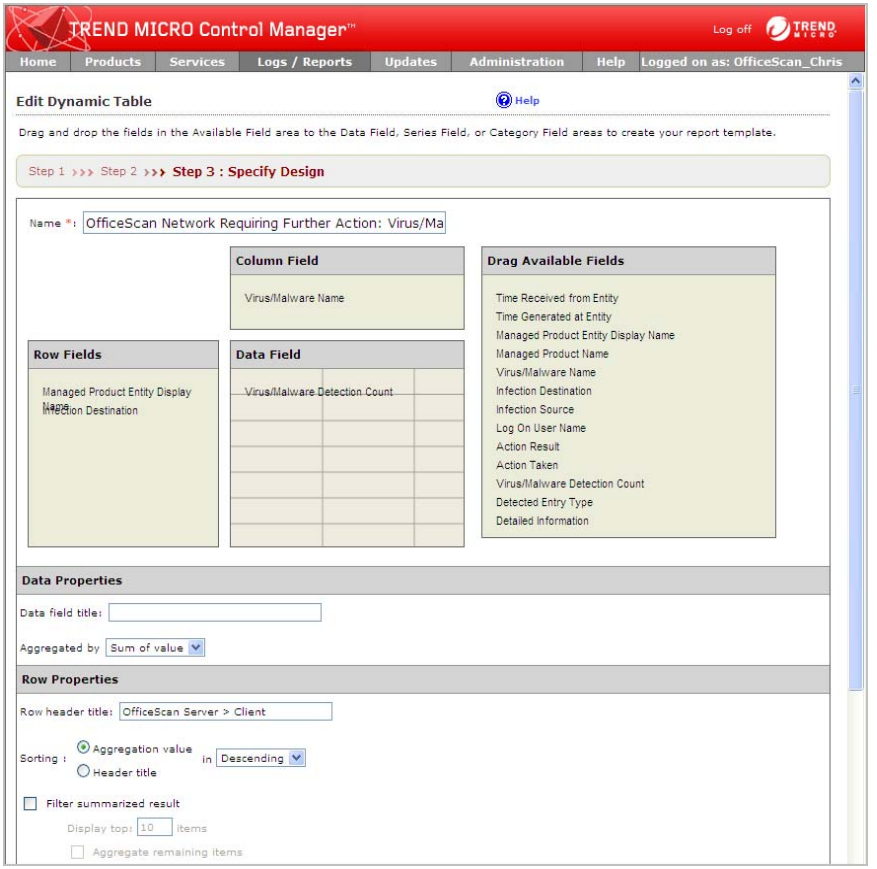
   a. Type the following in the **Label name** field:

      Further Action Required

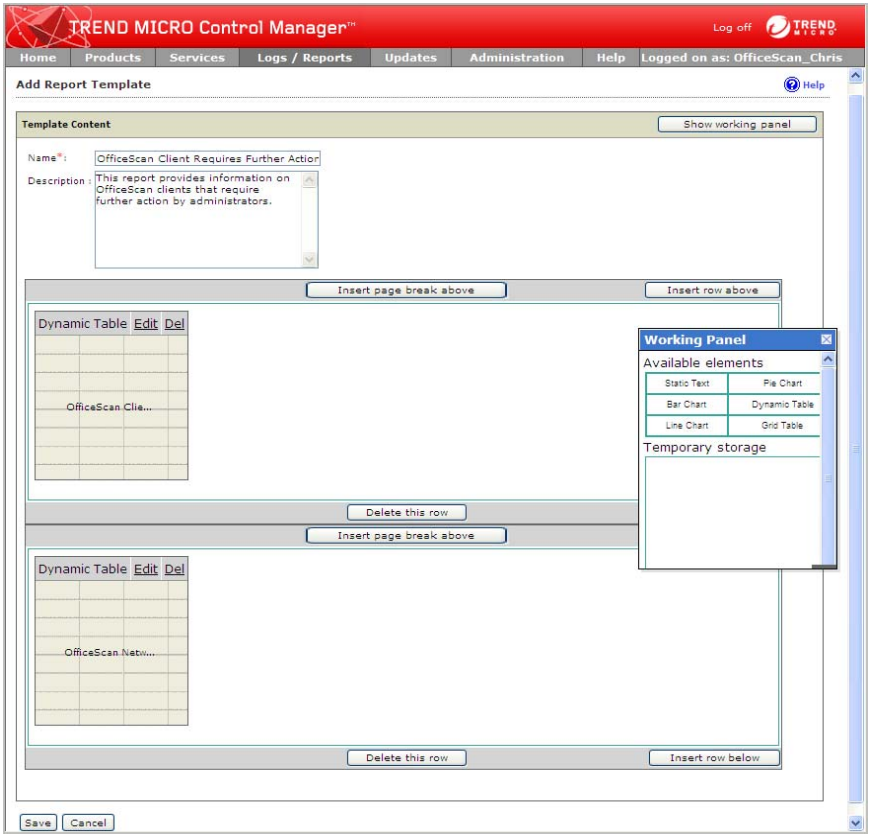
   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

The Edit Dynamic Table screen appears as follows after completing the steps for the screen.



8. Click **Save**. The Add Report Template screen appears.

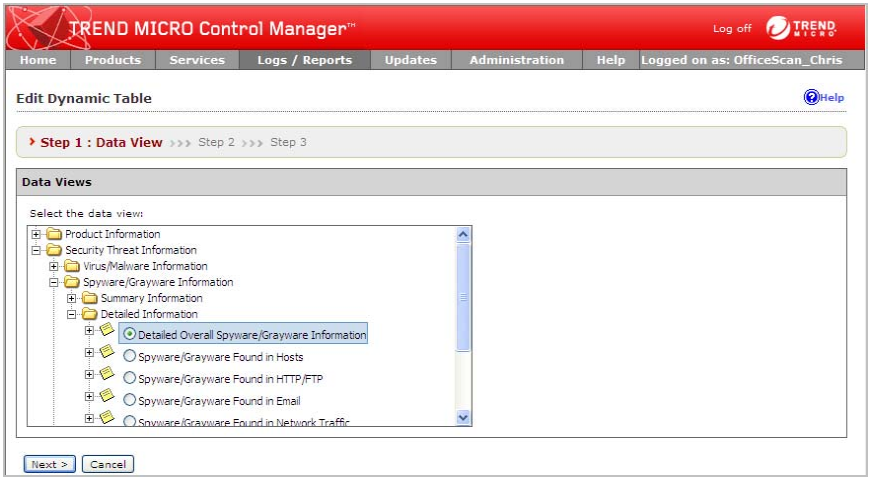


9. Click **Insert Row Below** under the second row. A row appears below the second row.
10. Drag-and-drop **Dynamic Table** to the work area in the third row.

Add a Report Element

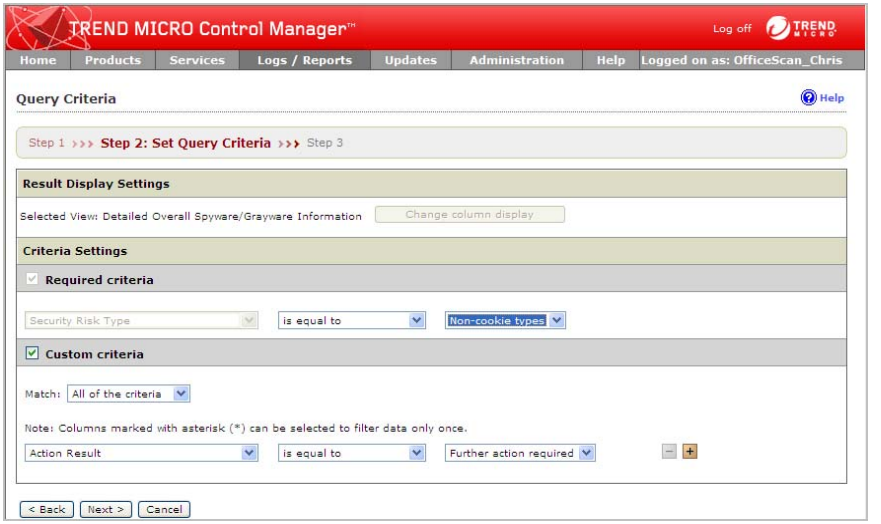
Step 1: Select the data view for the report element:

1. Click **Edit** on the dynamic table. The Edit Dynamic Table screen appears.



2. Expand the data view tree to the following: **Security Threat Information > Spyware/Grayware Information > Detailed Information**.
3. Select **Detailed Overall Spyware/Grayware Information**.

4. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the query criteria for the template:

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 the analysis of the data that the query returns.

Chris does not want cookies to appear in his table for spyware/grayware incidents. Chris also only wants to focus on computers that require further action on his part.

1. Specify the following:

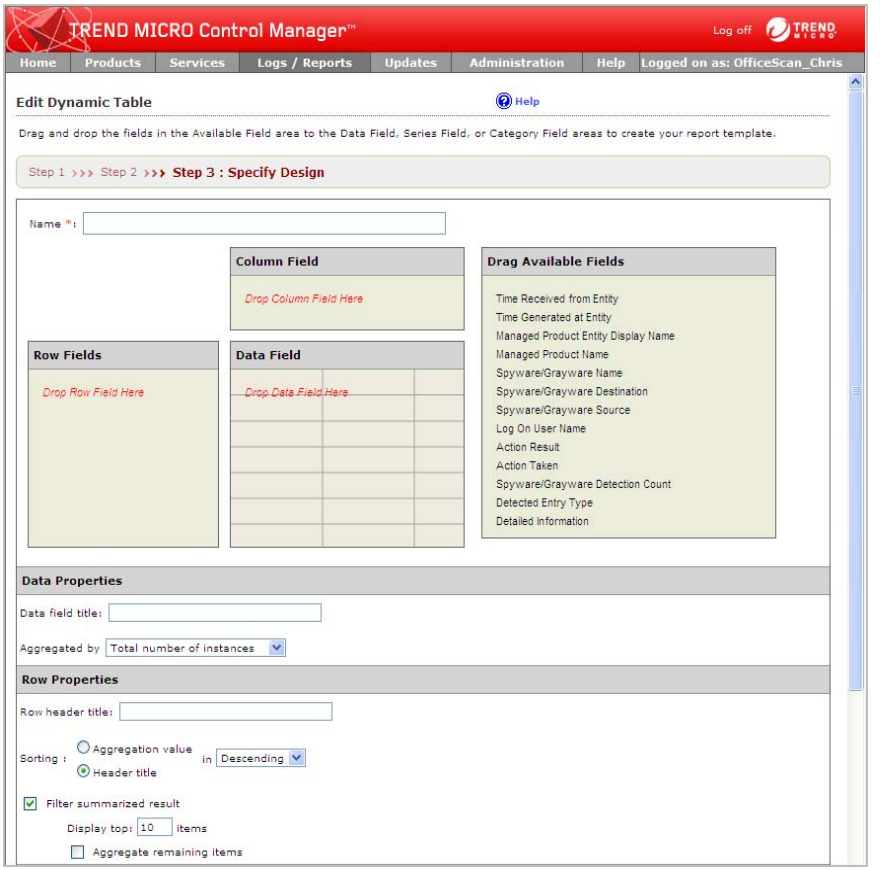
   Required criteria:

   - **Security Risk Type > is equal to > Non-cookie types**

   Custom criteria:

   - **Match: All of the criteria**
   - **Action Result > is equal to > Further action required**

2. Click **Next**. The Edit Dynamic Table > Step 3 Specify Design screen appears.



Step 3: Specify the design for the template:

Chris wants this table to display only the items that he will have to investigate. He is not concerned with clients that have successfully cleaned spyware. Chris also wants to see the name of clients upon which he has to take action.

1. Type the following in the **Name** field:

   OfficeScan Clients Requiring Further Action: Spyware/Grayware

2. Drag-and-drop **Action Taken** to **Drop Column Field Here.**

   This will display all the actions OfficeScan takes against virus/malware as columns for the table.

3. Drag-and-drop **Managed Product Entity Display Name** and then **Spyware/Grayware Destination** to **Drop Row Field Here.**

   The order which the fields are dropped is important. Chris wants the OfficeScan clients to display as secondary to the OfficeScan server that manages the clients. The OfficeScan server and clients display in the row fields.

4. Drag-and-drop **Spyware/Grayware Detection Count** to **Drop Data Field Here.**

   Chris wants to know the number of incidents he needs to take action against.

5. Specify the display settings for the Data Properties:

   Chris does not want to change the Data Properties settings.

   a. Specify how data displays for Data Fields from the **Aggregated by** drop-down list:

      - **Sum of value:** Specifies that the total number of spyware/grayware incidents are included

6. Specify the display settings for the Row Properties.

   a. Type the following in the **Label name** field:

      OfficeScan Server > Client

   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

   c. Clear the **Filter summarized result** check box.

7. Specify the display settings for the Column Properties.

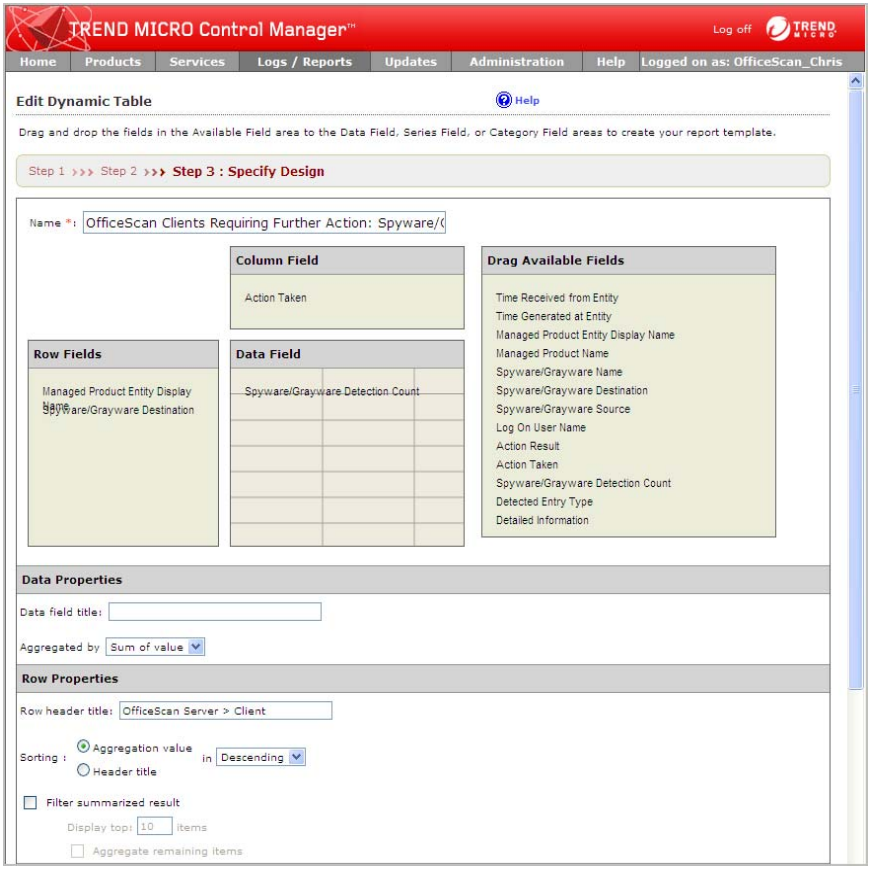
   a. Type the following in the **Label name** field:

      Further Action Required

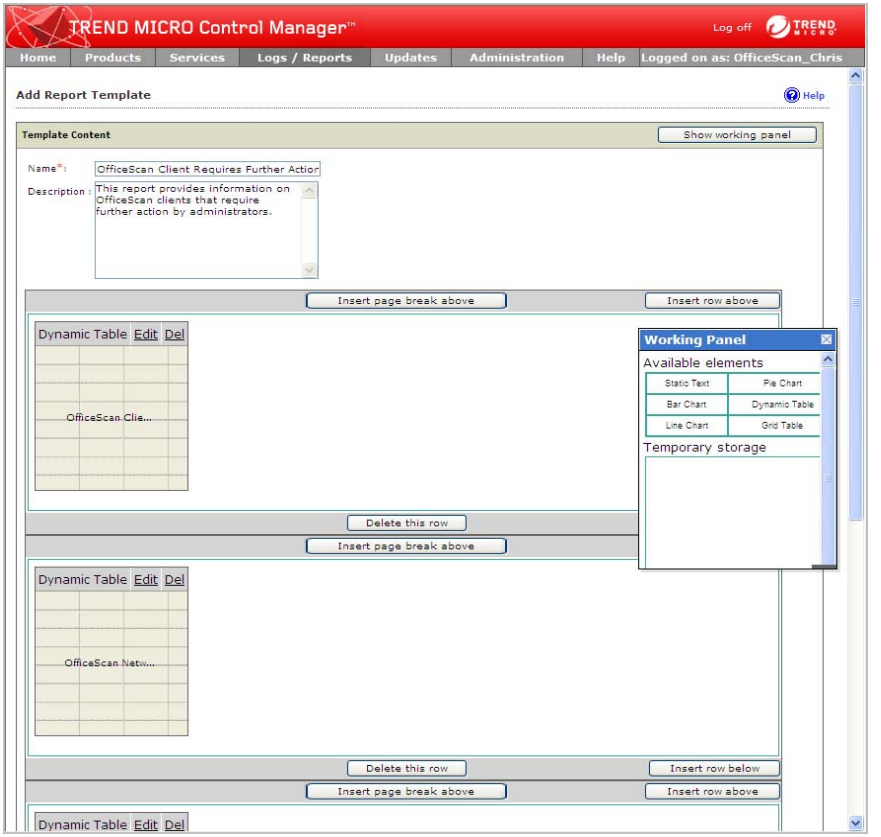
   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

The Edit Dynamic Table screen appears as follows after completing the steps for the screen.



