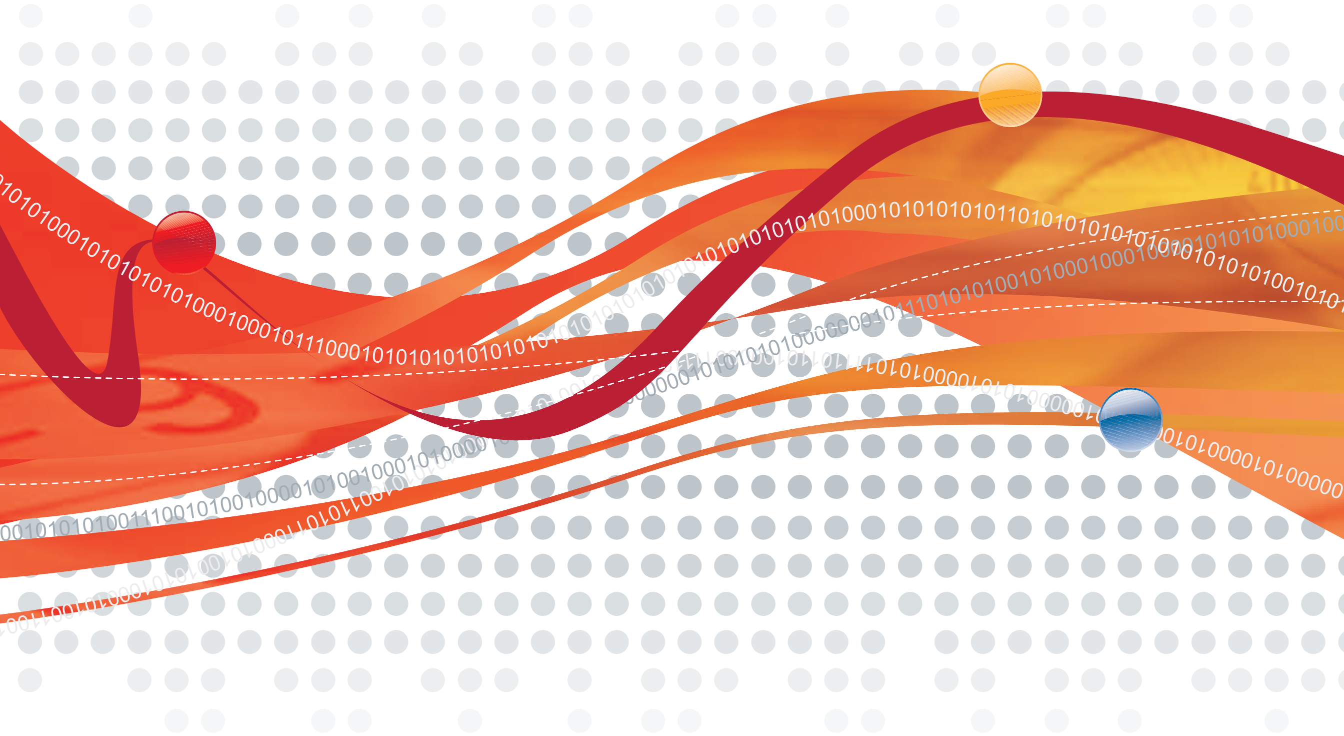
TREND MICRO™

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, please review the readme files, release notes and the latest version of the Control Manager documentation, which are available from the Trend Micro website at:

http://downloadcenter.trendmicro.com/

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.

Release Date: April 2011

The *Tutorial* is intended to introduce the main features of the software. You should read through it prior to installing or using the software.

Contents

Preface

Chapter 1: Preparing the Environment

Chapter 2: Installing Trend Micro Control Manager for the First Time

Chapter 3: Getting Started with Control Manager

Chapter 4: Monitoring the Control Manager Network

Chapter 5: Activating Managed Products

Chapter 6: Managing Managed Products

Chapter 7: Removing Trend Micro Control Manager

Appendix A: Data Views

Index

Preface

Preface

This *Tutorial* introduces Trend Micro™ Control Manager™ 5.5, and guides you through planning the installation and installing Control Manager and walks you through configuring Control Manager to function according to your needs.

This preface contains the following topics:

- What’s New in This Version on page x
- Control Manager Documentation on page xii
- Document Conventions on page xiii

What's New in This Version

Trend Micro Control Manager 5.5 represents a significant advance in monitoring and management software for antivirus and content security products. Architectural improvements in this new version make Control Manager more flexible and scalable than ever before.

Control Manager 5.5 Features and Enhancements

The following new features and enhancements are available in version 5.5.

Threat Intelligence-Oriented Dashboard

The Summary screen has been replaced with an Adobe™ Flash™-based, customizable dashboard that supports Trend Micro widgets. Trend Micro widgets provide administrators with at-a-glance information. For detailed information the administrator can click the content in the widget. Retrieving the detailed widget content leverages the Control Manager Ad Hoc Query feature.

The widget framework integration for Control Manager supports the following widget types.

TABLE PREFACE-1. Control Manager Widget Types

WIDGET TYPE	DESCRIPTION
Summary	• Threat Detection Results (Virus/Spyware/Web Security/Content Security/Network Virus) • Policy Violation Detections • Product Component Status
Smart Protection Network	• Smart Protection Network Connections • Smart Protection Network Threat Statistics • Web Reputation Top Threat Sources • Web Reputation Top Threatened Users • Email Reputation Threat Map • File Reputation Threat Map • File Reputation Top Threat Detections

TABLE PREFACE-1. Control Manager Widget Types (Continued)

WIDGET TYPE	DESCRIPTION
Enterprise Security Metrics	• Control Manager Top Threats • Control Manager Threat Statistics • Product Application Compliance • Product Connection Status • OfficeScan Endpoint Connection Status

OfficeScan Integration Enhancements

Control Manager enhances integration with OfficeScan by providing consummate data synchronization between OfficeScan and Control Manager. Control Manager also supports OfficeScan 10.5 integration with the inclusion of Plug-in Manager Plug-in Programs component updates.

Note: The OfficeScan web console displays all available Plug-in Programs. You can specify to download any of them from Control Manager. However, Control Manager may not have the downloaded the Plug-in Program. Which means that OfficeScan cannot download the specified Plug-in Program from Control Manager.

Before specifing a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.

Improved Scalability

Control Manager 5.5 has significantly improved log processing speeds, compared to Control Manager 5.0. With the improved log processing speeds, Control Manager can support significantly more managed products (and endpoints registered to managed products).

Other Enhancements

Control Manager also provides the following enhancements:

- Web console now renders faster
- Web console has been rebranded

Control Manager Documentation

This 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.

TABLE PREFACE-2. Control Manager Documentation

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Control Manager web console. The online help contains explanations of 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 website: http://esupport.trendmicro.com/enterprise/default.aspx
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, known issues, and product release history.
Installation Guide	PDF documentation is accessible from the Trend Micro Enterprise DVD or downloadable from the Trend Micro website. The *Installation Guide* contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".

TABLE PREFACE-2. Control Manager Documentation (Continued)

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The *Administrator's Guide* contains detailed instructions of how to deploy, install, configure, and manage Control Manager and managed products, and explanations on Control Manager concepts and features.
Tutorial	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The Tutorial contains hands-on instructions of how to deploy, install, configure, and manage Control Manager and managed products registered to Control Manager.

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

TABLE PREFACE-3. Control Manager Documentation Conventions

CONVENTION	DESCRIPTION
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 on page 1-2
- About the Control Manager Managed Product Network on page 1-3

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™ processor
Memory	4GB RAM
Disk space	A hard drive with 80GB of free disk space
Operating system	Microsoft™ Windows™ 2003 Server Standard Edition SP 2
Web server	Microsoft™ IIS server 6.0 (For 2003 platform)
Database	Microsoft SQL 2005 Server SP3
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 three OfficeScan 10.5 servers (with endpoints registered to them) to provide data for the dashboard (and widgets), logs, and reports.

The Tutorial also uses the following fictional users for purposes of demonstrating product capabilities.

TABLE 1-2. Managed Product Servers and Users

MANAGED PRODUCT	USERS			
	GLOBAL	REGIONAL	LOCAL	LIMITED
OfficeScan 10.5	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 on page 2-2
- Pre-Installation Tasks on page 2-7
- Installing a Control Manager Server on page 2-8
- Verifying Successful Installations on page 2-28
- Post-installation Configuration on page 2-30
- Registering and Activating Your Software on page 2-31

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: Control Manager 5.5 Advanced supports the following as child Control Manager servers:

- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition

Control Manager 5.0/5.5 Standard servers cannot be child servers.

Please refer to the managed product documentation for detailed agent system requirements.