8. Click **Save**. The Add Report Template screen appears.

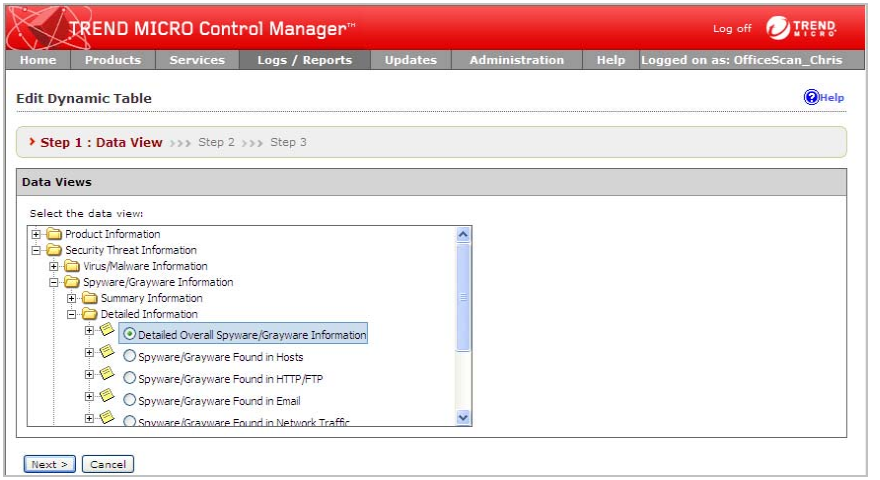


9. Click **Insert Row Below** under the third row. A row appears below the third row.
10. Drag-and-drop **Dynamic Table** to the work area in the fourth row.

Add a Report Element

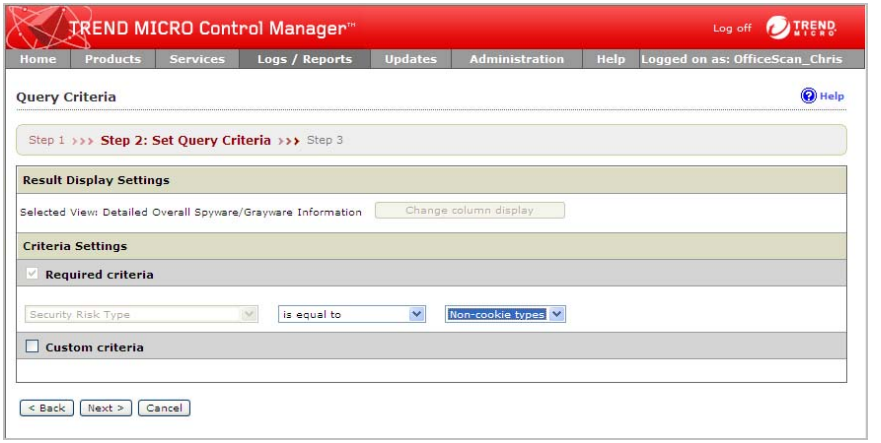
Step 1: Select the data view for the report element:

1. Click **Edit** on the dynamic table. The Edit Dynamic Table screen appears.



2. Expand the data view tree to the following: **Security Threat Information > Spyware/Grayware Information > Detailed Information**.
3. Select **Detailed Overall Spyware/Grayware Information**.

4. Click **Next**. The Query Criteria screen appears.



Step 2: Specify the filtering criteria for the template:

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 the analysis of the data that the query returns.

Chris does not want cookies to appear in his table for spyware/grayware incidents. Chris also only wants to focus on computers that require further action on his part.

1. Specify the following:

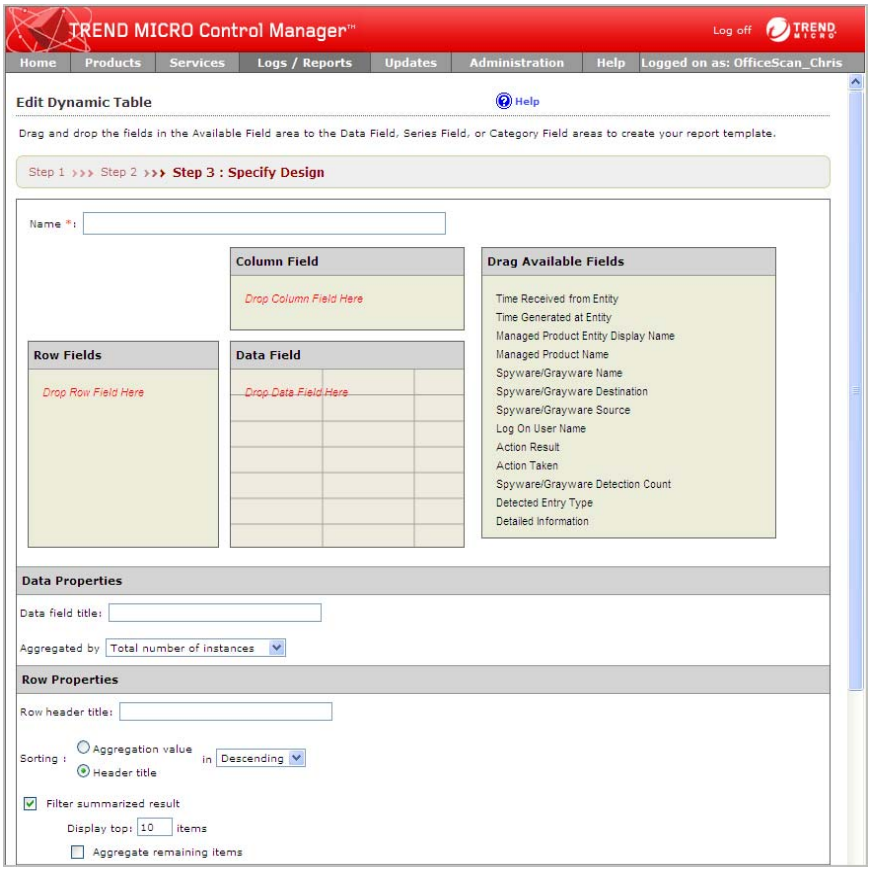
   Required criteria:

   - **Security Risk Type > is equal to > Non-cookie types**

   Custom criteria:

   - **Match: All of the criteria**
   - **Action Result > is equal to > Further action required**

2. Click **Next**. The Edit Dynamic Table > Step 3 Specify Design screen appears.



Step 3: Specify the design for the template:

Chris wants this table to display only the items that he will have to investigate. He is not concerned with clients that have successfully cleaned spyware. Chris also wants to see the name of clients upon which he has to take action.

1. Type the following in the **Name** field:

   OfficeScan Network Requiring Further Action: Spyware/Grayware

2. Drag-and-drop **Spyware/Grayware Name** to **Drop Column Field Here.**

   This will display all spyware/grayware that OfficeScan detects as columns for the table.

3. Drag-and-drop **Managed Product Entity Display Name** and then **Infection Destination** to **Drop Row Field Here.**

   The order which the fields are dropped is important. Chris wants the OfficeScan clients to display as secondary to the OfficeScan server that manages the clients. The OfficeScan server and clients display in the row fields.

4. Drag-and-drop **Spyware/Grayware Detection Count** to **Drop Data Field Here.**

   Chris wants to know the number of incidents he needs to take action against.

5. Specify the display settings for the Data Properties:

   Chris does not want to change the Data Properties settings.

   a. Specify how data displays for Data Fields from the **Aggregated by** drop-down list:

      - **Sum of value:** Specifies that the total number of spyware/grayware incidents are included

6. Specify the display settings for the Row Properties.

   a. Type the following in the **Label name** field:

      OfficeScan Server > Client

   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

   c. Clear the **Filter summarized result** check box.

7. Specify the display settings for the Column Properties.

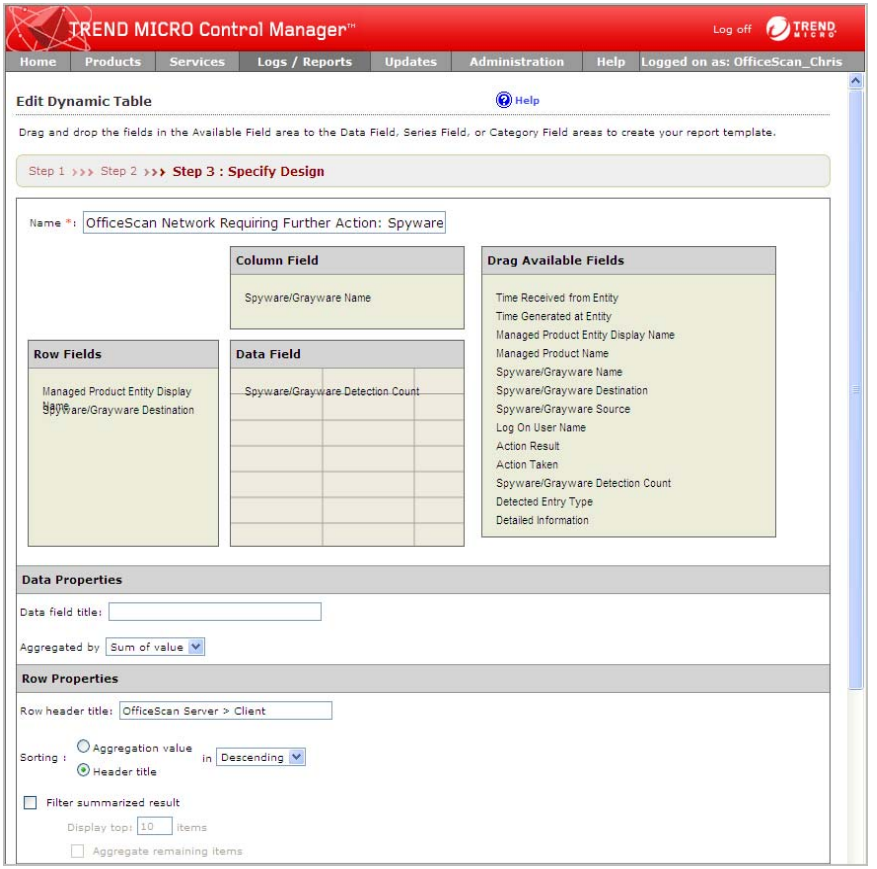
   a. Type the following in the **Label name** field:

      Further Action Required

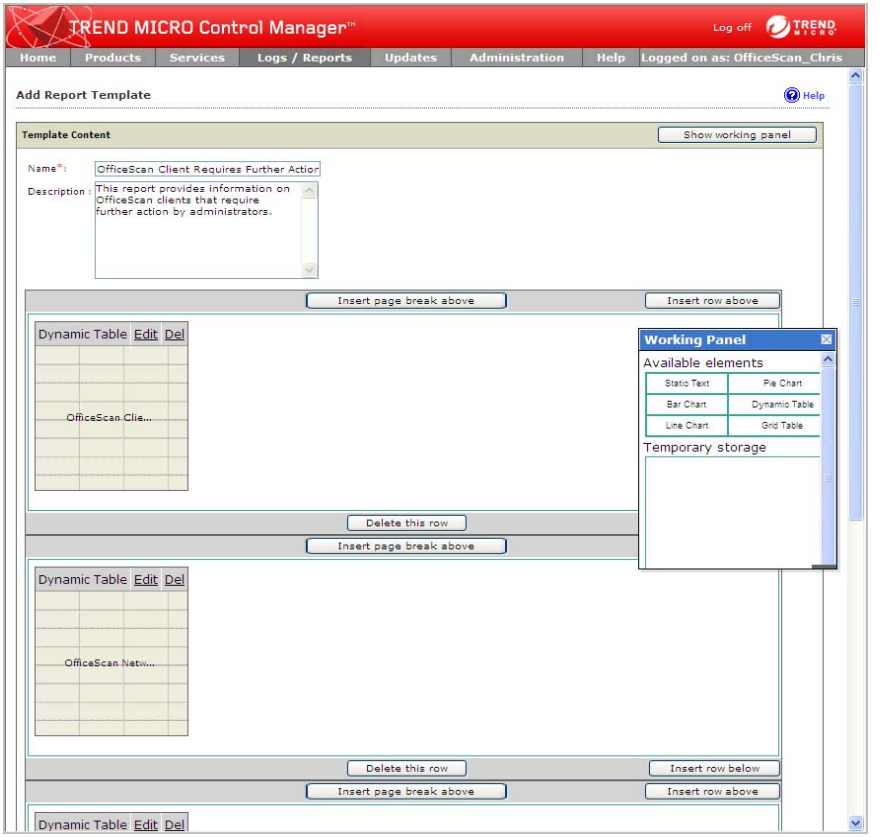
   b. Select the following from the **Sorting** drop-down lists:

      Aggregation value > Descending

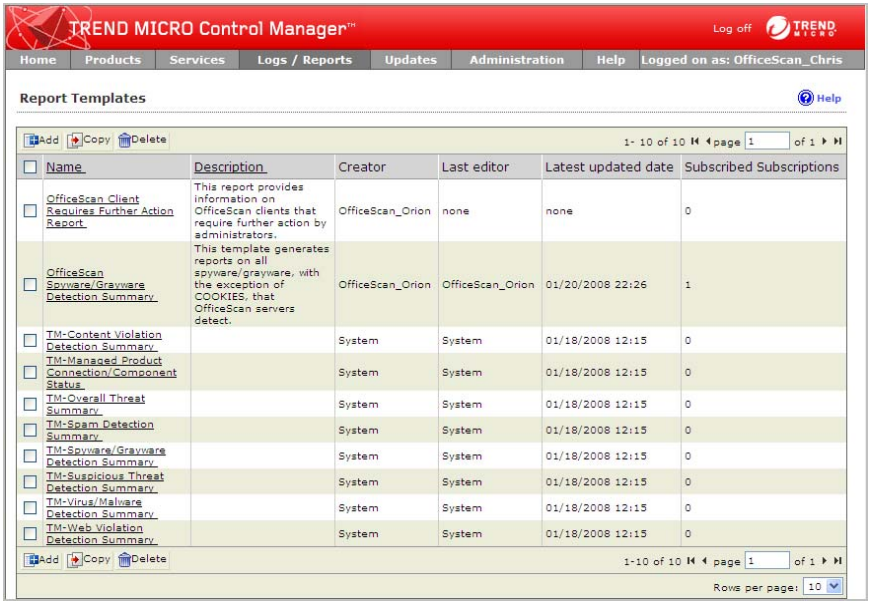
The Edit Dynamic Table screen appears as follows after completing the steps for the screen.



8. Click **Save**. The Add Report Template screen appears.



9. Click **Save.** The Report Templates screen appears with the modified template appearing at the top of the Report Template list.



Viewing the Generated Report

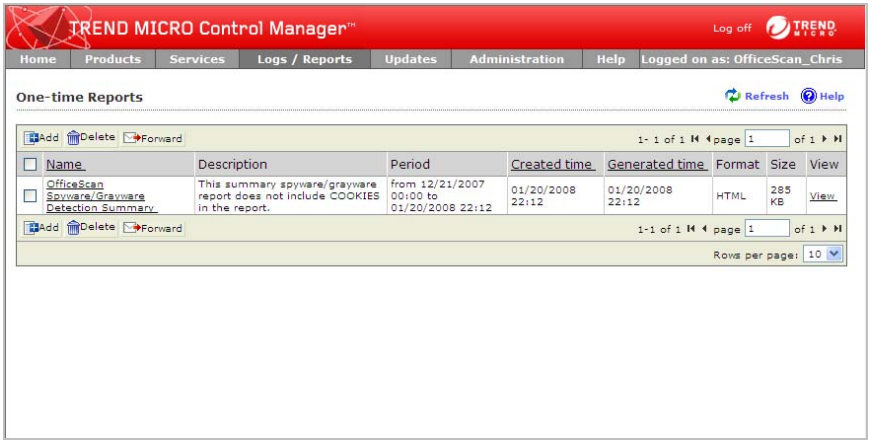
After modifying the template, Chris wants to see how the report would look. Again, to quickly view a report using this template, Chris needs to create a one-time report. Chris would also like to gather feedback from other OfficeScan administrators and his boss on the layout of the report. He will email the report, when the report completes generation, to his boss and the other OfficeScan administrators.