TABLE 2-1. Control Manager Server System Requirements

COMPONENT	REQUIREMENT
CPU	Intel™ Pentium™ or compatible processor
Memory	• 2GB minimum • **4GB recommended**
Hard Disk	• 900MB for Control Manager Standard/Advanced • 600MB for SQL Server 2005 Express SP3 (Optional) • 20GB additional space for growing logs, reports, and ActiveUpdate components

TABLE 2-1. Control Manager Server System Requirements (Continued)

COMPONENT	REQUIREMENT
Operating System	• Microsoft™ Windows™ Server 2008 Standard/Enterprise/Web Edition with SP1 or later (32-bit/64-bit) • Microsoft Windows Server 2008 Standard/Enterprise/Web Edition R2 (32-bit/64-bit) • Microsoft Windows 2003 Server Standard/Enterprise/Datacenter Edition SP2 (32-bit/64-bit) • Microsoft Windows 2003 Server Standard/Enterprise/Datacenter Edition R2 SP2 (32-bit/64-bit) **Note:** Control Manager is a 32-bit program. Control Manager installs under WOW on 64-bit computers (Windows 2003/2008/2008R2 Standard/Enterprise and Windows 2008/2008R2 Web Edition). When installed on 64-bit computers, modify IIS to use 32-bit mode. • VMware™ ESX™ 4.x/3.x • VMware ESXi™ 4.x/3.x • VMware Workstation 6.0 or later • Microsoft Server 2008 R2 Hyper-V™

TABLE 2-1. Control Manager Server System Requirements (Continued)

COMPONENT	REQUIREMENT
SQL Server application	• Microsoft™ SQL Server™ 2008 Express • Microsoft SQL Server 2008 Standard/Enterprise or later • Microsoft SQL Server 2008 Standard/Enterprise R2 • Microsoft SQL Server 2008 64-bit Standard/Enterprise or later • Microsoft SQL Server 2008 64-bit Standard/Enterprise R2 • Microsoft SQL Server 2005 Express SP2/SP3 • Microsoft SQL Server 2005 Standard/Enterprise SP2/SP3 • Microsoft SQL Server 2005 64-bit Standard/Enterprise SP2/SP3
IIS Server application	• Microsoft IIS server 7.5 (For 2008 R2 platforms) • Microsoft IIS server 7.0 (For 2008 platforms) • Microsoft IIS server 6.0 (For 2003 platforms)
Network protocol	• TCP/IP • UDP for heartbeat • HTTP • HTTPS
Display	VGA (1024 x 768 / 256 color) or higher

TABLE 2-1. Control Manager Server System Requirements (Continued)

COMPONENT	REQUIREMENT
Others	• Microsoft .NET Framework 2.0/3.0/3.5 • Visual C++ 2005 Redistribution • FastCGI 6.1.36.1 • PHP 5.2.9 • ASP.Net • Microsoft Message Queue **Note:** Control Manager installs the above components, if they are not installed on the server. However: - Microsoft Message Queue must be installed manually for all platforms - On Windows Server 2008, the following need to be installed manually: - ASP.Net - IIS 6 Management compatibility components.

TABLE 2-2. Control Manager Management Console System Requirements

COMPONENT	REQUIREMENT
Web Browser	Microsoft Internet Explorer 7.0 or later
Other	Adobe™ Flash™ version 8 or later

General Recommendations

- Do not install Control Manager on a Primary Domain Controller (PDC), a Backup Domain Controller (BDC), or on a server with any other Trend Micro product. Doing so can result in severe performance degradation.
- Physical memory is a system resource, meaning all applications on the server share it. Scale the memory with the processor; do not overpopulate with memory.

TABLE 2-1. General Control Manager server recommendations

HARDWARE/SOFTWARE SPECIFICATION	RECOMMENDED REQUIREMENT
Network adapter	100Mbps, 32-bit, adapter for both the Control Manager server and managed product. Preferably one designed for bus mastering, direct memory access (DMA)
File system	NT File System (NTFS) partition
Monitor	VGA monitor capable of 1024 x 768 resolution, with at least 256 colors.

Pre-Installation Tasks

If PHP already exists on the server where Control Manager will install, you must add `php_http.dll` to the `...PHP/ext` folder and edit the `php.ini` file. If the `php_http.dll` file is not added and the `php.ini` file is not modified, Control Manager widgets will not function properly.

To add the php_http.dll file and modify the php.ini:

1. Stop the web server.
2. Copy the `php_http.dll` file from the Control Manager folder `CD drive:\Control Manager\PHP` to the following location:

   ```
   ...\PHP\ext
   ```
3. Edit the end of the `PHP.ini` file with the following:

```
[PHP_HTTP]
extension=php_http.dll
```

4. Verify that all of the following appear at the end of the `PHP.ini` file:

```
[PHP_GMP]
extension=php_gmp.dll
[PHP_LDAP]
extension=php_ldap.dll
[PHP_MCRYPT]
extension=php_mcrypt.dll
[PHP_OPENSSL]
extension=php_openssl.dll
[PHP_PDO]
extension=php_pdo.dll
[PHP_PDO_SQLITE]
extension=php_pdo_sqlite.dll
[PHP_HTTP]
extension=php_http.dll
```

5. Restart the web server.
6. Install Control Manager 5.5.

Installing a Control Manager Server

After deciding on the topology to use for your network, you can begin to install your Control Manager server. See *Server Address Checklist* on page A-2 to help you record relevant information for installation.

You need the following information for the installation:

- Relevant target server address and port information
- Control Manager Registration Key

- Security Level 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, 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 authentication and SQL authentication 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 Server 2005 Express 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 5.5 instead of doing a fresh installation.

To install a Control Manager server:

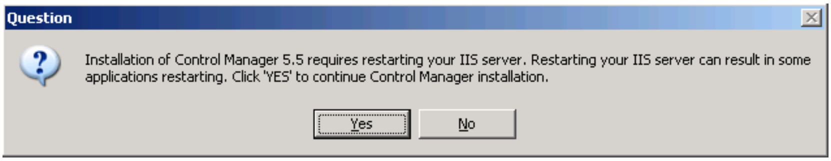
Step 1: Install all required components

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 DVD, go to the Control Manager folder on the DVD. If you downloaded the software from the Trend Micro website, 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:

   - **.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

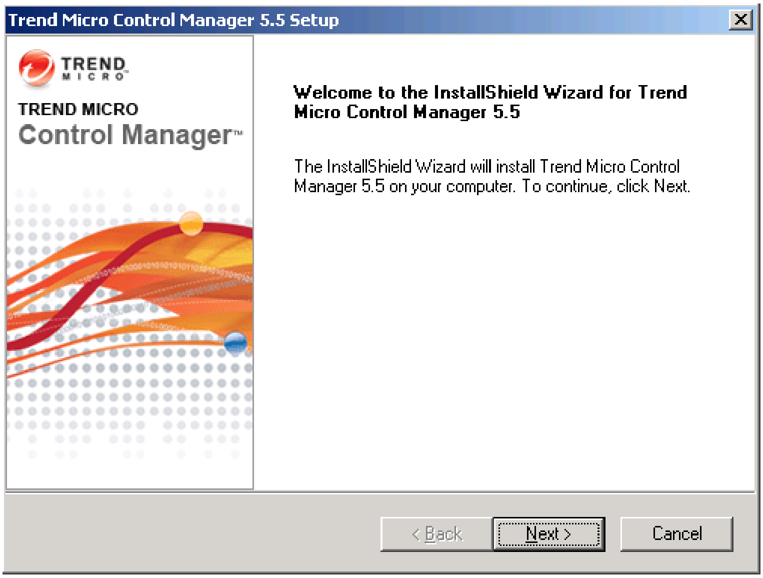
2. Install all missing components. The IIS confirmation dialog box appears.



Question

Installation of Control Manager 5.5 requires restarting your IIS server. Restarting your IIS server can result in some applications restarting. Click 'YES' to continue Control Manager installation.

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

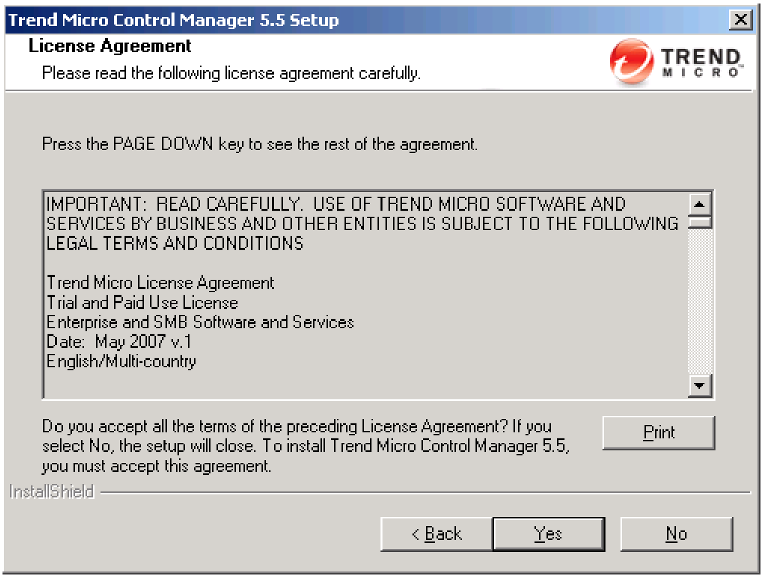


Welcome to the InstallShield Wizard for Trend Micro Control Manager 5.5

The InstallShield Wizard will install Trend Micro Control Manager 5.5 on your computer. To continue, click Next.

The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the Microsoft Management Console. For more information about migration, see *Migration Scenarios for Control Manager 2.x Agents* on page 4-15.

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



Trend Micro Control Manager 5.5 Setup

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

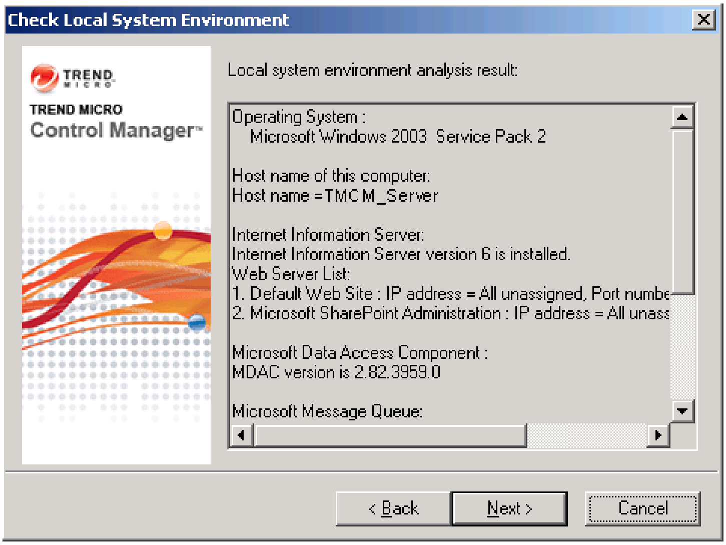
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement
Trial and Paid Use License
Enterprise and SMB Software and Services
Date: May 2007 v.1
English/Multi-country

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Trend Micro Control Manager 5.5, you must accept this agreement.

FIGURE 2-1. Click 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.



Check Local System Environment

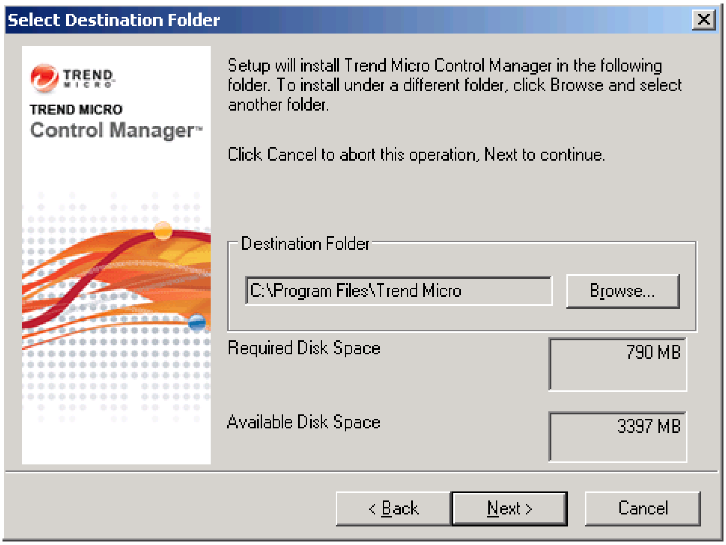
Local system environment analysis result:

```
Operating System :
   Microsoft Windows 2003  Service Pack 2

Host name of this computer:
Host name =TMCM_Server

Internet Information Server:
Internet Information Server version 6 is installed.
Web Server List:
1. Default Web Site : IP address = All unassigned, Port numbe
2. Microsoft SharePoint Administration : IP address = All unass

Microsoft Data Access Component :
MDAC version is 2.82.3959.0

Microsoft Message Queue:
```

FIGURE 2-2. Displays local system environment information

Step 2: Specify the installation location

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



Select Destination Folder

Setup will install Trend Micro Control Manager in the following folder. To install under a different folder, click Browse and select another folder.

Click Cancel to abort this operation, Next to continue.

Destination Folder: C:\Program Files\Trend Micro

Required Disk Space: 790 MB

Available Disk Space: 3397 MB

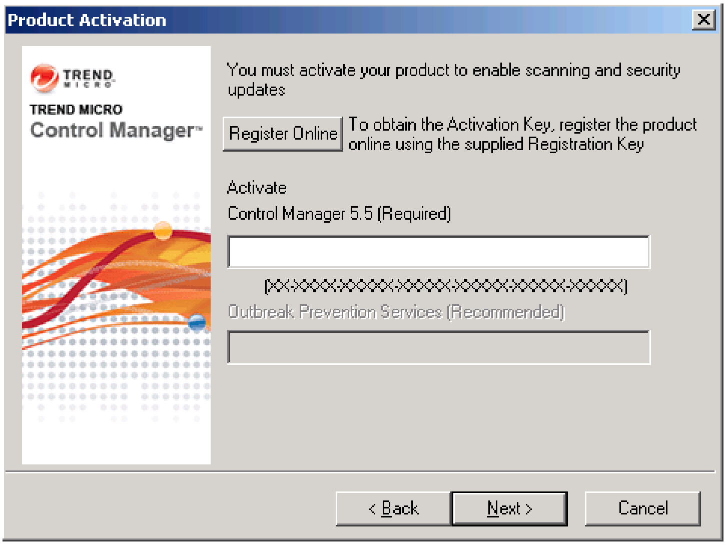
FIGURE 2-3. Select a destination folder

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 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.



Product Activation

You must activate your product to enable scanning and security updates

To obtain the Activation Key, register the product online using the supplied Registration Key

Activate

Control Manager 5.5 (Required)

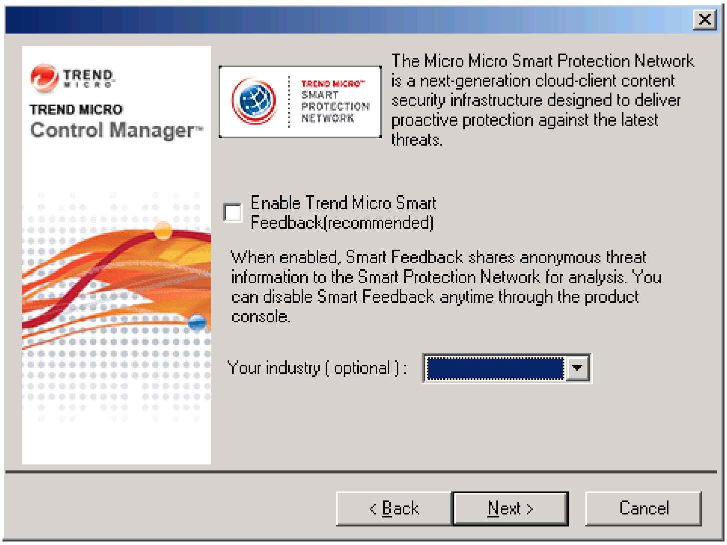
(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Outbreak Prevention Services (Recommended)

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 5.5 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 on the Trend Micro Online Registration website and obtain an Activation Code.

3. Click **Next**. The Smart Protection Network screen appears.



The Micro Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

□ Enable Trend Micro Smart Feedback(recommended)

When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. You can disable Smart Feedback anytime through the product console.

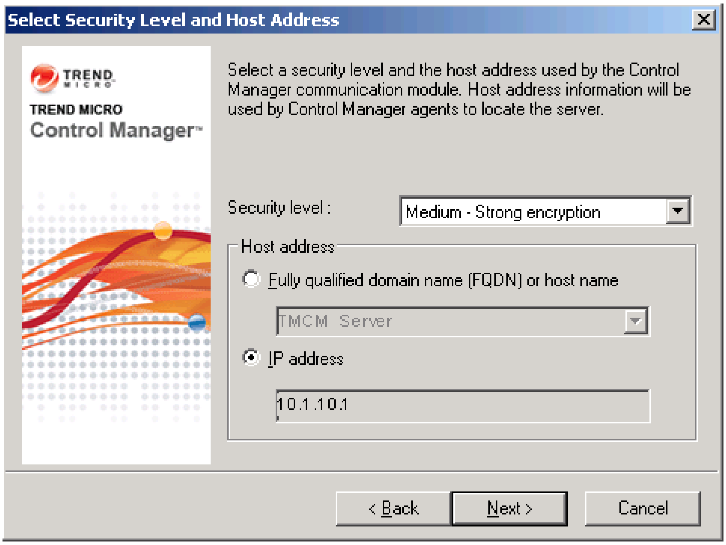
Your industry (optional) :

FIGURE 2-5. Smart Protection Network Settings

4. Select **Enable Trend Micro Smart Feedback** to participate in the Smart Protection Network program. When you choose to participate, Control Manager sends anonymous threat information to Trend Smart Protection Network servers. This allows proactive protection of your network. You can stop participating any time through the Control Manager web console.