To add a one-time report:

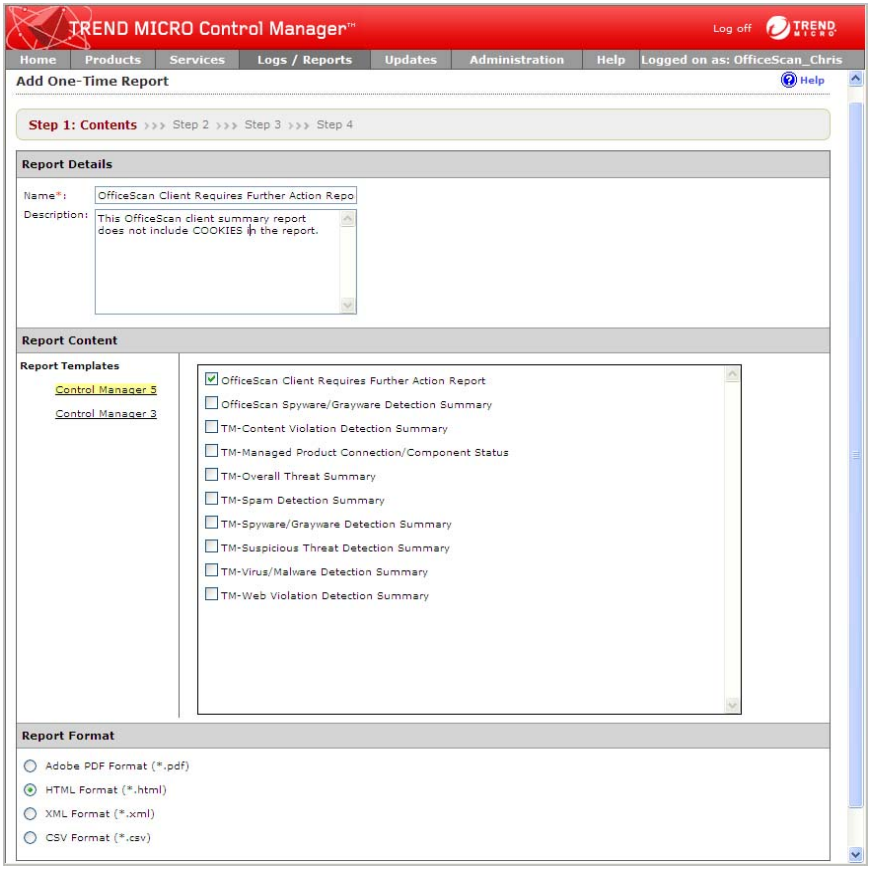
Step 1: Access the Add One-time Report screen and select the report type:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.

3. Click **One-time Reports** from the menu. The One-time Reports screen appears.



4. Click **Add**. The Add One-time Report > Step 1: Contents screen appears.



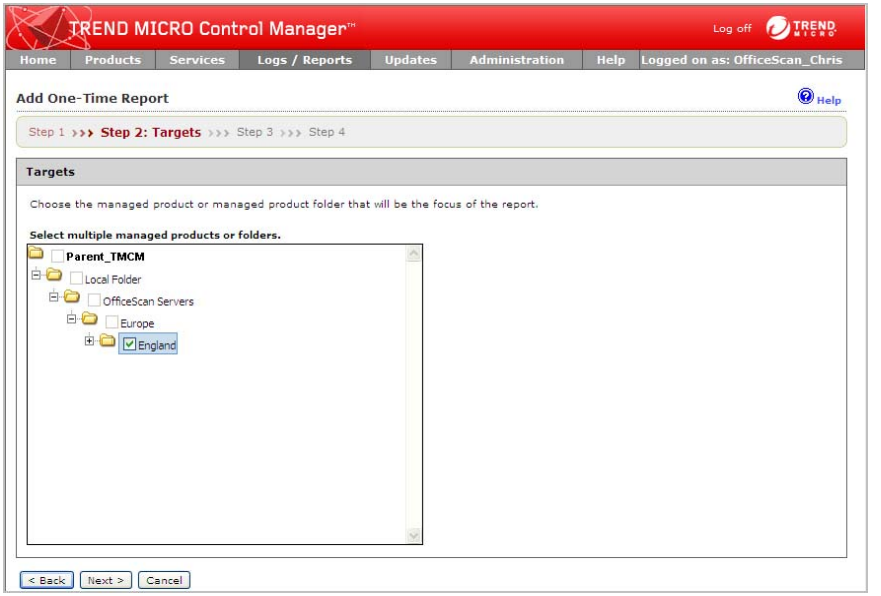
5. Type the following in the **Name** field, under Report Details:

   OfficeScan Client Requires Further Action Report

6. Type the following in the **Description** field, under Report Details:

   This OfficeScan client summary report does not include COOKIES in the report.

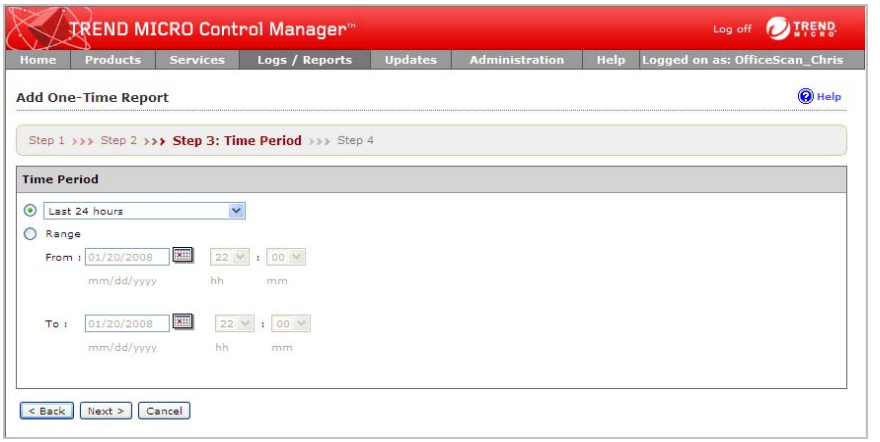
7. Select the **OfficeScan Client Requires Further Action Report** Control Manager template to generate the report:
8. Select **HTML Format (*.html)** for the report generation format:
9. Click **Next**. The Add One-Time Report > Step 2: Targets screen appears.



Step 2: Specify the product/products from which the report data generates:

1. Select **England** from the Product Directory.

2. Click **Next**. The Add One-Time Report > Step 3: Time Period screen appears.



Step 3: Specify the date that the product/products produced the data:

1. Specify the data generation date:

   From the drop-down list select one of the following:

   - All dates
   - Last 24 hours
   - Today
   - Last 7 days
   - Last 14 days
   - Last 30 days

   Specify a date range:

   a. Type a date in the **From** field.

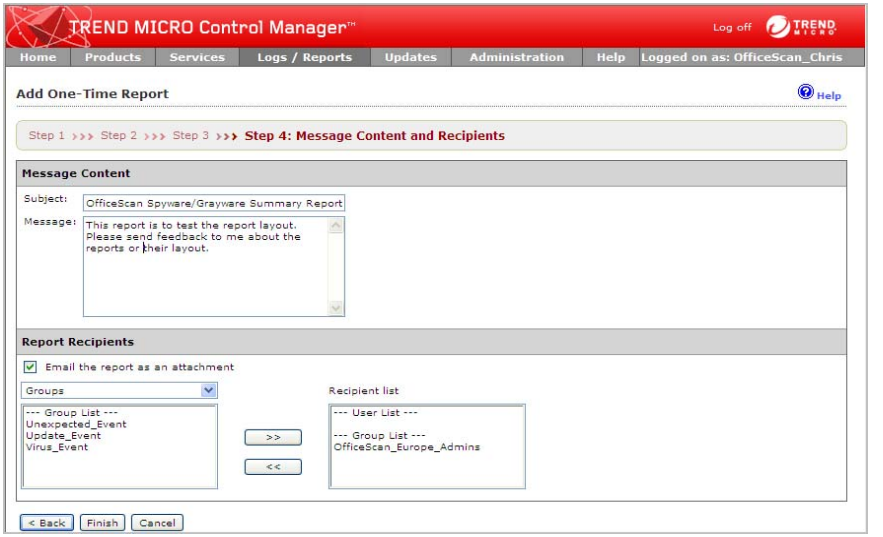
   b. Specify a time in the accompanying **hh** and **mm** fields.

   c. Type a date in the **To** field.

   d. Specify a time in the accompanying **hh** and **mm** fields.

Tip: Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**. The Add One-time Report > Step 4: Message Content and Recipients screen appears.



Step 4: Specify the email content and recipients of the report:

1. Type the following in the **Message** field:

   OfficeScan Spyware/Grayware Summary Report Test

2. Type the following in the **Message** field:

   This report is to test the report layout. Please send feedback to me about the reports or their layout.

3. Select **Email the report as an attachment**.

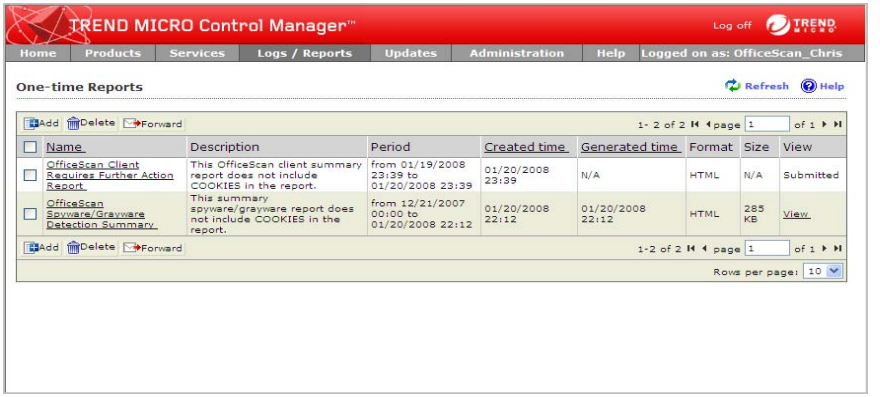
4. Add the following users to the **Report Recipients** list:

   Groups:

   - **OfficeScan_Europe_Admins**

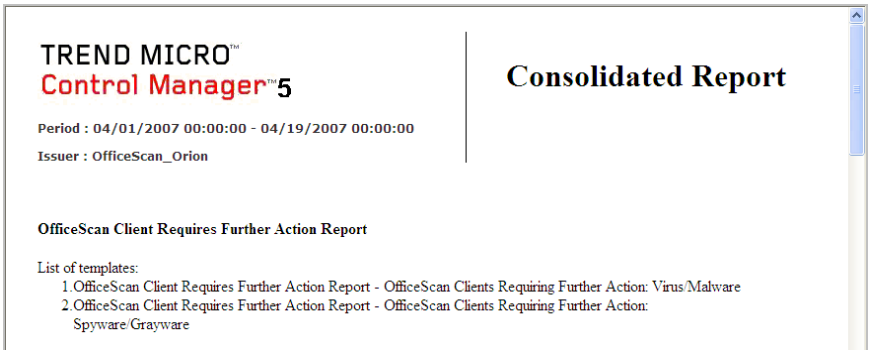
This report is for administrators not managers. Dana does not need to comment on this report.

5. Click **Finish**. The One-time Reports screen appears with the report in the One-time Reports list.



After report generation completes successfully **View** appears under the View column.

6. Click **View.** The Internet browser on your computer opens to display the HTML report. Each of the following figures corresponds to one of the report template elements. The settings for each template element are provided so you will have a better idea about how reports generate.



.

TABLE 4-20. OfficeScan Clients Requiring Further Action: Virus/Malware Dynamic Table

OfficeScan Clients Requiring Further Action: Virus/Malware

OfficeScan Server > Client		Further Action Required					
		Unable to quarantine file	File quarantined	File cleaned	Unable to upload file	File passed	Grand total
EN-OfficeScan_01	EN-ChrisFox01	3082	0	1	0	0	3083
	EN-ShellyTom s01	2381	0	0	0	0	2381
	EN-Sam Michaels02	991	17	99	0	0	1107
	EN-JohnSim s01	192	0	0	0	0	192
	EN-KayFederx60	9	0	180	0	0	189
	EN-TonyHenry02	100	11	39	0	0	150
	EN-EdwardJohn01	77	0	0	0	0	77
	EN-SarahSim pson	64	0	0	0	0	64
EN-OfficeScan_01 Total		6896	28	319	0	0	7243
EN-OfficeScan_02	EN-TaraMichaels01	51	1096	0	0	0	1147
	EN-JenTalverx60	932	62	0	0	0	994
	EN-JakeStyles02	0	146	2	0	0	148
	EN-BartCom bs01	111	65	0	0	0	176
	EN-HaroldPots02	109	1	0	0	0	110
EN-OfficeScan_02 Total		1203	1370	2	0	0	2575
EN-OfficeScan_03	EN-JadeHsux40	35	0	0	0	0	35
	EN-MaryMitchel01	32	0	0	0	0	32
	EN-PaulNichols02	30	0	0	0	0	30
	EN-PaulaJam es01	30	0	0	0	0	30
EN-OfficeScan_03 Total		127	0	0	0	0	127
Grand total		8226	1398	321	0	0	9945

Data view:

- Detailed Overall Virus/Malware Information

Query Criteria:

- Action Result > is equal to > Further action required

Data Properties:

- Virus/Malware Detection Count
- Aggregated by: Sum of value

Row Properties:

- Managed Product Entity Display Name + Infection Destination
- Label name: OfficeScan Server > Client
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Action Taken
- Label name: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-21. OfficeScan Network Requiring Further Action: Virus/Malware Dynamic Table

OfficeScan Network Requiring Further Action: Virus/Malware							
		Further Action Required					
OfficeScan Server > Client		BKDR_RASBA.C	WORM_NUWAR.AOK	TROJ_Generic	WORM_NUWAR.ZIP	JS_KAKWORM.A	Grand total
EN-OfficeScan_01	EN-SaraRosum01	2380	0	0	0	0	2380
	EN-JessSams01	0	0	479	0	0	479
	EN-BobJohns01	0	0	27	0	259	286
EN-OfficeScan_01 Total		2380	0	506	0	259	3145
EN-OfficeScan_02	EN-CarlaJames01	0	1147	0	0	0	1147
	EN-SeanConner01	0	814	0	0	0	814
	EN-MikeGerrardx60	0	3	0	130	0	133
	EN-JimWu02	0	128	0	20	0	148
	EN-TimHsu01	0	9	0	103	0	112
	EN-CathyMarks01	0	4	0	61	0	65
	EN-JohnWright02	0	1	0	58	0	59
EN-OfficeScan_02 Total		0	2106	0	372	0	2478
EN-OfficeScan_03	EN-RitaHoggx60	0	0	3	0	0	3
	EN-CarolRons01	0	0	0	1	0	1
	EN-LeslyYeh02	0	0	0	1	0	1
	EN-BelleSams01	0	0	0	0	1	1
EN-OfficeScan_03 Total		0	0	3	2	1	6
Grand total		2380	2106	509	374	260	5629

Data view:

- Detailed Overall Virus/Malware Information

Query Criteria:

- Action Result > is equal to > Further action required

Data Properties:

- Virus/Malware Detection Count
- Aggregated by: Sum of value

Row Properties:

- Managed Product Entity Display Name + Infection Destination
- Label name: OfficeScan Server > Client
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Virus/Malware Name
- Label name: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-22. OfficeScan Clients Requiring Further Action: Spyware/Grayware Dynamic Table

OfficeScan Clients Requiring Further Action: Spyware/Grayware						
		Further Action Required				
OfficeScan Server > Client		Unable to quarantine file	File quarantined	File deleted	File cleaned	Grand total
EN-OfficeScan_01	EN-OscarBell01	378	0	0	0	378
	EN-JenGerod02	313	0	0	0	313
	EN-RonWu01	107	0	0	0	107
	EN-BruceKent01	26	1	6	0	33
EN-OfficeScan_01	Total	901	15	6	1	923
EN-OfficeScan_02	EN-NinaMoorex60	0	22	0	0	22
	EN-JamesHo01	3	0	0	0	3
	EN-GinSherry02	2	1	0	0	3
	EN-AlexToms01	2	0	0	0	2
	EN-EmmaWicksx60	1	1	0	0	2
EN-OfficeScan_02	Total	8	24	0	0	32
EN-OfficeScan_03	EN-SamFox01	6	0	0	0	6
Total		6	0	0	0	6
Grand total		915	39	8	1	963

Data view:

- Detailed Overall Spyware/Grayware Information

Query Criteria:

- Security Risk Type > is equal to > Non-cookie types
- Action Result > is equal to > Further action required

Data Properties:

- Spyware/Grayware Detection Count
- Aggregated by: Sum of value

Row Properties:

- Managed Product Entity Display Name + Spyware/Grayware Destination
- Label name: OfficeScan Server > Client
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Action Taken
- Label name: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-23. OfficeScan Network Requiring Further Action: Spyware/Grayware Dynamic Table

OfficeScan Network Requiring Further Action: Spyware/Grayware							
		Further Action Required					
OfficeScan Server > Client		DIAL_AGENT.IVC	ADW_APROPOS.51	ADW_LOOK2ME.C	SPYW_PROAGENT.20	ADW_SLAGENT.A	Grand total
EN-OfficeScan_01	EN-OscarBell01	378	0	0	0	0	378
	EN-JenGerod02	0	27	14	0	0	41
	EN-RonWu01	0	0	10	21	18	49
	EN-CindyLiu01	0	0	0	0	0	0
EN-OfficeScan_01 Total		378	27	24	21	18	468
EN-OfficeScan_02	EN-NinaMoorex60	0	0	0	0	0	0
	EN-GinSherry02	0	0	0	0	0	0
	EN-EmmaWicksx60	0	0	0	0	0	0
	EN-AlexToms01	0	0	0	0	0	0
	EN-JamesHo01	0	0	0	0	0	0
EN-OfficeScan_02 Total		0	0	0	0	0	0
EN-OfficeScan_03	EN-SamFox01	0	0	0	0	0	0
EN-OfficeScan_03 Total		0	0	0	0	0	0
Grand total		378	27	24	21	18	468

Data view:

- Detailed Overall Spyware/Grayware Information

Query Criteria:

- Security Risk Type > is equal to > Non-cookie types
- Action Result > is equal to > Further action required

Data Properties:

- Spyware/Grayware Detection Count
- Aggregated by: Sum of value

Row Properties:

- Managed Product Entity Display Name + Spyware/Grayware Destination
- Label name: OfficeScan Server > Client
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Spyware/Grayware Name
- Label name: Further Action Required
- Sorting: Aggregation value > Descending

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a scheduled report is similar for all report types:

1. Access the Add Scheduled Report screen and select the report type.
2. Specify the product/products from which the report data generates.

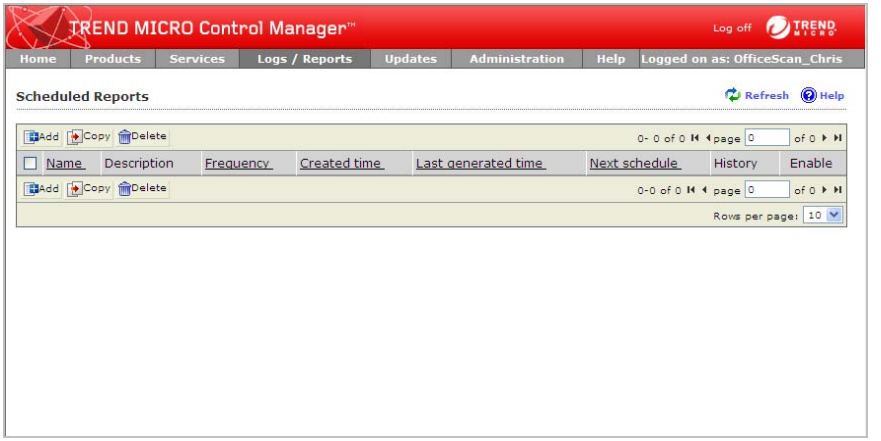
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Chris has gathered all feedback for the two reports he created. He is ready to have these reports generate on a schedule. The **OfficeScan Spyware/Grayware Detection Summary** only needs to be generated on a monthly basis. However, Chris wants to generate the **OfficeScan Requires Further Action Report** daily.

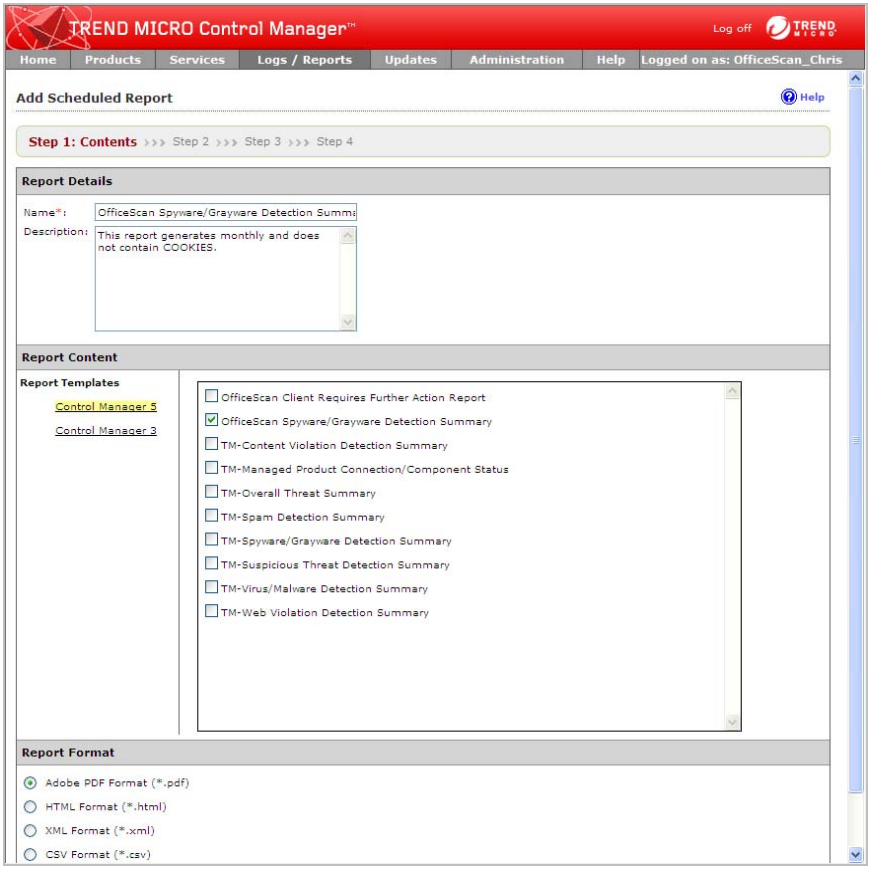
To add OfficeScan Spyware/Grayware Detection Summary as a scheduled report:

Step 1: Access the Add Scheduled Report screen and select the report type:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Scheduled Reports** from the menu. The Scheduled Reports screen appears.

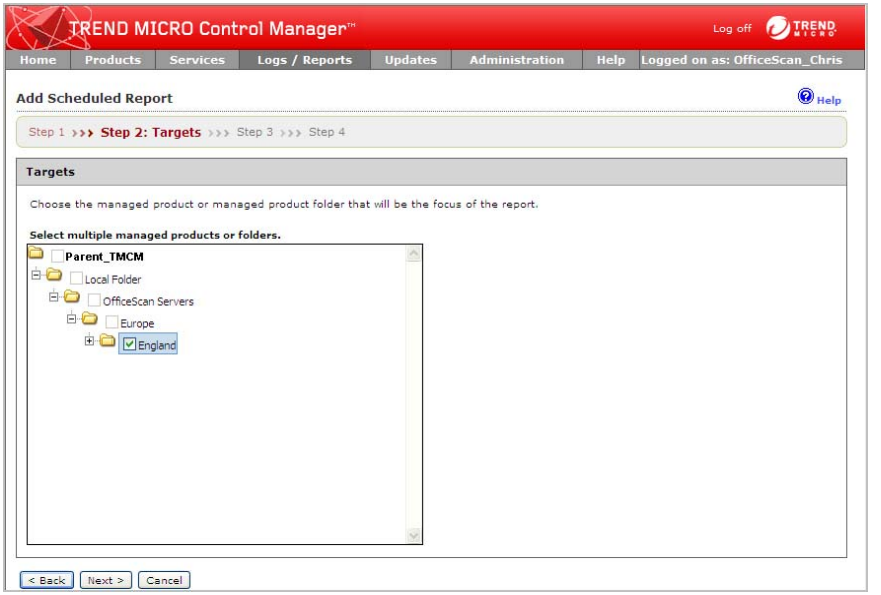


4. Click **Add**. The Add Scheduled Report > Step 1: Contents screen appears.



5. Type the following in the **Name** field:
   OfficeScan Spyware/Grayware Detection Summary
6. Type the following in the **Description** field:
   This report generates monthly and does not contain COOKIES.
7. Select the **OfficeScan Spyware/Grayware Detection Summary**.
8. Select **Adobe PDF Format (*.pdf)**.

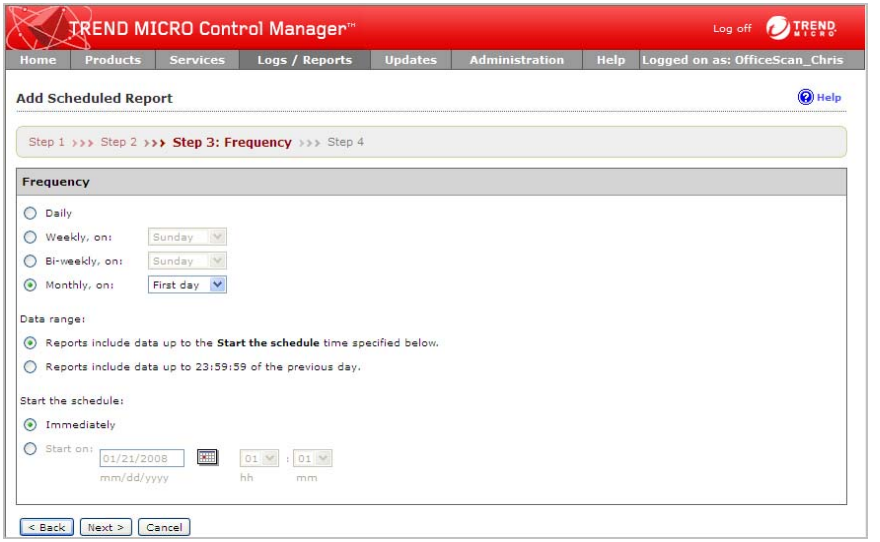
9. Click **Next**. The Add Scheduled Report > Step 2: Targets screen appears.



Step 2: Specify the product/products from which the report data generates:

1. Select **England** from the Product Directory.

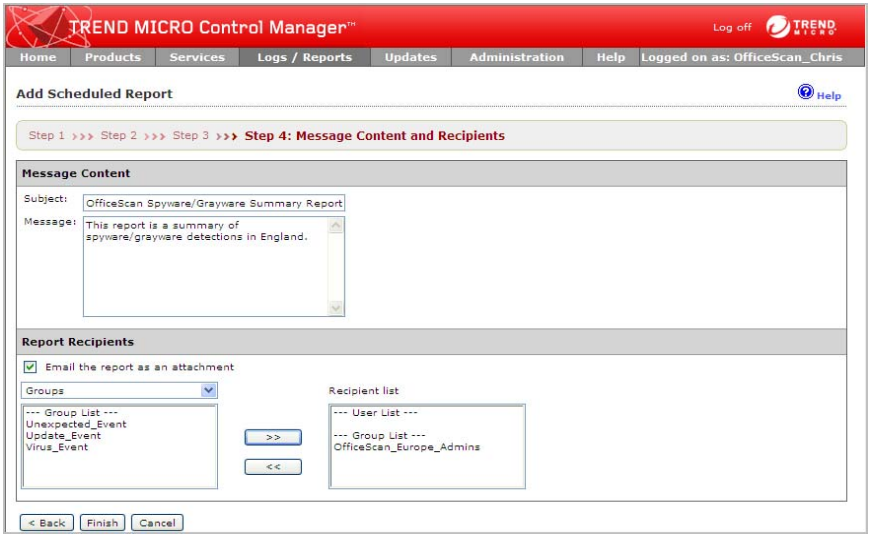
2. Click **Next**. The Add Scheduled Report > Step 3: Frequency screen appears.



Step 3: Specify the date that the product/products produced the data:

1. Select **Monthly** > **First day**.
2. Select **Reports include data up to the Start the schedule time specified below**.
3. Select **Immediately**.

4. Click **Next**. The Add Scheduled Report > Step 4: Message Content and Recipients screen appears.



Step 4: Specify the recipient of the report

1. Type the following in the **Subject** field:

   Monthly OfficeScan Spyware/Grayware Summary Report
2. Type the following in the **Message** field:

   This report is a summary of spyware/grayware detections in England.
3. Select **Email the report as an attachment**.
4. Add the following users to the **Report Recipients** list:

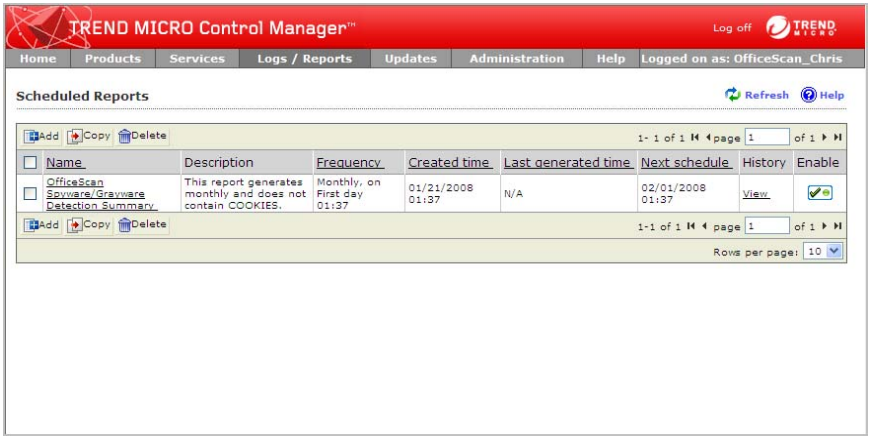
   Users:

   - **OfficeScan_Dana**

   Groups:

   - **OfficeScan_Europe_Admins**

5. Click **Finish**. The Scheduled Reports screen appears with the report in the Scheduled Reports list.

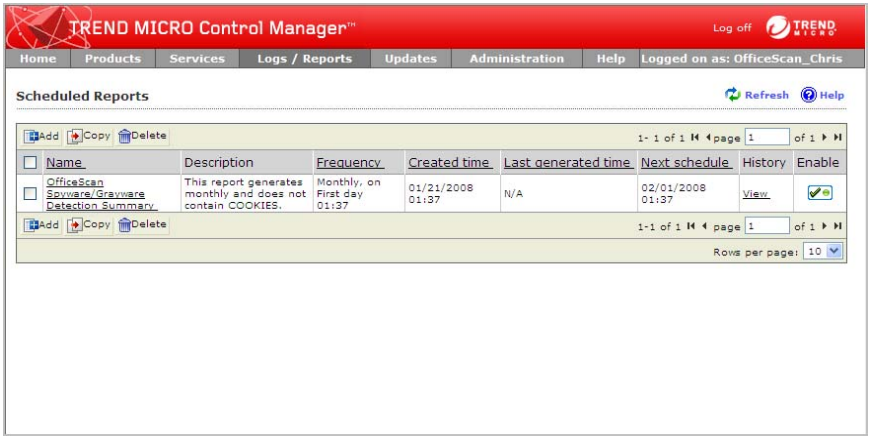


To add OfficeScan Requires Further Action Report as a scheduled report:

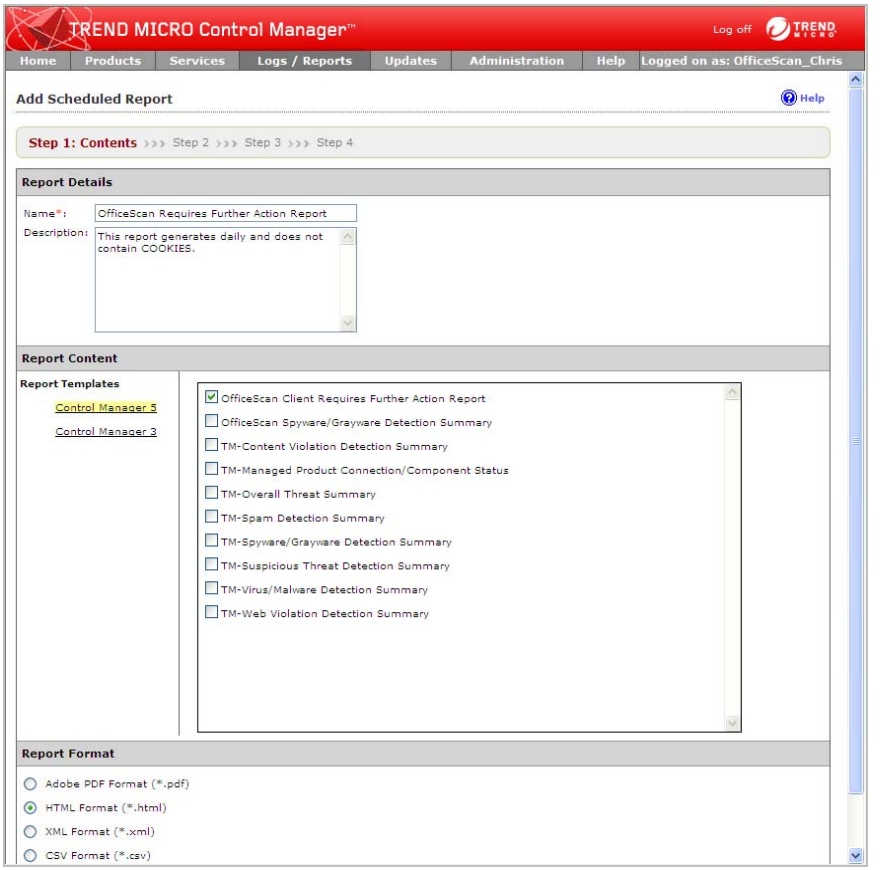
Step 1: Access the Add Scheduled Report screen and select the report type:

1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.

3. Click **Scheduled Reports** from the menu. The Scheduled Reports screen appears.

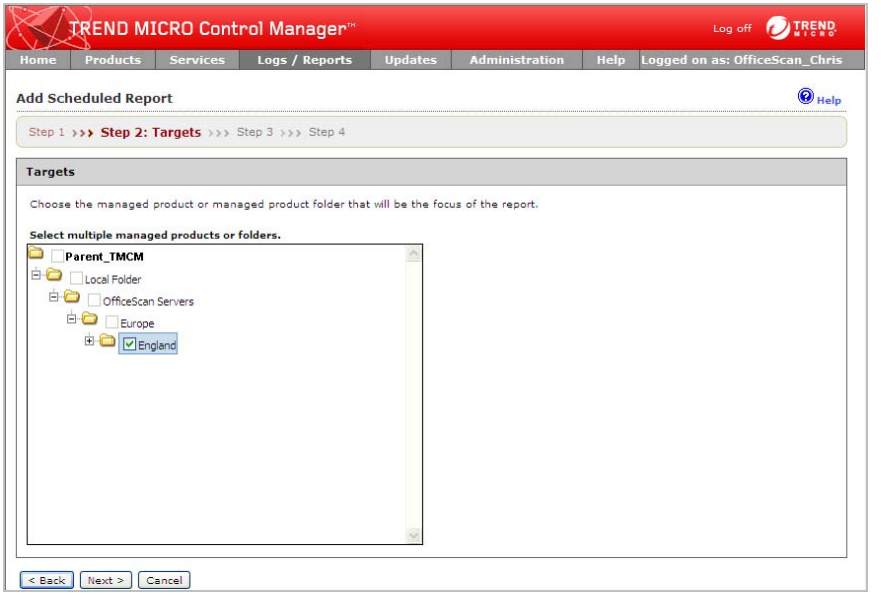


4. Click **Add**. The Add Scheduled Report > Step 1: Contents screen appears.



5. Type the following in the **Name** field:
   OfficeScan Requires Further Action Report
6. Type the following in the **Description** field:
   This report generates daily and does not contain COOKIES.
7. Select the **OfficeScan Client Requires Further Action Report**.
8. Select **HTML Format (*.html)**.