Step 4: Specify Control Manager security and Web server settings

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



Select Security Level and Host Address

Select a security level and the host address used by the Control Manager communication module. Host address information will be used by Control Manager agents to locate the server.

Security level : Medium - Strong encryption

Host address

○ Fully qualified domain name (FQDN) or host name

TMCM Server

● IP address

10.1.10.1

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. Administrators have to reinstall Control Manager if the server's IP address must change. Install using a host name to avoid 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.

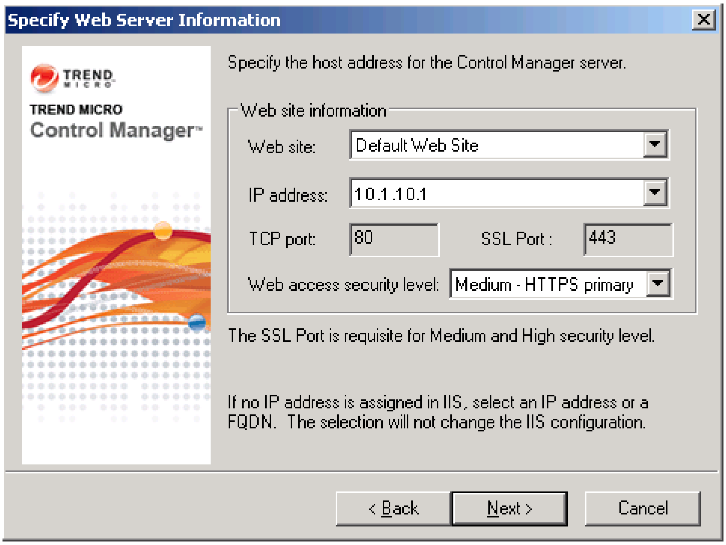
To use an IP address:

a. Select **IP address**.

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

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.



Specify Web Server Information

Specify the host address for the Control Manager server.

Web site information

Web site: Default Web Site

IP address: 10.1.10.1

TCP port: 80

SSL Port : 443

Web access security level: Medium - HTTPS primary

The SSL Port is requisite for Medium and High security level.

If no IP address is assigned in IIS, select an IP address or a FQDN. The selection will not change the IIS configuration.

FIGURE 2-7. **Specify Web server information**

5. From the **Web site** list, select the website 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.

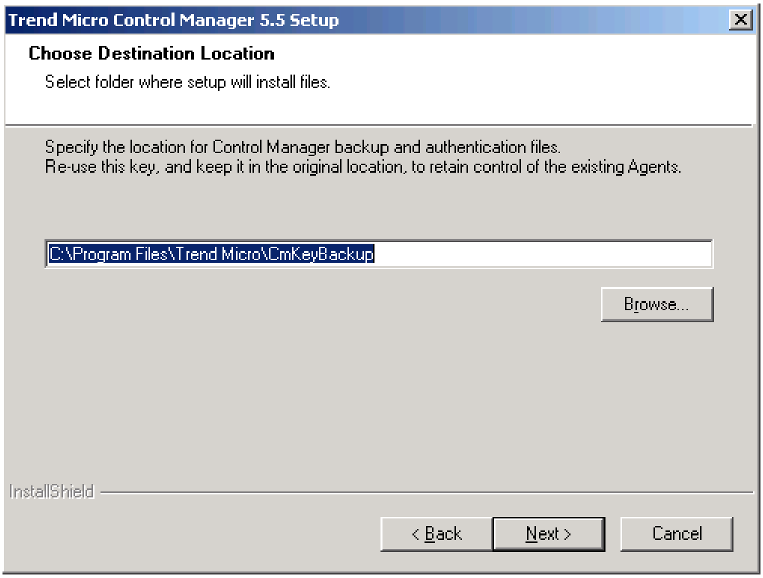
   If your server has more than one network interface card, or if you assign your server more than one FQDN, the names and IP addresses appear here. Choose the most appropriate address or name by selecting the corresponding option or item in the list.

   If you use the host name or FQDN to identify your server, make sure that this name can be resolved on the product computers; 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 between 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 IIS 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.



Trend Micro Control Manager 5.5 Setup

Choose Destination Location

Select folder where setup will install files.

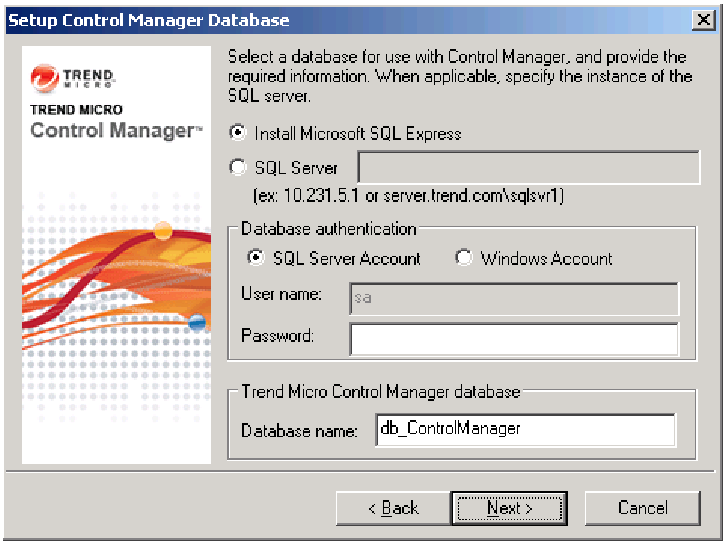
Specify the location for Control Manager backup and authentication files.
Re-use this key, and keep it in the original location, to retain control of the existing Agents.

C:\Program Files\Trend Micro\CmKeyBackup

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

2. Specify the location of the Control Manager backup and authentication files (for more information see the *Control Manager files that should be backed up* on page 4-8). Click **Browse** to specify an alternate location.

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



Setup Control Manager Database

Select a database for use with Control Manager, and provide the required information. When applicable, specify the instance of the SQL server.

● Install Microsoft SQL Express

○ SQL Server

(ex: 10.231.5.1 or server.trend.com\sqlsvr1)

Database authentication

● SQL Server Account ○ Windows Account

User name: sa

Password:

Trend Micro Control Manager database

Database name: db_ControlManager

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 computer. Do not forget to specify a password for this database in the field provided.

Tip: Microsoft SQL Server 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.

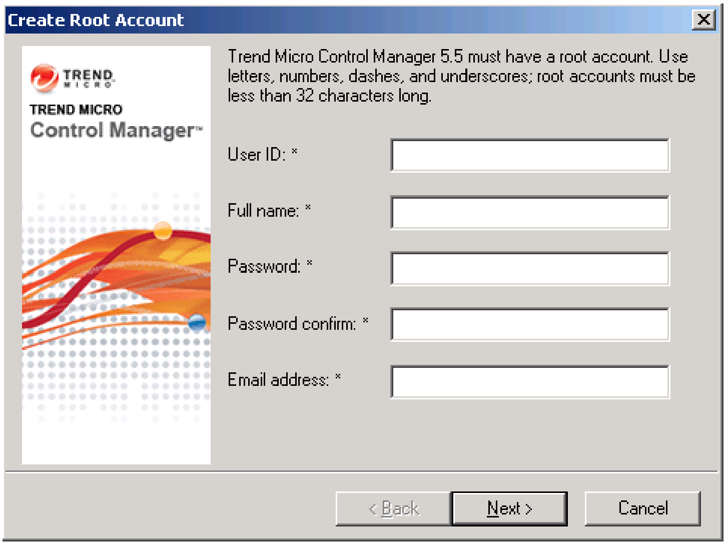
   Note: When installing Control Manager 5.5, you cannot select **Append new records to existing database** for previous Control Manager database versions.

   - **Delete existing records, and create a new database:** The existing database is deleted, and another is created using the same name.
   - **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:



Create Root Account

Trend Micro Control Manager 5.5 must have a root account. Use letters, numbers, dashes, and underscores; root accounts must be less than 32 characters long.

User ID: *

Full name: *

Password: *

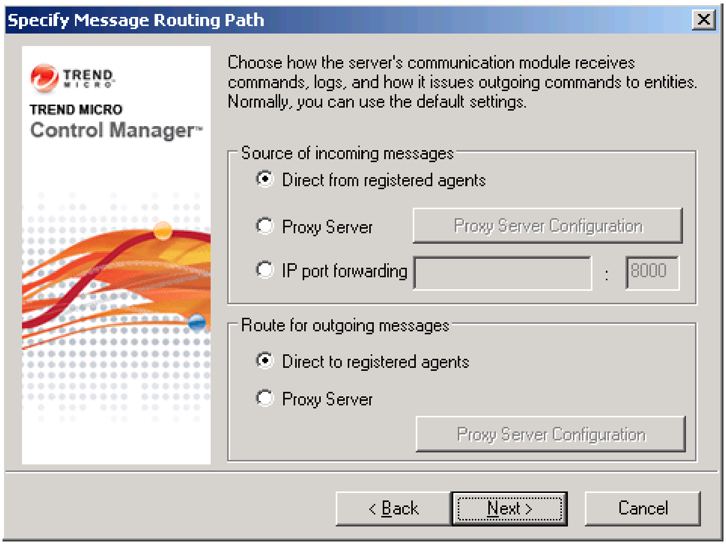
Password confirm: *

Email address: *

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

2. Provide the following required account information:
   - 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.



Specify Message Routing Path

Choose how the server's communication module receives commands, logs, and how it issues outgoing commands to entities. Normally, you can use the default settings.