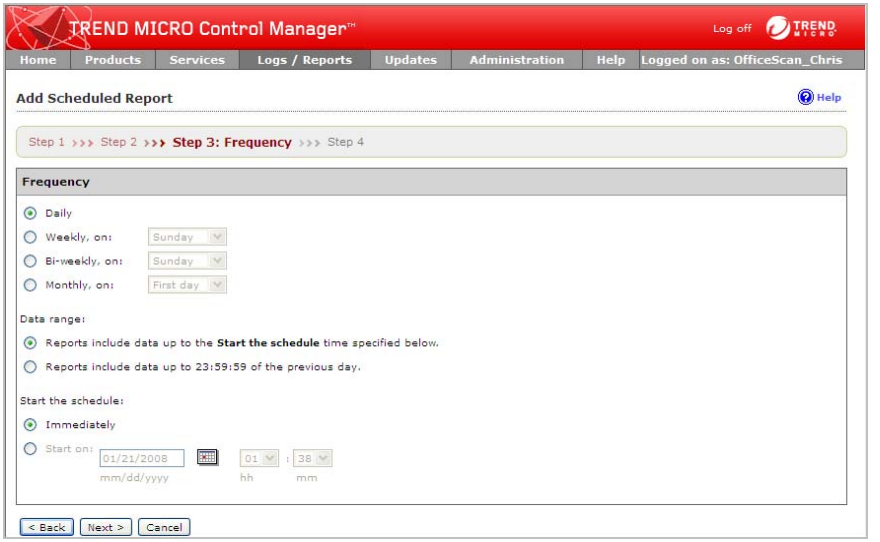
9. Click **Next**. The Add Scheduled Report > Step 2: Targets screen appears.



Step 2: Specify the product/products from which the report data generates:

1. Select **England** from the Product Directory.

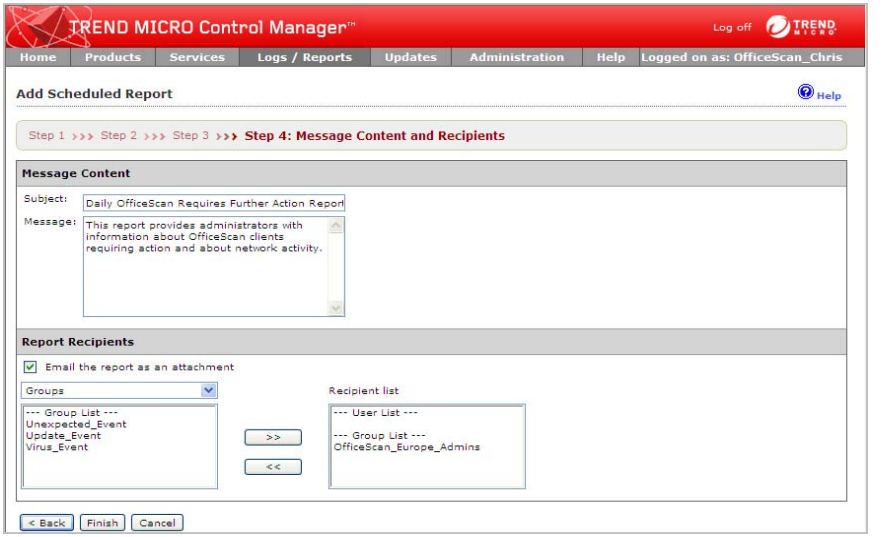
2. Click **Next**. The Add Scheduled Report > Step 3: Frequency screen appears.



Step 3: Specify the date that the product/products produced the data:

1. Select **Daily**.
2. Select **Reports include data up to the Start the schedule time specified below**.
3. Select **Immediately**.

4. Click **Next**. The Add Scheduled Report > Step 4: Message Content and Recipients screen appears.



Step 4: Specify the recipient of the report

1. Type the following in the **Subject** field:

   Daily OfficeScan Requires Further Action Report

2. Type the following in the **Message** field:

   This report provides administrators with information about OfficeScan clients requiring action and about network activity.

3. Select **Email the report as an attachment**.

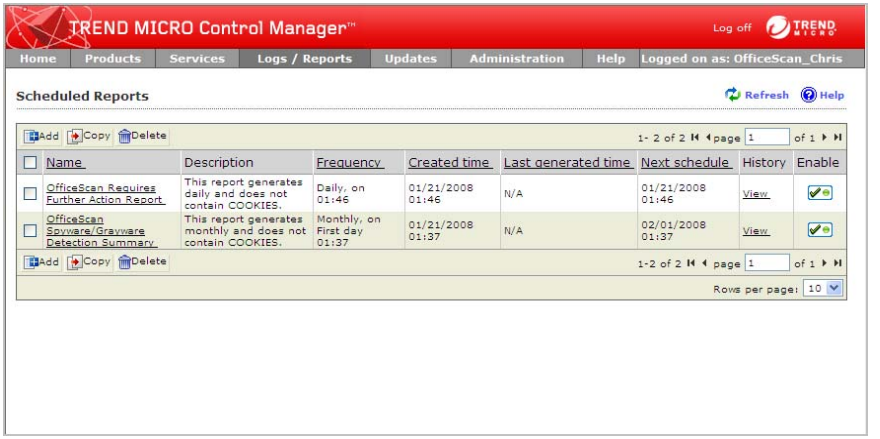
4. Add the following users to the **Report Recipients** list:

   Chris does not send this report to Dana because she is not an administrator.

   Groups:

   - **OfficeScan_Europe_Admins**

5. Click **Finish**. The Scheduled Reports screen appears with the report in the Scheduled Reports list.



Enabling/Disabling Scheduled Reports

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it through the Scheduled Reports screen.

To enable/disable scheduled reports:

1. Mouseover **Logs/Reports**. A drop-down menu appears.
2. Select **Scheduled Reports** from the drop-down menu. The Scheduled Reports screen appears.
3. Click the enabled/disabled icon in the **Enabled** column of the Scheduled Reports table. A disabled/enabled icon appears in the column.

Viewing Generated Reports

Aside from sending reports as email attachments, view generated reports from one of these areas:

- One-time Reports

- Scheduled Reports

To view reports:

1. Mouseover **Logs/Reports** from the main menu. A drop-down menu appears.
2. Select one of the following from the drop-down menu:

   One-time Reports:

   a. Click **One-time Reports** from the drop-down menu. The One-time Reports screen appears.

   b. Click the link for the report you want to view from the **View** column.

   Scheduled Reports:

   a. Click **Scheduled Reports** from the drop-down menu. The Scheduled Reports screen appears.

   b. Click the link for the report you want to view from the **History** column. The History screen for that report appears.

   c. Select the report to view from the History screen.

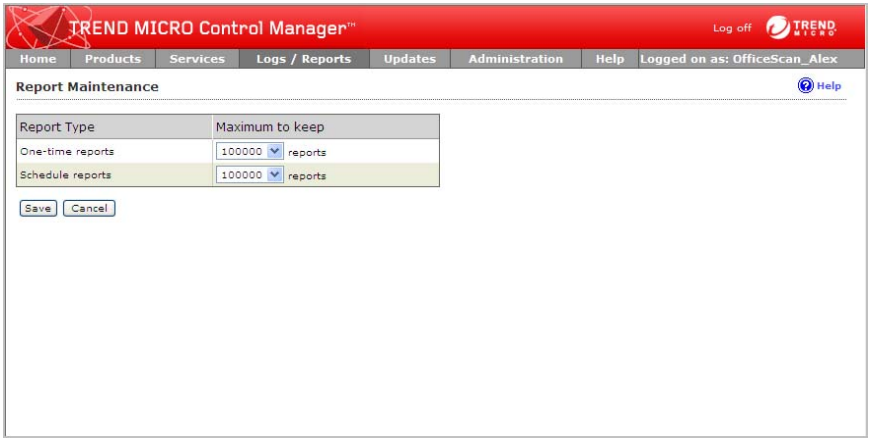
Configuring Report Maintenance

Alex wants to keep all reports for at least a year. She is not sure how many reports she will generate in a year, so she will set the value at the maximum that Control Manager allows.

To configure report maintenance:

1. Log on to the Control Manager Web console as **Alex**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Mouseover **Settings**. A sub-menu appears.

4. Select **Report Maintenance**. The Report Maintenance screen appears.



5. Specify the following for **One-time reports** and **Scheduled reports**:
   100000
6. Click **Save**.

Chapter 5

Administering Managed Products

This chapter presents material administrators will need to manage the Control Manager network. Topics introduced in this chapter are as follows:

Administering Managed Products From the Product Directory

Manually Deploying New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. Use this method of updating components during virus outbreaks.

Download new components before deploying updates to specific or groups of managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu. The Product Directory screen appears.
2. Select a managed product or directory from the Product Directory. The managed product or directory highlight.
3. Mouseover **Tasks** from the Product Directory menu. A drop-down menu appears.
4. Select **Deploy <component>** from the drop-down menu.
5. Click **Next>>**.
6. Click **Deploy Now** to start the manual deployment of new components.
7. Monitor the progress through the Command Tracking screen.
8. Click the **Command Details** link in the Command Tracking screen to view details for the Deploy Now task.

View 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.

There are two ways to view the managed products status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This

summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or managed product.
   - If you click a managed product, the Product Status tab displays the managed product's summary
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries

---

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configuring Managed Products

Depending on the product and agent version:

- You can configure products either individually or in groups according to folder division

  Perform group configuration using the folder Configuration tab.

Note: When performing a group configuration, verify that you want all managed product in a group to have the same configuration. Otherwise, add managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration screen shows either the product's Web console or a Control Manager-generated console

To configure a product:

1. Access the Product Directory.
2. Select the desired managed product from the Product Directory. The product status appears in the right-hand area of the screen.

3. Mouseover **Configuration** from the Product Directory menu. A drop-down menu appears.
4. Select **<Product Name>** from the drop-down menu. The managed product Web-based console or Control Manager-generated console appears. Configure the product.

Note: For additional information about configuring managed products, refer to the managed product's documentation.

To configure a group of managed products:

1. Access the Product Directory.
2. Select the desired managed products or folder from the Product Directory. The product status appears in the right-hand area of the screen.
3. Mouseover **Configuration** from the Product Directory menu. A drop-down menu appears.
4. Select **<Product Name>** from the drop-down menu. The managed product Web-based console or Control Manager-generated console appears. Configure the products.

Issuing Tasks to Managed Products

Use the Tasks tab to invoke available actions to 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/cleanup templates
- Deploy program files
- Enable/Disable Real-time Scan
- Start Scan Now

Deploy the latest spam rule, pattern, or scan engine to managed products with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to managed products:

1. Access the Product Directory.
2. Select the managed product or directory to issue a task.
3. Mouseover **Tasks**. A drop-down menu appears.
4. Click a task from the list. Monitor the progress through Command Tracking. Click the Command Details link at the response screen to view command information.

Querying and Viewing Managed Product Logs

Use the Logs tab to query and view logs for a group or specific managed product.

To query and view managed product logs:

1. Access the Product Directory.
2. Select the desired managed product or folder from the Product Directory.
3. Mouseover **Logs** in the Entity Tree menu. A drop-down list appears.
4. Click **Logs** from the drop-down menu. The Select Data View Step 1: Select Data View screen appears.
5. Specify the data view for the log:
   a. Select the data to query from the Available Data Views area.
   b. Click **Next**. The Step 2: Query Criteria screen appears.
6. Specify the filter criteria for the log:
   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.
7. Specify the data to appear in the log and the order in which the data appears:
   a. Click **Change column display**. The Select Display Sequence screen appears.
   b. Select a query column from the Available Fields list. The selected item highlights.

      Select multiple items using the Shift or Ctrl keys.

c. Click **>** to add items to the Selected Fields list.

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.

8. To save the query:
   a. Click **Save this query to the saved Ad Hoc Queries list**.
   b. Type a name for the saved query in the **Query Name** field.
9. Click **Query**. The Results screen appears.

Searching for Managed Products, Product Directory Folders or Computers

Use the Search button to quickly find and locate a specific managed product in the Product Directory.

To search for a folder or managed product:

1. Access the Product Directory.
2. Type the entity display name of the managed product in the Find Entity field.
3. Click **Search**.

To perform an advanced search:

1. Access the Product Directory.
2. Click **Advanced Search**. The Advanced Search screen appears.
3. 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.
4. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
5. Click **Query** to start searching. Search results appear in the Search Result folder of the Product Directory.

Refreshing the Product Directory

To refresh the Product Directory:

- In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Activating and Registering your Managed Products

To use the functionality of Control Manager 5.0, managed products (OfficeScan, ScanMail for Microsoft Exchange), and other services (Outbreak Prevention Services, Damage Cleanup Services, or Vulnerability Assessment), you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key that you use to register your software online to the Trend Micro Online Registration Web site and obtain an Activation Code.

As managed products register to Control Manager, the managed products add their Activation Codes to the managed product Activation Code list on the Managed Product License Management screen. Administrators can add new Activation Codes to the list and redeploy renewed Activation Codes.

- Activation Code Characteristics
- Created in real-time during registration
- Created based on Registration Key information
- Has an expiration date
- Product version independent

Note: In previous versions of Control Manager, a serial number was included with the product, and users needed to register online to use the full functionality of the software.

Activating Managed Products

Activating managed products allows you to use their full functionality, including downloading updated program components. You can activate managed products after

obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

To register and activate managed products:

1. Mouseover **Administration** from the main menu. A drop-down menu appears.
2. Mouseover **License Management** from the drop-down menu. A sub-menu appears.
3. Click **Managed Products** from the sub-menu. The Managed Products License Management screen appears.
4. Click **Add and Deploy**. The Add And Deploy A New License Step 1: Input Activation Code screen appears.
5. Type an Activation Code for the product you want to activate in the New activation code.
6. Click **Next**. The Add And Deploy A New License Step 2: Select Targets screen appears.
7. Select the managed product which to deploy the Activation Code.
8. Click **Finish**. The Managed Products License Management screen appears with the new Activation Code listed in the table.

Renewing Managed Product Licenses

Control Manager can deploy or redeploy Activation Codes to registered products from the Product Directory or from the Managed Product License Management screen.

To renew managed product licenses from the License Management screen:

1. Mouseover **Administration** from the main menu. A drop-down menu appears.
2. Mouseover **License Management** from the drop-down menu. A sub-menu appears.
3. Click **Managed Products** from the sub-menu. The Managed Products License Management screen appears.
4. Select an Activation Code from the list.
5. Click **Re-Deploy**. The Re-Deploy License screen appears.
6. Select a product or directory from the Product Directory.
7. Click **Save**.

Note: If no products appear in the list, the selected Activation Code does not support any products currently registered to Control Manager.

To renew managed product licenses from the Product Directory:

1. Access the Product Directory.
2. Select a managed product from the Product Directory tree.
3. Click **Tasks** from the Product Directory menu. A drop-down menu appears.
4. From the list of tasks, select **Deploy license profiles**.
5. Select a product from the Supported Products list and click the **Next >>** button to open the License Profiles screen.
6. On the License Profiles screen, click the **Deploy Now** link to make Control Manager load updated license information from the Trend Micro license server. Control Manager then deploys the license profiles automatically.
7. Click the Command Details link to open the Command Details screen, where you can review when Control Manager deployed the license profiles, the time of the last report, the user who authorized the deployment, and a breakdown of deployments in progress and successfully or unsuccessfully completed. You can also see a list of deployments by server.

Activating Control Manager

Activating Control Manager allows you to use its full functionality, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Tip: After activating Control Manager, log off and then log on for changes to take effect.

To register and activate Control Manager:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.

4. On the working area under **Control Manager License Information**, click the **Activate the product** link.
5. Click the **Register online** link and follow the instructions on the Online Registration Web site.
6. In the **New box**, type your Activation Code.
7. Click **Activate**.
8. Click **OK**.

Renewing Control Manager or Managed Service Maintenance

Renew maintenance for Control Manager or its integrated related products and services (that is, Outbreak Prevention Services, Vulnerability Assessment, or Damage Cleanup Services) using one of the following methods.

Make sure you already have obtained an updated Registration Key to acquire a new Activation Code to renew your product or service maintenance.

To renew maintenance using Check Status Online:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager** from the sub-menu. The License Information screen appears.
4. On the working area under the product or service to renew, click **Check Status**.
5. Click **OK**.

Note: Log off and then log on to the management console for changes to take effect.

To renew maintenance by manually entering an updated Activation Code:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager** from the sub-menu. The License Information screen appears.

4. On the working area under the product or service to renew, click the **Specify a new Activation Code** link (to obtain an Activation Code, click the Register online link and follow the instructions on the Online Registration Web site).
5. In the **New box**, type your Activation Code.
6. Click **Activate**.
7. Click **OK**.

Note: Log off and then log on to the management console for changes to take effect.

Chapter 6

Removing Trend Micro Control Manager

This chapter contains information about how to remove Control Manager components from your network, including the Control Manager server, Control Manager agents, and other related files.

This chapter contains the following sections:

Removing a Control Manager Server

You have two ways to remove Control Manager automatically (the following instructions apply to a Windows 2000 environment; details may vary slightly, depending on your Microsoft Windows platform):

- From the Start menu, click **Start** > **Programs** > **Trend Micro Control Manager** > **Uninstalling Trend Micro Control Manager**.
- Using Add/Remove Programs:
  - **a.** Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
  - **b.** Select **Trend Micro Control Manager**, and then click **Remove**.

    This action automatically removes other related services, such as the Trend Management Infrastructure and Common CGI services, as well as the Control Manager database.
  - **c.** Click **Yes** to keep the database, or **No** to remove the database.

Note: Keeping the database allows you to re-install Control Manager on the server and retain all system information, such as agent registration, and user account data.

If you re-installed the Control Manager server, and deleted the original database, but did not remove the agents that originally reported to the previous installation then the agents will re-register with the server when:

- Managed product servers restart the agent services
- Control Manager agents re-verify their connection after an 8-hour period

Manually Removing Control Manager

This section describes how to remove Control Manager manually. Use the procedures below only if the Windows Add/Remove function or the Control Manager uninstall program is unsuccessful.

Note: Windows-specific instructions may vary between operating system versions. The following procedures are written for Windows 2000.

Removing Control Manager actually involves removing distinct components. These components may be removed in any order; they may even be removed together. However, for purposes of clarity, the uninstallation for each module is discussed individually, in separate sections. The components are:

- Control Manager application
- Trend Micro Management Infrastructure
- Common CGI Modules
- Control Manager Database (optional)

Other Trend Micro products also use the Trend Micro Management Infrastructure and Common CGI modules, so if you have other Trend Micro products installed on the same machine, Trend Micro recommends not removing these two components.

Note: After removing all components, you must restart your server. You only have to do this once — after completing the removal.

Removing the Control Manager Application

Manual removal of the Control Manager application involves the following steps:

1. Stopping Control Manager Services.
2. Removing Control Manager IIS Settings.
3. Removing Crystal Reports, TMI, and CCGI.
4. Deleting Control Manager Files/Directories and Registry Keys.
5. Removing the Database Components.
6. Removing Control Manager and NTP Services.

Stopping Control Manager Services

Use the Windows Services screen to stop all of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro CCGI
- Trend Micro Control Manager
- Trend Micro NTP

Note: These services run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

To stop Control Manager services:

1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click <Control Manager service>, and then click **Stop**.

To stop IIS and Control Manager services from the command prompt:

Run the following commands at the command prompt:

- `net stop w3svc`
- `net stop tmcm`

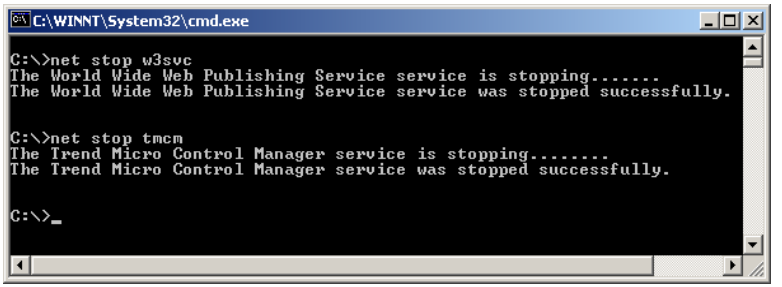


FIGURE 6-1. View of the command line with the necessary services stopped

Removing Control Manager IIS Settings

Remove the Internet Information Services settings after stopping the Control Manager services.

To remove Control Manager IIS settings:

1. From the Control Manager server, click **Start > Run**. The Run dialog box appears.
2. Type the following in the **Open** field:

   %SystemRoot%\System32\mmc.exe %SystemRoot%\System32\Inetsrv\iis.msc

3. On the left-hand menu, double-click the server name to expand the console tree.
4. Double-click **Default Web Site**.
5. Delete the following virtual directories:
   - ControlManager
   - TVCSDownload
   - Viewer9
   - TVCS
   - Jakarta
   - WebApp
6. Right-click the IIS Web site you set during installation.
7. Click **Properties**.
8. Click the **ISAPI Filters** tab.
9. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
10. On IIS 6 only, delete the following Web service extensions:
    - Trend Micro Common CGI Redirect Filter (If removing CCGI)
    - Trend Micro Control Manager CGI Extensions
11. Click **OK**.

Removing Crystal Reports, TMI, and CCGI

Removal of TMI and CCGI is optional. Use Add/Remove Programs to uninstall Crystal Reports.

To remove Crystal Reports:

1. On Control Manager server, click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Scroll down to Crystal Reports Runtime Files, then click **Remove** to remove the Crystal Reports related files automatically.

To remove TMI and CCGI:

- Use Microsoft's service tool Sc.exe to remove TMI and CCGI: *http://support.microsoft.com/kb/251192/en-us*

Deleting Control Manager Files/Directories and Registry Keys

To manually remove a Control Manager server:

1. Delete the following directories:
   - ...\Trend Micro\Control Manager
   - ...\Trend Micro\COMMON\ccgi
   - ...\Trend Micro\COMMON\TMI
2. Delete the following Control Manager registry keys:
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\VulnerabilityAssessmentServices
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP

Removing the Database Components

To remove Control Manager ODBC settings:

1. On the Control Manager server, click **Start > Run**. The Run dialog box appears.
2. Type the following in the **Open** field:

   odbcad32.exe
3. On the ODBC Data Source Administrator window, click the **System DSN** tab.
4. Under **Name**, select **ControlManager_Database**.
5. Click **Remove**, and click **Yes** to confirm.

To remove the Control Manager SQL Server 2005 Express database:

1. On Control Manager server, click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Scroll down to **SQL Server 2005 Express**, then click **Remove** to remove the Crystal Reports related files automatically.

Tip: Trend Micro recommends visiting Microsoft's Web site for instructions on removing SQL Server 2005 Express if you have any issues with the uninstallation: *http://support.microsoft.com/kb/909967*

Removing Control Manager and NTP Services

To remove Control Manager and NTP services:

- Use Microsoft's service tool **Sc.exe** to remove Control Manager and NTP services: *http://support.microsoft.com/kb/251192/en-us*

Appendix A

Appendix A: Understanding Data Views

Database views are available to Control Manager 5.0 report templates and to Ad Hoc Query requests.

This appendix contains the following sections:

Product Information

Product Information Data Views provide information about Control Manager, managed products, components, and product licenses.

TABLE A-1. Product Information Data Views

DATA VIEW	DESCRIPTION
Control Manager Information	Displays information about Control Manager user access, Command Tracking information, and Control Manager server events.
Managed Product Information	Displays status, detailed, and summary information about managed product or managed product clients.
Component Information	Displays status, detailed, and summary information about out-of-date and up-to-date and component deployment of managed product components.
License Information	Displays status, detailed, and summary information about Control Manager and managed product license information.

Security Threat Information

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

TABLE A-2. Security Threat Data Views

DATA VIEW	DESCRIPTION
Overall Threat Information	Displays summary and statistical data about the overall threat landscape of your network.
Virus/Malware Information	Displays summary and detailed data about malware/viruses managed products detect on your network.

TABLE A-2. Security Threat Data Views

DATA VIEW	DESCRIPTION
Spyware/Grayware Information	Displays summary and detailed data about spyware/grayware managed products detect on your network.
Content Violation Information	Displays summary and detailed data about prohibited content managed products detect on your network.
Spam Violation Information	Displays summary and detailed data about spam managed products detect on your network.
Web Violation Information	Displays summary and detailed data about Internet violations managed products detect on your network.
Policy/Rule Violation Information	Displays summary and detailed data about policy/rule violations managed products detect on your network.
Suspicious Threat Information	Displays summary and detailed data about suspicious activity managed products detect on your network.

Data Views: Product Information

Displays information about Control Manager, Managed Products, components, and licenses.

License Information

Managed Product License Status

Displays detailed information about the managed product and information about the Activation Code the managed product uses. Examples: managed product information,

whether the Activation Code is active, the number of managed products the Activation Code activates

TABLE A-3. Managed Product License Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Service	Displays the name of the managed product service. Example: Vulnerability Assessment, Outbreak Protection Service
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Activation Code	Displays the Activation Code for managed products.
Activation Code Count	Displays the number of Activation Codes a managed products uses.
License Expiration Date	Displays the date the license expires for the managed product

Managed Product License Information Summary

Displays detailed information about the Activation Code and information on managed products that use the Activation Code. Examples: seat count the Activation Code allows, trial or full product version, user-defined description about the Activation Code

TABLE A-4. Managed Product License Information Summary Data View

DATA	DESCRIPTION
Activation Code	Displays the Activation Code for managed products.
User-defined Description	Displays the user-defined description for the Activation Code.
Managed Product/Service Count	Displays the number of managed products or services that use the Activation Code.
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Managed Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
License Expiration Date	Displays the date the license expires for the managed product
Seat Count	Displays the number of seats the Activation Code allows.

Detailed Managed Product License Information

Displays information about the Activation Code and information on managed products which use the Activation Code. Examples: managed product information, evaluation or full product version, license expiration date

TABLE A-5. Detailed Managed Product License Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Service	Displays the name of the managed service. Example: Vulnerability Assessment, Web Reputation Service
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Managed Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
Activation Code	Displays the Activation Code for managed products.
License Expiration Date	Displays the date the license expires for the managed product.
Seat Count	Displays the number of seats the Activation Code allows.
Description	Displays the description for the Activation Code.

Managed Product Information

Managed Product Distribution Summary

Displays summary information about managed products registered to Control Manager. Examples: managed product name, version number, and number of managed products

TABLE A-6. Managed Product Distribution Summary Data View

DATA	DESCRIPTION
Registered to Control Manager	Displays the Control Manager server to which the managed product is registered.
Managed Product Category	Displays the threat protection category for a managed product. Example: Server-based products, Desktop products
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Managed Product Count	Displays the total number of a specific managed product a network contains.

Managed Product Status Information

Displays detailed information about managed products registered to Control Manager. Examples: managed product version and build number, operating system

TABLE A-7. Managed Product Status Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.
Managed Product MAC Address	Displays the MAC address of the server on which the managed product installs.
Managing Control Manager Entity Display Name	Displays the entity display name of the Control Manager server to which the managed product is registered.
Managing Server Entity Display Name	Displays the entity display name of the managed product server to which a client is registered.
Domain Name	Displays the domain to which the managed product belongs.
Managed Product Connection Status	Displays the managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline
Pattern File Status	Displays the status of the pattern files/rules the managed product uses. Example: up-to-date, out-of-date
Scan Engine Status	Displays the status of the scan engines the managed product uses. Example: up-to-date, out-of-date

TABLE A-7. Managed Product Status Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Build Number	Displays the build number of the managed product. This information appears on the About screen for products. Example: Version: 5.0 (**Build 1219**)
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
OS Name	Displays the operating system of the computer where the managed product installs.
OS Version	Displays the version number of the operating system of the computer where the managed product installs.
OS Service Pack	Displays the service pack number of the operating system of the computer where the managed product installs.

ServerProtect and OfficeScan Server/Domain Status Summary

Displays summary information about client/server managed products. Examples: pattern file out-of-date, scan engine out-of-date,

TABLE A-8. ServerProtect and OfficeScan Server/Domain Status Summary Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product.

TABLE A-8. ServerProtect and OfficeScan Server/Domain Status Summary Data View

DATA	DESCRIPTION
Domain Name	Displays the domain to which the managed product belongs.
Managed Server/Client Count	Displays the number of managed product servers or managed product clients.
Pattern File Out-of-Date Server/Client	Displays the number of managed product servers/clients with out-of-date pattern files.
Pattern File Up-to-Date Rate (%)	Displays the percentage of managed product servers/clients with up-to-date pattern files.
Scan Engine Out-of-Date Server/Client	Displays the number of managed product servers/clients with out-of-date scan engines.
Scan Engine Up-to-Date Rate (%)	Displays the percentage of managed product servers/clients with up-to-date scan engines.

Managed Product Event Information

Displays information relating to managed product events. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE A-9. Managed Product Event Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data about the managed product event.
Time Generated at Entity	Displays the time that the managed product generates data about the event.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE A-9. Managed Product Event Information Data View

DATA	DESCRIPTION
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Event Severity	Displays the severity of an event. Example: Information, Critical, Warning
Event Type	Displays the type of event that occurred. Example: download virus found, file blocking, rollback
Command Status	Displays the status of the command. Example: successful, unsuccessful, in progress
Description	Displays the description a managed product provides for the event.

Component Information

Managed Product Scan Engine Status

Displays detailed information about scan engines managed products use. Examples: scan engine name, time of the latest scan engine deployment, and which managed products use the scan engine

TABLE A-10. Managed Product Scan Engine Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the host name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.

TABLE A-10. Managed Product Scan Engine Status Data View

DATA	DESCRIPTION
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Scan Engine Name	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
Scan Engine Version	Displays the version of the scan engine. Example: Anti-spam Engine (Windows): **3.000.1153**, Virus Scan Engine IA 64 bit Scan Engine: **8.000.1008**
Scan Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Time of Latest Scan Engine Update	Displays the time of the latest scan engine deployment to managed products or clients.

Managed Product Pattern File/Rule Status

Displays detailed information about pattern files/rules managed products use. Examples: pattern file/rule name, time of the latest pattern file/rule deployment, and which managed products use the pattern file/rule

TABLE A-11. Managed Product Pattern File/Rule Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Pattern File/Rule Name	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern File/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Pattern File/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date

TABLE A-11. Managed Product Pattern File/Rule Status Data View

DATA	DESCRIPTION
Time of Latest Pattern File/Rule Update	Displays the time of the latest pattern file/rule deployment to managed products or clients.

Managed Product Component Deployment

Displays detailed information about components managed products use. Examples: pattern file/rule name, pattern file/rule version number, and scan engine deployment status

TABLE A-12. Managed Product Component Deployment Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Pattern File/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date
Pattern File/Rule Deployment Status	Displays the deployment status for the latest pattern file/rule update. Example: successful, unsuccessful, in progress
Time of Latest Pattern File/Rule Deployment	Displays the time of the latest pattern file/rule deployment to managed products or clients.

TABLE A-12. Managed Product Component Deployment Data View

DATA	DESCRIPTION
Scan Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Scan Engine Deployment Status	Displays the deployment status for the latest scan update. Example: successful, unsuccessful, in progress
Time of Latest Scan Engine Deployment	Displays the time of the latest scan engine deployment to managed products or clients.

Scan Engine Status Summary

Displays summary information about scan engines managed products use. Examples: scan engine name, scan engine rate, and the number of scan engines out-of-date

TABLE A-13. Scan Engine Status Summary Data View

DATA	DESCRIPTION
Scan Engine Name	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
Scan Engine Version	Displays the version of the scan engine. Example: Anti-spam Engine (Windows): **3.000.1153**, Virus Scan Engine IA 64 bit Scan Engine: **8.000.1008**
Scan Engines Up-to-Date	Displays the number of managed products with up-to-date scan engines.
Scan Engines Out-of-Date	Displays the number of managed products with out-of-date scan engines.
Scan Engine Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return N/A as a value.

Pattern File/Rule Status Summary

Displays summary information about pattern files/rules managed products use. Examples: pattern file/rule name, pattern file/rule up-to-date rate, and the number of pattern files/rules out-of-date

TABLE A-14. Pattern File/Rule Status Summary Data View

DATA	DESCRIPTION
Pattern File/Rule Name	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern File/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Pattern Files/Rules Up-to-Date	Displays the number of managed products with up-to-date pattern files or rules.
Pattern Files/Rules Out-of-Date	Displays the number of managed products with out-of-date pattern files or rules.
Pattern Files/Rules Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date pattern files/rules. This includes pattern files/rules that return n/a as a value.

Control Manager Information

User Access Information

Displays Control Manager user access and the activities users perform while logged on to Control Manager.

TABLE A-15. User Access Information Data View

DATA	DESCRIPTION
Time of Activity	Displays the time that the activity starts.
Log On User Name	Displays the name of the user who initiates the activity.

TABLE A-15. User Access Information Data View

DATA	DESCRIPTION
Account Type	Displays the account type a Control Manager administrator assigns to a user. For example: Root, Power User, or Operator.
Account Type Description	Displays the description of the Account Type. This description comes from Control Manager for default account types and from user-defined descriptions for custom account types.
Activity	Displays the activity the user performs on Control Manager. Example: log on, edit user account, add deployment plan
Activity Result	Displays the result of the activity.
Description	Displays the a description of the activity, if a description exists.

Control Manager Event Information

Displays information relating to Control Manager Server events. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE A-16. Control Manager Event Information Data View

DATA	DESCRIPTION
Time of Event	Displays the that the event occurred.
Event Type	Displays the type of event that occurred. Example: notify TMI agent, server notify user, report service notify user
Event Result	Displays the result of the event. Example: successful, unsuccessful
Description	Displays the description of the activity, if a description exists.

Command Tracking Information

Displays information relating to commands Control Manager delivers to managed products. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE A-17. Command Tracking Information Data View

DATA	DESCRIPTION
Time of Command	Displays the time that the issuer of the command issues the command.
Command Type	Displays the type of command issued. Example: scheduled update, Activation Code deployment
Command Parameter	Displays the specific information relating to the command. Example: specific pattern file name, specific Activation Code
Issuer of Command	Displays the user who issued the command.
Time of Latest Status Update	Displays the time of the latest status check of all commands for the selected Control Manager.
Successful	Displays the number of successful commands.
Unsuccessful	Displays the number of unsuccessful commands.
In Progress	Displays the number of commands that are still in progress.
All	Displays the total number of commands (Successful + Unsuccessful + In progress).