Source of incoming messages

● Direct from registered agents

○ Proxy Server

○ IP port forwarding : 8000

Route for outgoing messages

● Direct to registered agents

○ Proxy Server

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.

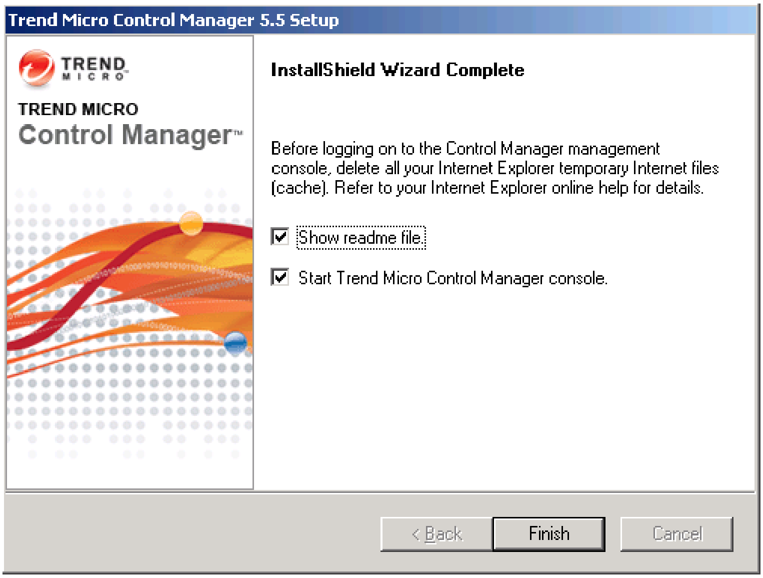
Source of incoming messages

- **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.



Trend Micro Control Manager 5.5 Setup

InstallShield Wizard Complete

Before logging on to the Control Manager management console, delete all your Internet Explorer temporary Internet files (cache). Refer to your Internet Explorer online help for details.

☑ Show readme file.

☑ Start Trend Micro Control Manager console.

FIGURE 2-12. Setup complete

Verifying Successful Installations

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

Verify a Successful Control Manager Server Installation

To confirm a successful Control Manager server installation, check the items in the following table.

TABLE 2-3. Control Manager Installation Verification

ITEM	DESCRIPTION
Control Panel > Add/Remove Programs dialog	The following programs appear in Add/Remove Programs: • Trend Micro Command CGI • Trend Micro Control Manager • Trend Micro Management Infrastructure • Crystal Report Runtime Files (optional component) • Microsoft Visual C++ 2005 Redistributable (latest version) • FastCGI • PHP • SQL Server 2005 Express SP3 (if installed with Control Manager 5.5)
`C:\Program Files`	The following folders appear under the directory: • `Trend Micro\Common\TMI` • `Trend Micro\Common\CCGI` • `Trend Micro\Control Manager` • `PHP` (The PHP folder should be created by the Control Manager installation)

TABLE 2-3. Control Manager Installation Verification (Continued)

ITEM	DESCRIPTION
Control Manager Database files	• db_ControlManager.mdf • db_ControlManager_Log.LDF
The Setup program creates the following services and processes	
Control Manager Services	• Trend Micro Control Manager • Trend Micro Common CGI • Trend Micro Management Infrastructure • Trend Micro Network Time Protocol
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

TABLE 2-3. Control Manager Installation Verification (Continued)

ITEM	DESCRIPTION
Message Queue process	LogProcessor.exe

Post-installation Configuration

After successfully installing Control Manager, Trend Micro recommends you perform the following post-installation configuration tasks.

1. Configure user accounts and account types
2. Download the latest components
3. Set notifications

Registering and Activating Control Manager

After successfully installing Control Manager, please check the license status and expiration date on the web console, by clicking **Administration** > **License Management > Control Manager**. If the status is not *Activated* or is expired, obtain an Activation Code and activate your software (on the web console, click **Administration > License Management > Control Manager > Specify a new Activation Code**).

Configuring User Accounts

Create Control Manager user accounts based on your needs. Consider the following when creating your accounts:

- The number of different user types (Administrators, Power Users, and Operators)
- Assign appropriate permissions and privileges to each kinds of user types
- For users to take advantage of the cascading management structure, they need to have Power User rights or greater

Downloading the Latest Components

After installation, manually download the latest components (Pattern files\Cleanup templates, Engine updates) from the Trend Micro ActiveUpdate server to help maintain the highest security protection. If a proxy server exists between a Control Manager server and the Internet, configure the proxy server settings (on the web console, click **Administration > Settings > Proxy Settings**).

Setting Notifications

After installation, configure the events that will trigger notifications to monitor significant virus/malware attacks and related security activities. Besides specifying notification recipients, choose notification channels and test them to make sure they work as expected (on the web console, click **Administration > Event Center**).

Registering and Activating Your Software

Activate the Control Manager server to keep your security and product updates current. To activate your product, 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 all of its features, 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:

Path: Administration > License Management > Control Manager

1. Navigate to the License Information screen.
2. Click the **Activate the product/Specify a new Activation Code** link.
3. 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 website to obtain one.
4. Click **Activate**, and then click **OK**.

Converting to the Full Version

Activate your Control Manager to continue to use it beyond the evaluation period. Activate Control Manager to use its full functionality including downloading updated program components.

To convert to the full version:

1. Purchase a full version Registration Key from a Trend Micro reseller.
2. Register your software online.
3. Obtain an Activation Code.
4. Activate Control Manager according to the instructions in the procedure above.

Renewing Your Product Maintenance

Renew maintenance for Control Manager or its integrated related products and services (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:

Path: Administration > License Management > Control Manager

1. Navigate to the License Information screen.
2. On the working area under **Control Manager License Information**, click **Check Status Online**, and then click **OK**.
3. Log off and then log on to the web console for changes to take effect.

To renew maintenance by manually entering an updated Activation Code:

Path: Administration > License Management > Control Manager

1. Navigate to the License Information screen.
2. On the working area under **Control Manager License Information**, click the **Activate the product** link.
3. Click the **Specify a new Activation Code** link and follow the instructions on the Online Registration website.
4. In the **New** box, type your Activation Code.
5. Click **Activate**.
6. 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 on page 3-2
- Configuring Control Manager User Access on page 3-9
- What Each User Views and Can Perform on page 3-34
- Configuring User Groups on page 3-40
- Downloading and Deploying New Components on page 3-43

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

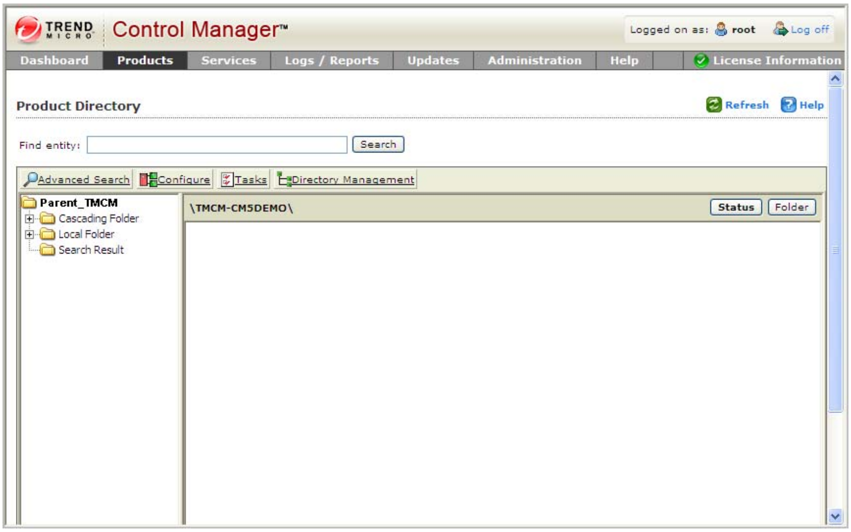
GROUPING TYPE	ADVANTAGE	DISADVANTAGE
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure,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

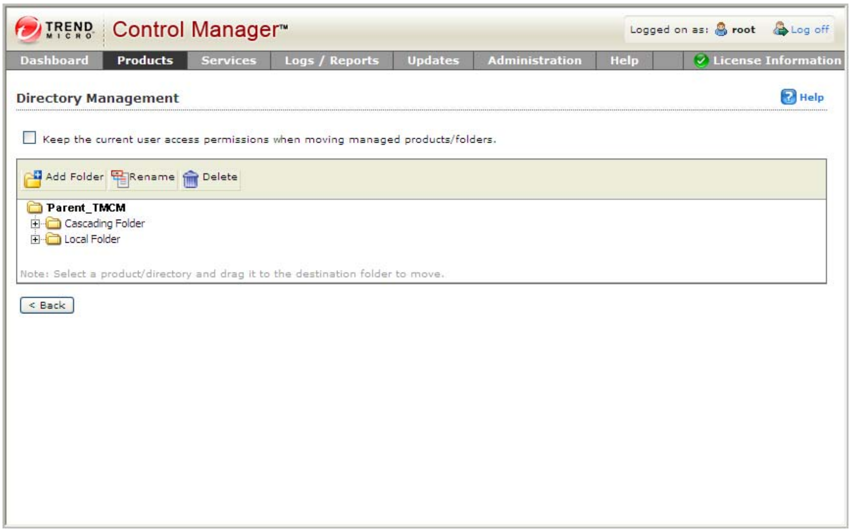
Note: Control Manager reorders structures alphabetically after you specify your Product Directory structure using the Directory Management dialog box.

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 2-25 for more information.
2. Click **Products** from the main menu. The Product Directory screen appears.



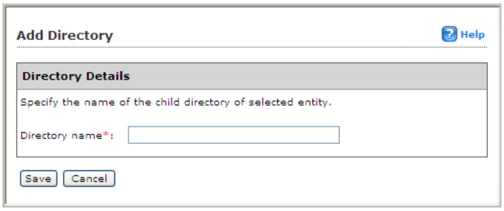
3. Click **Directory Management** on the Product Directory menu. The Directory Management screen appears.



□ Keep the current user access permissions when moving managed products/folders.

Note: Select a product/directory and drag it to the destination folder to move.

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



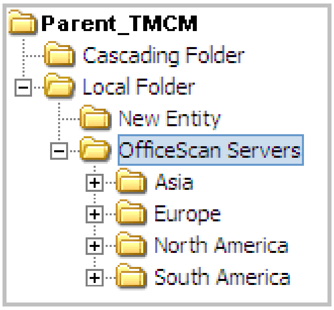
Specify the name of the child directory of selected entity.

Directory name*:

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:



Parent_TMCM
Cascading Folder
Local Folder
New Entity
OfficeScan Servers
Asia
Europe
North America
South America

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

    Asia:

    - Japan
    - India
    - China

    Europe:

    - France
    - Germany
    - England

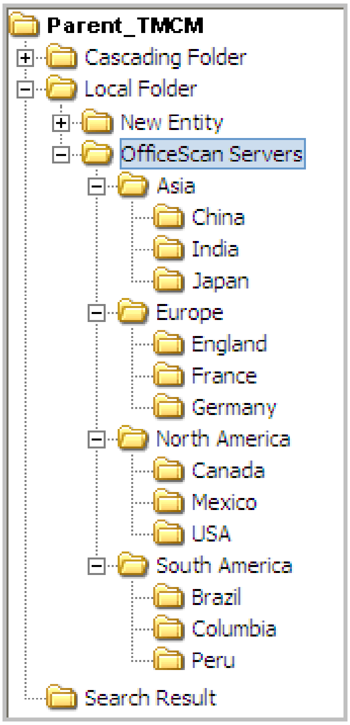
    North America:

    - Canada
    - Mexico
    - United States of America

    South America

    - Peru
    - Brazil
    - Columbia

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



- Parent_TMCM
  - Cascading Folder
  - Local Folder
    - New Entity
    - OfficeScan Servers
      - Asia
        - China
        - India
        - Japan
      - Europe
        - England
        - France
        - Germany
      - North America
        - Canada
        - Mexico
        - USA
      - South America
        - Brazil
        - Columbia
        - Peru
  - Search Result

11. Repeat the process for the following managed products:
    - **IWSS and IWSVA**
    - **IMSS and IMSVA**
    - **TDA**
    - **TMTM**

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.

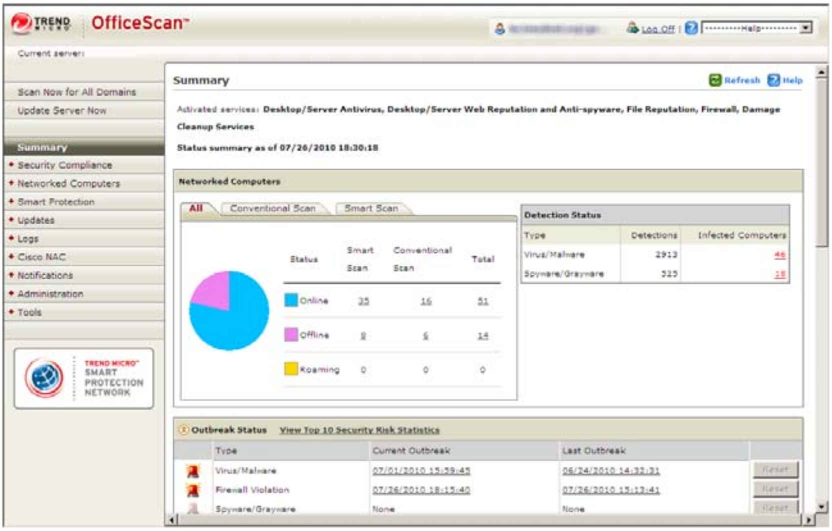
Registering Managed Products to Control Manager

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.



Summary

Activated services: **Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Firewall, Damage Cleanup Services**

Status summary as of 07/26/2010 18:30:18

Networked Computers

Status	Smart Scan	Conventional Scan	Total
🟦 Online	35	16	51
🟪 Offline	8	6	14
🟨 Roaming	0	0	0

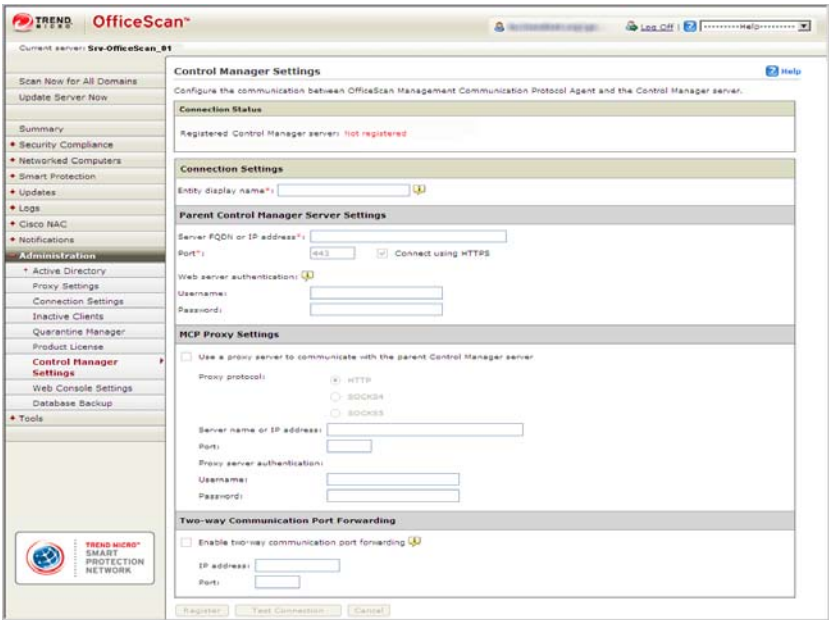
Detection Status

Type	Detections	Infected Computers
Virus/Malware	2913	46
Spyware/Grayware	325	18

Outbreak Status

Type	Current Outbreak	Last Outbreak
Virus/Malware	07/01/2010 15:59:45	06/24/2010 14:32:31
Firewall Violation	07/26/2010 18:15:40	07/26/2010 15:13:41
Spyware/Grayware	None	None

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



Control Manager Settings

Configure the communication between OfficeScan Management Communication Protocol Agent and the Control Manager server.