Detailed Command Tracking Information

Displays detailed information relating to commands. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE A-18. Detailed Command Tracking Information Data View

DATA	DESCRIPTION
Time of Command	Displays the time that the command was issued.
Command Type	Displays the type of command issued. Example: scheduled update, Activation Code deployment
Command Parameter	Displays the specific information relating to the command. Example: specific pattern file name, specific Activation Code
Managed Product Entity Display Name	Displays the managed product to which the command was issued.
Issuer of Command	Displays the user who issued the command.
Command Status	Displays the status of the command: successful, unsuccessful, in progress
Time of Latest Status Update	Displays the time of the latest status check of all commands for the selected Control Manager.
Result Detail Description	Displays the description Control Manager provides for events.

Data View: Security Threat Information

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

Virus/Malware Information

Summary Information

Overall Virus/Malware Summary

Provides overall specific summary for virus/malware detections. Example: name of virus/malware, number of clients affected by the virus, total number of instances of the virus on the network

TABLE A-19. Overall Virus/Malware Summary Data View

DATA	DESCRIPTION
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Unique Infection Destination Count	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Overall Virus/Malware Type Summary

Provides broad summary for virus/malware detections. Example: type of virus/malware (Trojans, hacking tools) , number of unique viruses/malware on your network, total number of instances of viruses/malware on the network

TABLE A-20. Overall Virus/Malware Type Summary Data View

DATA	DESCRIPTION
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Unique Infection Destination Count	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. The Unique Infection Source Count equals 2.
Virus/Malware Detection count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Virus/Malware Infection Source Summary

Provides a summary of virus/malware detections from the source of the outbreak. Example: name of source computer, number of specific virus/malware instances from the source computer, total number of instances of viruses/malware on the network

TABLE A-21. Virus/Malware Infection Source Summary Data View

DATA	DESCRIPTION
Infection Source	Displays the IP address/host name of the computer where viruses/malware originate.
Unique Infection Destination Count	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. The Unique Infection Destination Count equals 3.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Infection Destination Summary

Provides a summary of virus/malware detections from specific clients. Example: name of client, number of specific virus/malware instances on the client, total number of instances of viruses/malware on the network

TABLE A-22. Virus/Malware Infection Destination Summary Data View

DATA	DESCRIPTION
Infection Destination	Displays the IP address/host name of the computer affected by viruses/malware.
Unique Infection Source Count	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. The Unique Infection Source Count equals 2.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Detections Over Time Summary

Provides a summary of virus/malware detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of

clients affected by the virus, total number of instances of viruses/malware on the network

TABLE A-23. Virus/Malware Detections Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Unique Infection Destination Count	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Action/Result Summary

Provides a summary of the actions managed products take against viruses/malware. Example: specific actions taken against viruses/malware, the result of the action taken, total number of instances of viruses/malware on the network

TABLE A-24. Virus/Malware Action/Result Summary Data View

DATA	DESCRIPTION
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Unique Infection Destination Count	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Detailed Information

Detailed Overall Virus/Malware Information

Provides specific information about the virus/malware instances on your network. Example: the managed product which detects the viruses/malware, the name of the virus/malware, the name of the client with viruses/malware

TABLE A-25. Detailed Overall Virus/Malware Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/host name of the computer affected by viruses/malware.
Infection Source	Displays the IP address/host name of the computer where viruses/malware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required

TABLE A-25. Detailed Overall Virus/Malware Information Data View

DATA	DESCRIPTION
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Detected Entry Type	Displays the entry point for the virus/malware that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)
Detailed Information	Used only for Ad Hoc Queries. Displays detailed information about the selection. In Ad Hoc Queries this column displays the selection as underlined. Clicking the underlined selection displays more information about the selection. Example: Host Details, Network Details, HTTP/FTP Details

Virus/Malware Found in Hosts Information

Provides specific information about the virus/malware instances found on clients. Example: the managed product that detects the viruses/malware, the type of scan that detects the virus/malware, the file path on the client to detected viruses/malware

TABLE A-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.

TABLE A-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the name of the computer affected by viruses/malware.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Detecting Scan Type	Displays the type of scan the managed product uses to detect the virus/malware. Example: Real-time, scheduled, manual
Detected File Name	Displays the name of the file managed products detect affected by viruses/malware.
File Path	Displays the file path on the infection destination where managed products detect the virus/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE A-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in HTTP/FTP Information

Provides specific information about the virus/malware instances found in HTTP or FTP traffic. Example: the managed product that detects the viruses/malware, the direction of traffic where the virus/malware occurs, the Internet browser or FTP client that downloads the virus/malware.

TABLE A-27. Virus/Malware Found in HTTP/FTP Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/host name of the computer on which managed products detect viruses/malware.

TABLE A-27. Virus/Malware Found in HTTP/FTP Information Data View

DATA	DESCRIPTION
Source URL	Displays the URL of the Web/FTP site which the virus/malware originates.
Log On User Name	Displays the log on name of the user with a virus/malware instance.
Inbound/Outbound Traffic/Connection	Displays the direction of virus/malware entry.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the viruses/malware originates.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in Email Information

Provides specific information about the virus/malware instances found in email messages. Example: the managed product that detects the viruses/malware, the subject line content of the email message, the sender of the email message that contains viruses/malware

TABLE A-28. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.

TABLE A-28. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Recipient	Displays the recipient of email message containing viruses/malware.
Sender	Displays the sender of email message containing viruses/malware.
Log On User Name	Displays the log on name of the user with a virus/malware instance.
Email Subject Content	Displays the content of the subject line of the email message containing viruses/malware.
Detected File Name	Displays the name of the file managed products detect affected by viruses/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE A-28. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Virus/Malware Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in Network Traffic Information

Provides specific information about the virus/malware instances found in network traffic. Example: the managed product that detects the viruses/malware, the protocol the virus/malware uses to enter your network, specific information about the source and destination of the virus/malware

TABLE A-29. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/ host name of the computer affected by viruses/malware.

TABLE A-29. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Infection Source	Displays the IP address/host name of the computer where viruses/malware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Inbound/Outbound Traffic/Connection	Displays the direction of virus/malware entry.
Protocol	Displays the protocol that the virus/malware uses to enter the network. Example: HTTP, SMTP, FTP
Destination Host Name	Displays the host name of the computer affected by viruses/malware.
Destination Port	Displays the port number of the computer affected by viruses/malware.
Destination MAC Address	Displays the MAC address of the computer affected by viruses/malware.
Source Host Name	Displays the host name of the computer where viruses/malware originates.
Source Port	Displays the port number of the computer where viruses/malware originates.
Source MAC Address	Displays the MAC address of the computer where viruses/malware originates.
Detected File Name	Displays the name of the file managed products detect affected by viruses/malware.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE A-29. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Spyware/Grayware Information

Summary Information

Overall Spyware/Grayware Summary

Provides overall specific summary for spyware/grayware detections. Example: name of spyware/grayware, number of clients affected by the spyware/grayware, total number of instances of the spyware/grayware on the network

TABLE A-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Unique Spyware/Grayware Destination Count	Displays the number of unique computers affected by the spyware/grayware. OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. The Unique Spyware/Grayware Destination Count equals 3.
Unique Spyware/Grayware Source Count	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. The Unique Spyware/Grayware Source Count equals 2.

TABLE A-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect.

Spyware/Grayware Source Summary

Provides a summary of spyware/grayware detections from the source of the outbreak. Example: name of source computer, number of specific spyware/grayware instances from the source computer, total number of instances of spyware/grayware on the network

TABLE A-31. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Source	Displays the name of the computer where spyware/grayware originates.
Unique Spyware/Grayware Destination Count	Displays the number of unique computers affected by the spyware/grayware. OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. The Unique Spyware/Grayware Destination Count equals 3.
Unique Spyware/Grayware Count	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

TABLE A-31. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Destination Summary

Provides a summary of spyware/grayware detections from specific clients. Example: name of client, number of specific spyware/grayware instances on the client, total number of instances of spyware/grayware on the network

TABLE A-32. Spyware/Grayware Destination Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Destination	Displays the host name or IP address of the computer affected by spyware/grayware.
Unique Spyware/Grayware Source Count	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. The Unique Spyware/Grayware Source Count equals 2.
Unique Spyware/Grayware Count	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

TABLE A-32. Spyware/Grayware Destination Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Detection Over Time Summary

Provides a summary of spyware/grayware detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data collected, number of clients affected by the spyware/grayware, total number of instances of spyware/grayware on the network

TABLE A-33. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Spyware/Grayware Count	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.
Unique Spyware/Grayware Destination Count	Displays the number of unique computers affected by the spyware/grayware. OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. The Unique Spyware/Grayware Destination Count equals 3.

TABLE A-33. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Spyware/Grayware Source Count	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. The Unique Spyware/Grayware Source Count equals 2.
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Action/Result Summary

Provides a summary of the actions managed products take against spyware/grayware. Example: specific actions taken against spyware/grayware, the result of the action taken, total number of instances of spyware/grayware on the network

TABLE A-34. Spyware/Grayware Action/Result Summary Data View

DATA	DESCRIPTION
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Unique Spyware/Grayware Destination Count	Displays the number of unique computers affected by the spyware/grayware. OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. The Unique Spyware/Grayware Destination Count equals 3.

TABLE A-34. Spyware/Grayware Action/Result Summary Data View

DATA	DESCRIPTION
Unique Spyware/Grayware Source Count	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. The Unique Spyware/Grayware Source Count equals 2.
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Detailed Information

Detailed Overall Spyware/Grayware Information

Provides specific information about the spyware/grayware instances on your network. Example: the managed product that detects the spyware/grayware, the name of the spyware/grayware, the name of the client with spyware/grayware

TABLE A-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE A-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the name of the computer affected by spyware/grayware.
Spyware/Grayware Source	Displays the name of the computer where spyware/grayware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.
Detected Entry Type	Displays the entry point for the spyware/grayware that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)

TABLE A-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Detailed Information	Used only for Ad Hoc Queries. Displays detailed information about the selection. In Ad Hoc Queries this column displays the selection as underlined. Clicking the underlined selection displays more information about the selection. Example: Host Details, Network Details, HTTP/FTP Details

Spyware/Grayware Found in Hosts

Provides specific information about the spyware/grayware instances found on clients. Example: the managed product that detects the spyware/grayware, the type of scan that detects the spyware/grayware, the file path on the client to detected spyware/grayware

TABLE A-36. Spyware/Grayware Found in Hosts Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the computer that is affected by spyware/grayware.

TABLE A-36. Spyware/Grayware Found in Hosts Data View

DATA	DESCRIPTION
Spyware/Grayware Source	Displays the name of the computer where the spyware/grayware originates.
Log On User Name	Displays the user name logged on to the spyware/grayware destination when a managed product detects spyware/grayware.
Detecting Scan Type	Displays the type of scan the managed product uses to detect the spyware/grayware. Example: Real-time, scheduled, manual
Affected Resource	Displays the specific resource affected. Example: application.exe, H Key Local Machine\SOFTWARE\ACME
Affected Resource Type	Displays the type of resource affected by spyware/grayware. Example: registry, memory resource
Spyware/Grayware Risk Type	Displays the specific type of spyware/grayware managed products detect. Example: adware, COOKIE, peer-to-peer application
Spyware/Grayware Risk Level	Displays the Trend Micro-defined level of risk the spyware/grayware poses to your network. Example: High security, Medium security, Low security
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted

Spyware/Grayware Found in HTTP/FTP

Provides specific information about the spyware/grayware instances found in HTTP or FTP traffic. Example: the managed product that detects the spyware/grayware, the

direction of traffic where the spyware/grayware occurs, the Internet browser or FTP client that downloads the spyware/grayware

TABLE A-37. Spyware/Grayware Found in HTTP/FTP Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the IP address/host name of the computer on which managed products detect spyware/grayware.
Source URL	Displays the URL of the Web/FTP site which the spyware/grayware originates.
Inbound/Outbound Traffic/Connection	Displays the direction of spyware/grayware entry.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the spyware/grayware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required

TABLE A-37. Spyware/Grayware Found in HTTP/FTP Data View

DATA	DESCRIPTION
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Found in Email

Provides specific information about the spyware/grayware instances found in email messages. Example: the managed product that detects the spyware/grayware, the subject line content of the email message, the sender of the email message that contains spyware/grayware

TABLE A-38. Spyware/Grayware Found in Email Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.

TABLE A-38. Spyware/Grayware Found in Email Data View

DATA	DESCRIPTION
Recipient	Displays the recipient of email message containing spyware/grayware.
Sender	Displays the sender of email message containing spyware/grayware.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Email Subject Content	Displays the content of the subject line of the email message containing spyware/grayware.
Detected File Name	Displays the name of the file managed products detect affected by spyware/grayware.
File in Compressed File	Displays the file name of the spyware/grayware occurring in a compressed file.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Found in Network Traffic

Provides specific information about the spyware/grayware instances found in network traffic. Example: the managed product that detects the spyware/grayware, the protocol

the spyware/grayware uses to enter your network, specific information about the source and destination of the spyware/grayware

TABLE A-39. Spyware/Grayware Found in Network Traffic Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Inbound/Outbound Traffic/Connection	Displays the direction of spyware/grayware entry.
Protocol	Displays the protocol that the spyware/grayware uses to enter the network. Example: HTTP, SMTP, FTP
Spyware/Grayware Destination	Displays the IP address/host name of the computer affected by spyware/grayware.
Spyware/Grayware Destination Host Name	Displays the host name of the computer affected by spyware/grayware.
Spyware/Grayware Destination Port	Displays the port number of the computer affected by spyware/grayware.
Spyware/Grayware Destination MAC Address	Displays the MAC address of the computer affected by spyware/grayware.
Spyware/Grayware Source	Displays the IP address/host name of the computer where spyware/grayware originates.

TABLE A-39. Spyware/Grayware Found in Network Traffic Data View

DATA	DESCRIPTION
Spyware/Grayware Source Host Name	Displays the host name of the computer where spyware/grayware originates.
Spyware/Grayware Source Port	Displays the port number of the computer where spyware/grayware originates.
Spyware/Grayware Source MAC Address	Displays the MAC address of the computer where spyware/grayware originates.
Log On User Name	Displays the user name logged on to the spyware/grayware destination when a managed product detects spyware/grayware.
Detected File Name	Displays the name of the file managed products detect affected by spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Content Violation Information

Summary Information

Content Violation Policy Summary

Provides a summary of content violation detections due to specific policies. Example: name of the policy in violation, the type of filter that detects the content violation, the total number of content violations on the network

TABLE A-40. Content Violation Policy Summary Data View

DATA	DESCRIPTION
Policy in Violation	Displays the name of the policy that clients violate.
Filter Type	Displays the type of filter that triggers the violation. Example: content filter, phishing filter, URL reputation filter
Unique Policy Violation Sender Count	Displays the number of unique email message addresses sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. The Unique Policy Violation Sender Count equals 3.
Unique Policy Violation Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. The Unique Policy Violation Recipient Count equals 2.
Policy Violation Detection Count	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

Content Violation Sender Summary

Provides a summary of content violation detections due to specific senders. Example: name of the content sender, the number of unique content violations, the total number of content violations on the network

TABLE A-41. Content Violation Sender Summary Data View

DATA	DESCRIPTION
Policy Violation Sender	Displays the email message address sending content that violates managed product policies.
Policy Violation Detection Count	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.
Unique Policy Violation Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. The Unique Policy Violation Recipient Count equals 2.
Unique Policy in Violation Count	Displays the number of unique policies in violation managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

Content Violation Detection Over Time Summary

Provides a summary of content violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data collected, number of clients

affected by the content violation, total number of unique content violations and total number of content violations on the network

TABLE A-42. Content Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Policy in Violation Count	Displays the number of unique policies in violation managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.
Unique Policy Violation Sender Count	Displays the number of unique email message addresses sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. The Unique Policy Violation Sender Count equals 3.
Unique Policy Violation Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. The Unique Policy Violation Recipient Count equals 2.
Policy Violation Detection Count	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

Content Violation Action/Result Summary

Provides a summary of actions managed products take against content violations. Example: the action managed products take against the content violation, the number of email messages affected by the action taken

TABLE A-43. Content Violation Action/Result Summary Data View

DATA	DESCRIPTION
Action Taken	Displays the type of action managed products take against email message in violation of content policies. Example: forwarded, attachments stripped, deleted
Email Count	Displays the number of email messages with the specified action taken by managed products.

Detailed Information

Detailed Overall Content Violation Information

Provides specific information about the content violations on your network. Example: the managed product that detects the content violation, the name of the specific policy in violation, the total number of content violations on the network

TABLE A-44. Detailed Overall Content Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE A-44. Detailed Overall Content Violation Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Recipient	Displays the email recipients receiving content that violate managed product policies.
Sender	Displays the email address sending content that violates managed product policies.
Email Subject Content	Displays the content of the subject line of the email that violates a policy.
Policy in Violation	Displays the name of the policy an email violates.
Policy Settings	Displays the settings for the policy that an email violates.
Detected File Name	Displays the name of the file that violates a policy.
Detecting Filter Type	Displays the type of filter that detects the email in violation. Example: content filter, size filter, attachment filter
Detecting Filter Action	Displays the action the detecting filter takes against email in violation of a policy. Example: clean, quarantine, strip
Action Taken	Displays the type of action managed products take against email in violation of content policies. Example: deliver, strip, forward
Policy Violation Detection Count	Displays the total number of policy violations managed products detect.