Connection Status

Registered Control Manager server: Not registered

Connection Settings

Entity display name*:

Parent Control Manager Server Settings

Server FQDN or IP address*:

Port*: 443 ☑ Connect using HTTPS

Web server authentication:

Username:

Password:

MCP Proxy Settings

□ Use a proxy server to communicate with the parent Control Manager server

Proxy protocol: ● HTTP ○ SOCKS4 ○ SOCKS5

Server name or IP address:

Port:

Proxy server authentication:

Username:

Password:

Two-way Communication Port Forwarding

□ Enable two-way communication port forwarding

IP address:

Port:

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

TABLE 3-2. Control Manager User Account Options

SECTION	DESCRIPTION
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 on page 3-12 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 10.5	Alex	Blair	Chris	Dana
Control Manager	Erin			

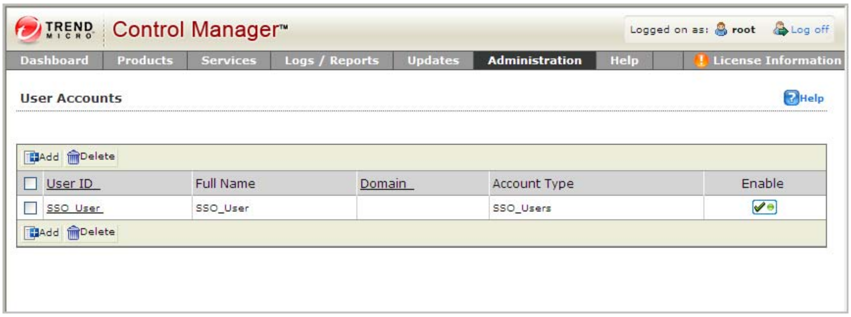
Adding a User Account for Alex (Global Administrator)

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:

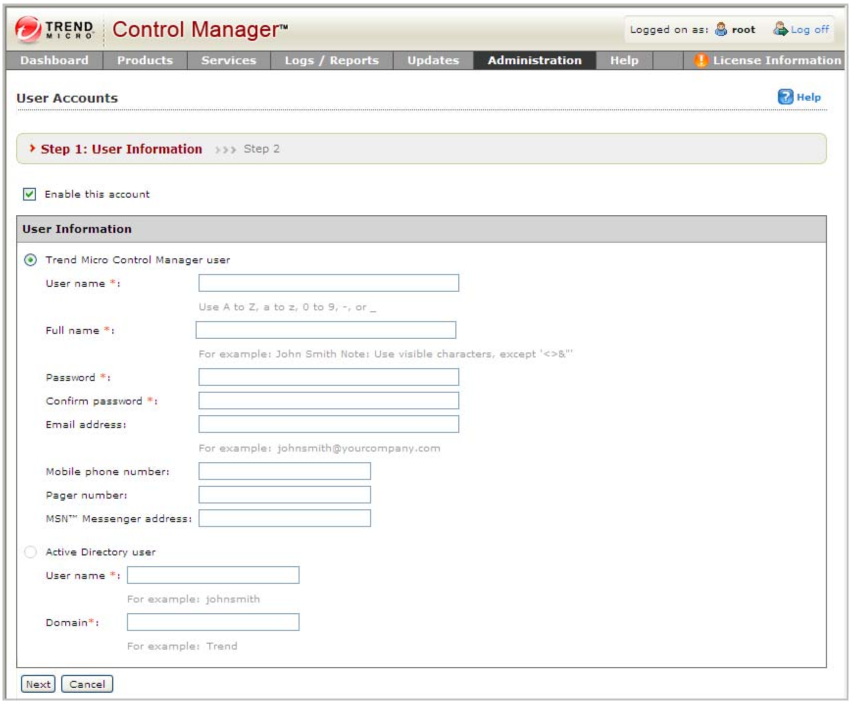
Path: Administration > Account Management > User Accounts

1. Navigate to the User Accounts screen



□	User ID	Full Name	Domain	Account Type	Enable
□	SSO_User	SSO_User		SSO_Users	✓

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



User Accounts

› Step 1: User Information ››› Step 2

☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:

Use A to Z, a to z, 0 to 9, -, or _

Full name *:

For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:

For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

User name *:

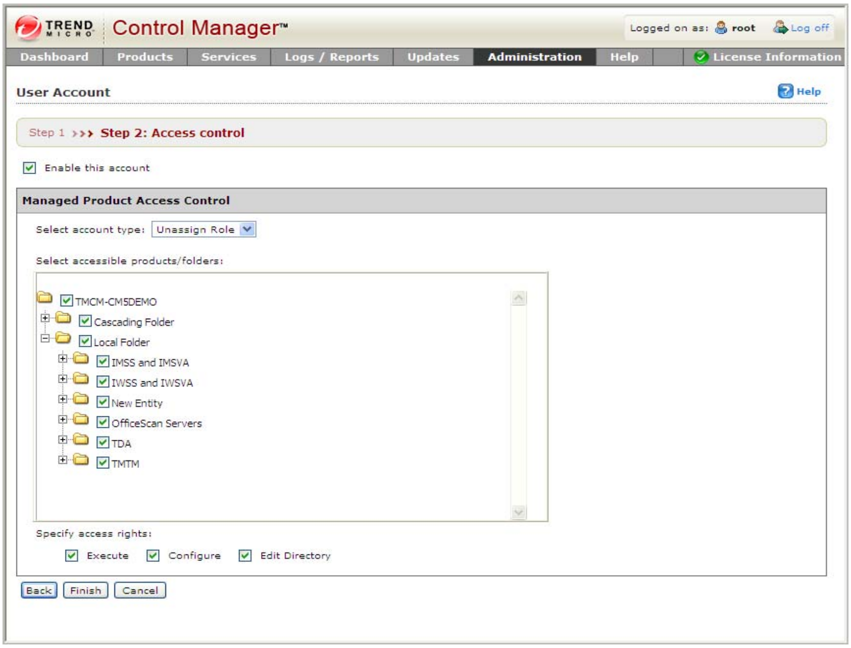
For example: johnsmith

Domain*:

For example: Trend

3. Select **Enable this account** to enable the user.
4. Select **Trend Micro Control Manager user**.
5. 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.

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



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Unassign Role

Select accessible products/folders:

- ☑ TMCM-CM5DEMO
  - ☑ Cascading Folder
  - ☑ Local Folder
    - ☑ IMSS and IMSVA
    - ☑ IWSS and IWSVA
    - ☑ New Entity
    - ☑ OfficeScan Servers
    - ☑ TDA
    - ☑ TMTM

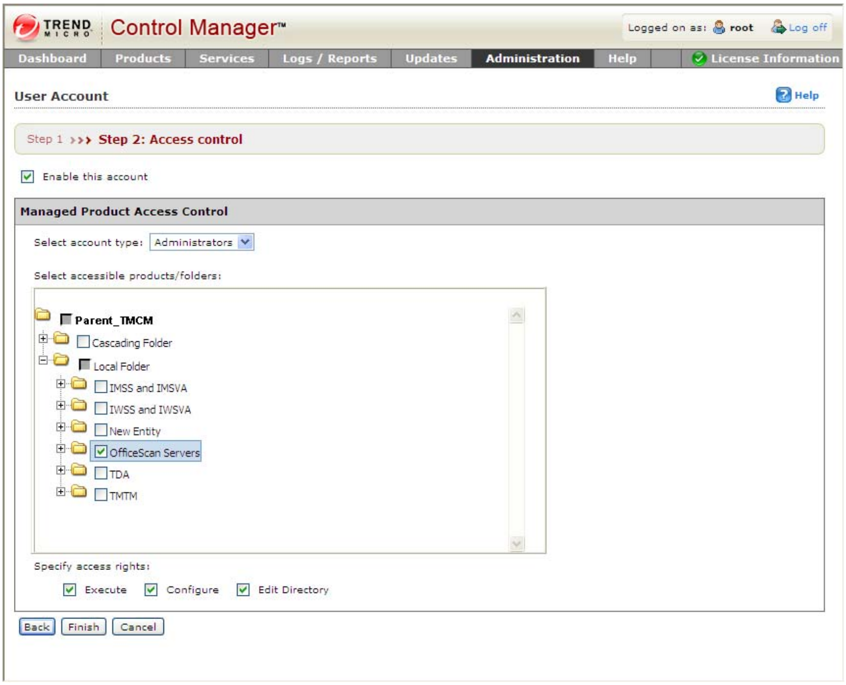
Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

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

8. 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).



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Administrators

Select accessible products/folders:

- ▣ Parent_TMCM
  - □ Cascading Folder
  - ▣ Local Folder
    - □ IMSS and IMSVA
    - □ IWSS and IWSVA
    - □ New Entity
    - ☑ OfficeScan Servers
    - □ TDA
    - □ TMTM

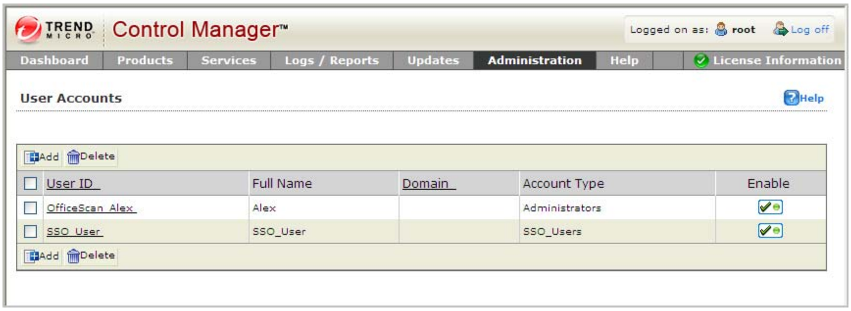
Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

9. 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.