Spam Violation Information

Summary Information

Overall Spam Violation Summary

Provides a summary of spam detections on specific domains. Example: name of the domain receiving spam, the number of clients receiving spam, the total number of spam violations on the network

TABLE A-45. Overall Spam Violation Summary Data View

DATA	DESCRIPTION
Recipient Domain	Displays the domain that receives spam.
Unique Recipient Count	Displays the number of unique recipients receiving spam from the specified domain. Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers. The Unique Recipient Count equals 3.
Spam Violation Detection Count	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. The Spam Violation Detection Count equals 10.

Spam Recipient Summary

Provides a summary of spam violations on specific clients. Example: name of client, total number of instances of viruses/malware on the client

TABLE A-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Recipient Name	Displays the name of the recipient who receives spam.

TABLE A-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Spam Violation Detection Count	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. The Spam Violation Detection Count equals 10.

Spam Detection Over Time Summary

Provides a summary of spam detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data collected, number of clients affected by spam, the total number of spam violations on the network

TABLE A-47. Spam Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Recipient Domain Count	Displays the total number of unique recipient domains affected by spam. Example: A managed product detects 10 violation instances of the same spam from 2 domains on 1 recipient domain. The Unique Recipient Domain Count equals 1.
Unique Recipient Count	Displays the number of unique recipients receiving spam from the specified domain. Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers. The Unique Recipient Count equals 3.
Spam Violation Detection Count	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. The Spam Violation Detection Count equals 10

Detailed Information

Detailed Overall Spam Information

Provides specific information about the spam violations on your network. Example: the managed product that detects the content violation, the name of the specific policy in violation, the total number of spam violations on the network

TABLE A-48. Detailed Overall Spam Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Recipient	Displays the recipients of email containing spam.
Sender	Displays the sender of email containing spam.
Email Subject Content	Displays the content of the subject line of the email containing spam.
Policy in Violation	Displays the name of the policy the email violates.
Action Taken	Displays the type of action managed products take against spam found in email. Example: deliver, forward, strip
Spam Violation Detection Count	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. The Spam Violation Detection Count equals 10.

Spam Connection Information

Provides specific information about the spam violations on your network. Example: the managed product that detects the spam violation, the specific action managed products take against spam violations, the total number of spam violations on the network

TABLE A-49. Spam Connection Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spam Source IP Address	Displays the IP address of the mail server where spam originates.
Detecting Filter Type	Displays the type of filter that detects the email in violation. Example: Real-time Blackhole List (RBL+), Quick IP List (QIL)
Action Taken	Displays the type of action managed products take against spam to prevent spam from entering the email server. Example: drop connection, bypass connection
Spam Violation Detection Count	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. The Spam Violation Detection Count equals 10.

Policy/Rule Violation Information

Detailed Information

Detailed Overall Firewall Rule Violation Information

Provides specific information about the firewall violations on your network. Example: the managed product that detects the firewall violation, specific information about the source and destination, the total number of firewall violations on the network

TABLE A-50. Detailed Overall Firewall Rule Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Event Type	Displays the type of event that triggers the violation. Example: intrusion, policy violation
Security Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security
Inbound/Outbound Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol the intrusion uses. Example: HTTP, SMTP, FTP
Source IP Address	Displays the IP address of the computer attempting an intrusion on your network.

TABLE A-50. Detailed Overall Firewall Rule Violation Information Data View

DATA	DESCRIPTION
Destination Port	Displays the port number of the computer under attack.
Destination IP Address	Displays the IP address of the computer under attack.
Target Application	Displays the application the intrusion targets.
Description	Detailed description of the incident by Trend Micro.
Action Taken	Displays the type of action managed products take against policy violations. Example: file cleaned, file quarantined, file passed
Policy/Rule Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Policy/Rule Violation Detection Count equals 10.

Detailed Overall Endpoint Security Violation Information

Provides specific information about the endpoint security violations on your network. Example: the managed product that detects the Web violation, the name of the specific policy in violation, the total number of Web violations on the network

TABLE A-51. Detailed Overall Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.

TABLE A-51. Detailed Overall Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Client in Violation	Displays the host name of the computer in violation of the policy/rule.
IP Address of Client in Violation	Displays the IP address of the computer in violation of the policy/rule.
MAC Address of Client in Violation	Displays the MAC address of the computer in violation of the policy/rule.
Policy/Rule in Violation	Displays the name of the policy/rule in violation.
Service in Violation	Displays the name of the service/program in violation of the policy/rule.
Log On User Name	Displays the user name logged on to the client when a managed product detects a policy/rule violation.
Enforcement Action	Displays the action a managed product takes to protect your network. Example: block, redirect, pass
Remediation Action	Displays the action a managed product takes to solve the policy violation. Example: file cleaned, file quarantined, file deleted
Description	Displays a detailed description of the incident by Trend Micro.
Policy/Rule Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Policy/Rule Violation Detection Count equals 10.

Detailed Overall Endpoint Security Compliance Information

Provides specific information about the endpoint security compliance instances on your network. Example: the managed product that detects the security compliance, the name of the specific policy in compliance, the total number of security compliances on the network

TABLE A-52. Detailed Overall Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Client in Compliance	Displays the host name of the computer in compliance of the policy/rule.
IP Address of Client in Compliance	Displays the IP address of the computer in compliance of the policy/rule.
MAC Address of Client in Compliance	Displays the MAC address of the computer in compliance of the policy/rule.
Policy/Rule in Compliance	Displays the name of the policy/rule in compliance.
Service in Compliance	Displays the name of the service/program in compliance of the policy/rule.
Log On User Name	Displays the user name logged on to the client when a managed product detects a policy/rule compliance.

TABLE A-52. Detailed Overall Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Description	Detailed description of the incident by Trend Micro.
Policy/Rule Compliance Detection Count	Displays the total number of policy/rule compliances managed products detect. Example: A managed product detects 10 compliance instances of the same type on one computer. The Policy/Rule Compliance Detection Count equals 10.

Web Violation Information

Summary Information

Overall Web Violation Summary

Provides a summary of Web violations of specific policies. Example: name of the policy in violation, the type of filter/blocking to stop access to the URL, the total number of Web violations on the network

TABLE A-53. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Policy in Violation	Displays the name of the policy the URL violates.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Web blocking
Unique Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.

TABLE A-53. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Unique URLs in Violation Count	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on 1 computer. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.

Web Violation Client Host Summary

Provides a summary of Web violation detections from a specific client. Example: IP address of the client in violation, number of policies in violation, the total number of Web violations on the network

TABLE A-54. Web Violation Client IP Address Summary Data View

DATA	DESCRIPTION
Host of Client in Violation	Displays the IP address/host name of clients in violation of Web policies.
Unique Policies in Violation Count	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies in Violation Count equals 1.
Unique URLs in Violation Count	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.

TABLE A-54. Web Violation Client IP Address Summary Data View

DATA	DESCRIPTION
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Web Violation URL Summary

Provides a summary of Web violation detections from specific URLs. Example: name of the URL causing the Web violation, the type of filter/blocking to stop access to the URL, the total number of Web violations on the network

TABLE A-55. Web Violation URL Summary Data View

DATA	DESCRIPTION
URL in Violation	Displays the URL violating a Web policy.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Web blocking
Unique Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Web Violation Filter/Blocking Type Summary

Provides a summary of the action managed products take against Web violations. Example: the type of filter/blocking to stop access to the URL, the total number of Web violations on the network

TABLE A-56. Web Violation Filter/Blocking Type Summary Data View

DATA	DESCRIPTION
Blocking Category	Displays the broad type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Anti-spyware
Filter/Blocking Type	Displays the specific type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Virus/Malware
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Web Violation Detection Over Time Summary

Provides a summary of Web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data collected, number of clients in violation, the total number of Web violations on the network

TABLE A-57. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.

TABLE A-57. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Policies in Violation Count	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies in Violation Count equals 1.
Unique Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.
Unique URLs in Violation Count	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Detailed Information

Detailed Overall Web Violation Information

Provides specific information about the Web violations on your network. Example: the managed product that detects the Web violation, the name of the specific policy in violation, the total number of Web violations on the network

TABLE A-58. Detailed Overall Web Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Inbound/Outbound Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
URL in Violation	Displays the name of the URL that violates a Web policy.
Client Host	Displays the IP address/host name of the client that violates a policy.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Web blocking
Policy in Violation	Displays the name of the policy the URL violates.

TABLE A-58. Detailed Overall Web Violation Information Data View

DATA	DESCRIPTION
File in Violation	Displays the name of the file that violates the policy.
Web Reputation Rating	Displays the relative safety, as a percentage, of a Web site according to Trend Micro.
Action Taken	Displays the type of action managed products take against policy violations. Example: pass, block
Web Violation Detection Count	Displays the total number of Web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Suspicious Threat Information

Summary Information

Overall Suspicious Threat Summary

Provides specific information about suspicious threats on your network. Example: the rule/violation in violation, summary information about the source and destination, the total number of suspicious threats on the network

TABLE A-59. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Policy/Rule in Violation	Displays the name of the policy/rule in violation.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP

TABLE A-59. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Destination Count	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. The Unique Suspicious Threat Recipient Count equals 2.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.
Mitigation Count	Displays the number of clients Network VirusWall Enforcer devices or Total Discovery Mitigation Server take action against.

TABLE A-59. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Cleaned Client Count	Displays the total number of clients Total Discovery Mitigation Server cleans.
Clean Client Rate (%)	Displays the percentage of clients Total Discovery Mitigation Server cleans compared to the total Suspicious Threat Violation Detection Count.

Suspicious Threat Source Summary

Provides a summary of suspicious threat detections from a specific source. Example: name of the source, summary information about the destination and rules/violations, the total number of suspicious threats on the network

TABLE A-60. Suspicious Threat Source Summary Data View

DATA	DESCRIPTION
Suspicious Threat Source IP Address	Displays the IP addresses of sources where suspicious threats originate.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Destination Count	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. The Unique Suspicious Threat Destination Count equals 2.

TABLE A-60. Suspicious Threat Source Summary Data View

DATA	DESCRIPTION
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Riskiest Destination Summary

Provides a summary of the clients with the most suspicious threat detections. Example: name of the destination, summary information about the source and rules/violations, the total number of suspicious threats on the network

TABLE A-61. Suspicious Threat Riskiest Destination Summary Data View

DATA	DESCRIPTION
Suspicious Threat Destination IP Address	Displays the IP addresses of computers affected by suspicious threats.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Source Count	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. The Unique Suspicious Threat Source Count equals 3.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Riskiest Recipient Summary

Provides a summary of the recipients with the most suspicious threat detections. Example: name of the recipient, summary information about the senders and rules/violations, the total number of suspicious threats on the network

TABLE A-62. Suspicious Threat Riskiest Recipient Summary Data View

DATA	DESCRIPTION
Suspicious Threat Recipient	Displays the email address of the recipient affected by the suspicious threat.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Sender Summary

Provides a summary of suspicious threat detections from a specific sender. Example: name of the sender, summary information about the recipient and rules/violations, the total number of suspicious threats on the network

TABLE A-63. Suspicious Threat Sender Summary Data View

DATA	DESCRIPTION
Suspicious Threat Sender	Displays the email address for the source of policy/rule violations.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. The Unique Suspicious Threat Recipient Count equals 2.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Protocol Detection Summary

Provides a summary of suspicious threats detections over a specific protocol. Example: name of the protocol, summary information about the source and destination, the total number of suspicious threats on the network

TABLE A-64. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Protocol Name	Displays the name of the protocol over which the suspicious threat occurs. Example: HTTP, FTP, SMTP
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Destination Count	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. The Unique Suspicious Threat Recipient Count equals 2.

TABLE A-64. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Detection Over Time Summary

Provides a summary of suspicious threats detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data collected, summary information about the source and destination, the total number of suspicious threats on the network

TABLE A-65. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies/Rules in Violation Count equals 1.

TABLE A-65. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Destination Count	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. The Unique Suspicious Threat Recipient Count equals 2.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Detailed Information

Detailed Overall Suspicious Threat Information

Provides specific information about suspicious threats on your network. Example: the managed product that detects the suspicious threat, specific information about the source and destination, the total number of suspicious threats on the network

TABLE A-66. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Mitigation Server Entity Display Name	Displays the entity display name for the mitigation server. Control Manager identifies managed products using the managed product's entity display name.
Inbound/Outbound Traffic/Connection	Displays the direction of network traffic or the position on the network the suspicious threat originates.
Protocol Group	Displays the broad protocol group from which a managed product detects the suspicious threat. Example: FTP, HTTP, P2P
Protocol	Displays the protocol from which a managed product detects the suspicious threat. Example: ARP, Bearshare, BitTorrent

TABLE A-66. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Suspicious Threat Destination IP Address	Displays the IP address of the client the suspicious threat affects.
Suspicious Threat Destination Port	Displays the port number of the client the suspicious threat affects.
Suspicious Threat Destination MAC Address	Displays the MAC address of the client the suspicious threat affects.
Suspicious Threat Source IP Address	Displays the IP address of the source where the suspicious threat originates.
Suspicious Threat Source Host Name	Displays the host name of the source where the suspicious threat originates.
Suspicious Threat Source Port	Displays the port number of the source where the suspicious threat originates.
Suspicious Threat Source MAC Address	Displays the MAC address of the source where the suspicious threat originates.
Domain Name	Displays the domain of the source where the suspicious threat originates.
VLAN ID	Displays the VLAN ID of the source where the suspicious threat originates.
Risk Type	Displays the specific type of security risk managed products detect. Example: virus, spyware/grayware, fraud
Threat Confidence Level	Displays Trend Micro's confidence that the suspicious threat poses a danger to your network.
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
Policy/Rule in Violation	Displays the policy/rule the suspicious threat violates.
Recipient	Displays the recipient of the suspicious threat.
Sender	Displays the sender of the suspicious threat.

TABLE A-66. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Email Subject Content	Displays the content of the subject line of the email containing spyware/grayware.
URL in Violation	Displays the URL considered a suspicious threat.
Log On User Name	Displays the user name logged on to the destination when a managed product detects a suspicious threat.
Instant Messaging/IRC User Name	Displays the instant messaging or IRC user name logged on when Total Discovery Appliance detects a violation.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the suspicious threat originates.
Channel Name	Displays the protocol that the instant messaging software or IRC use for communication.
File Name of Suspicious File	Displays the name of the suspicious file.
Suspicious File in Compressed File	Displays whether the suspicious threat originates from a compressed file.
File Size	Displays the size of the suspicious file.
File Extension	Displays the file extension of the suspicious file. Example: .wmf, .exe, .zip
True File Type	Displays the "true" file type which is detected using the file's header not the file's extension.
Shared Folder	Displays whether the suspicious threat originates from a shared folder.
Authentication	Displays whether authentication was used.
BOT Command	Displays the command that bots send or receive to or from the control channel.
BOT URL	Displays the URL that bots receive their commands from.

TABLE A-66. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Constraint Type	Displays the reason that a file cannot be scanned correctly.
Mitigation Result Description	Displays the result of the action the mitigation server takes against suspicious threats.
Mitigation Action Taken	Displays the action the mitigation server takes against suspicious threats. Example: File cleaned, File dropped, File deleted
Suspicious Threat Violation Detection Count	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. The Suspicious Threat Violation Detection Count equals 10.

Overall Threat Information

Complete Network Security Risk Analysis Information

Displays information for overall security risks affecting your desktops. Examples: name of the security risk, total number of security risk detections, number of clients affected

TABLE A-67. Complete Network Security Risk Analysis Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Detected Entry Type	Displays the entry point for the security risk that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)

TABLE A-67. Complete Network Security Risk Analysis Information Data View

DATA	DESCRIPTION
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Network Protection Boundary Information

Displays information for a broad overview of security risks affecting your entire network. Examples: managed product network protection type (gateway, email), type of security risk, number of clients affected

TABLE A-68. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Managed Product Category	Displays the category to which the managed product belongs. Example: desktop products, mail server products, network products
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE A-68. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Security Risk Entry Point Analysis Information

Displays information with the entry point of security risks as the focus. Examples: managed product network protection type (gateway, email, desktop), name of the security risk, time of the last security risk detection

TABLE A-69. Security Risk Entry Point Analysis Information Data View

DATA	DESCRIPTION
Detected Entry Type	Displays the point of entry for security risks managed products detect. Example: Virus found in file, FTP, File transfer

TABLE A-69. Security Risk Entry Point Analysis Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product which detects the security risk. Example: OfficeScan, ScanMail for Microsoft Exchange
Security Risk Category	Displays the specific category for security risks managed products detect. Example: Antivirus, Anti-spyware, Content filtering
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Security Risk Destination Analysis Information

Displays information with affected clients as the focus. Examples: name of the client, the broad range of how the security risk enters your network, number of clients affected

TABLE A-70. Security Risk Destination Analysis Information Data View

DATA	DESCRIPTION
Security Risk/Violation Destination	Displays the name of computers affected by the security risk/violation.
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10.
Time of Latest Infection/Violation	Displays the time and date of the last security risk/violation detection on the computer affected the security risk/violation.

Security Risk Source Analysis Information

Displays information with the security risk source as the focus. Examples: name of the security risk source, the broad range of how the security risk enters your network, number of clients affected

TABLE A-71. Security Risk Source Analysis Information Data View

DATA	DESCRIPTION
Security Risk/Violation Source	Displays the name of the computer where the cause of the security risk/violation originates.

TABLE A-71. Security Risk Source Analysis Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10.
Time of Latest Infection/Violation	Displays the time and date of the last security risk/violation detection on the computer affected the security risk/violation.

Index

W