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



User Accounts

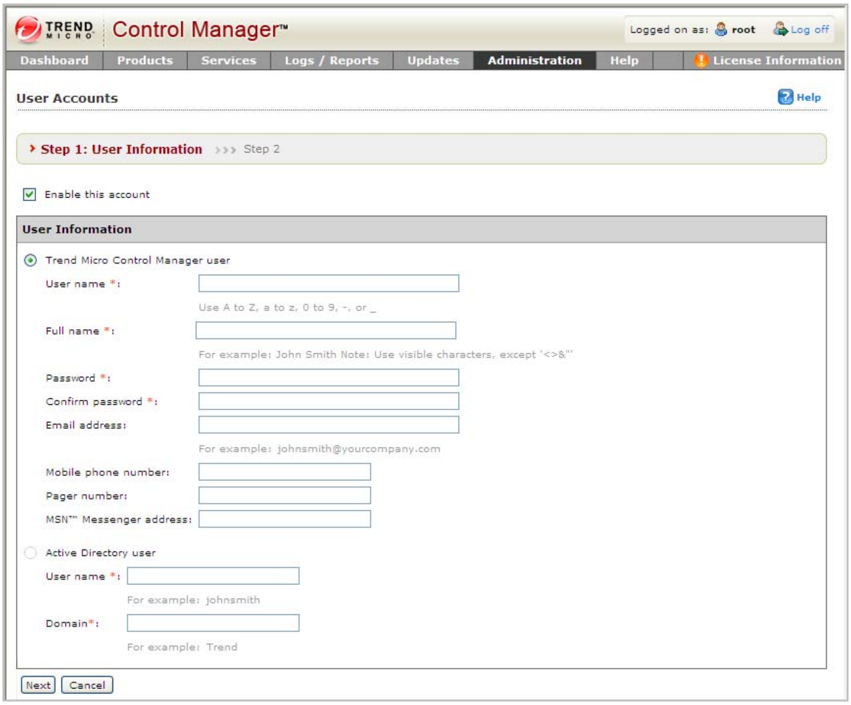
□	User ID	Full Name	Domain	Account Type	Enable
□	OfficeScan_Alex	Alex		Administrators	✓
□	SSO_User	SSO_User		SSO_Users	✓

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.



User Accounts

› Step 1: User Information ››› Step 2

☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:

Use A to Z, a to z, 0 to 9, -, or _

Full name *:

For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:

For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

User name *:

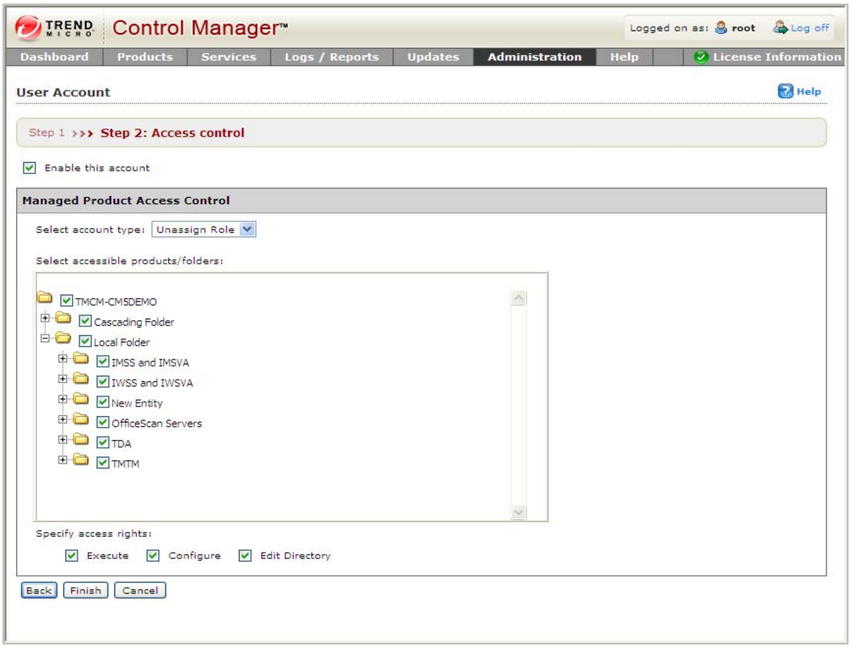
For example: johnsmith

Domain*:

For example: Trend

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.



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Unassign Role

Select accessible products/folders:

- ☑ TMCM-CM5DEMO
  - ☑ Cascading Folder
  - ☑ Local Folder
    - ☑ IMSS and IMSVA
    - ☑ IWSS and IWSVA
    - ☑ New Entity
    - ☑ OfficeScan Servers
    - ☑ TDA
    - ☑ TMTM

Specify access rights:

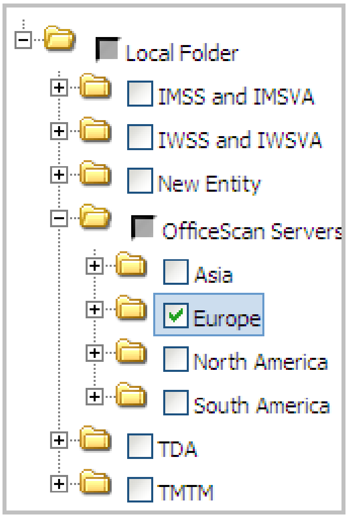
☑ Execute ☑ Configure ☑ Edit Directory

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).

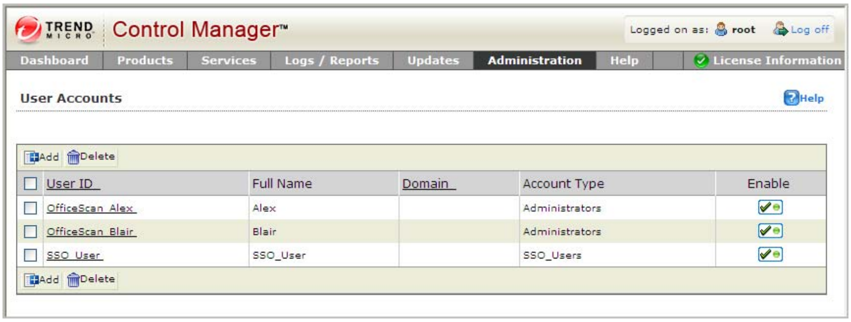


- Local Folder
  - ☐ IMSS and IMSVA
  - ☐ IWSS and IWSVA
  - ☐ New Entity
  - OfficeScan Servers
    - ☐ Asia
    - ☑ Europe
    - ☐ North America
    - ☐ South America
  - ☐ TDA
  - ☐ TMTM

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.



User Accounts

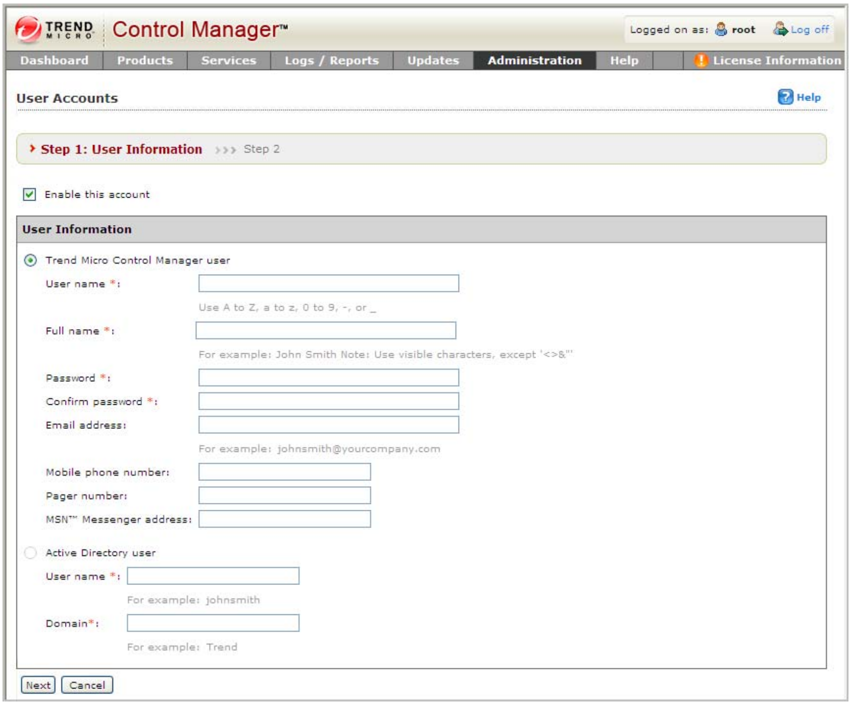
☐	User ID	Full Name	Domain	Account Type	Enable
☐	OfficeScan_Alex	Alex		Administrators	✓
☐	OfficeScan_Blair	Blair		Administrators	✓
☐	SSO_User	SSO_User		SSO_Users	✓

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.



User Accounts

› Step 1: User Information ››› Step 2

☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:
Use A to Z, a to z, 0 to 9, -, or _

Full name *:
For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:
For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

User name *:
For example: johnsmith

Domain*:
For example: Trend

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

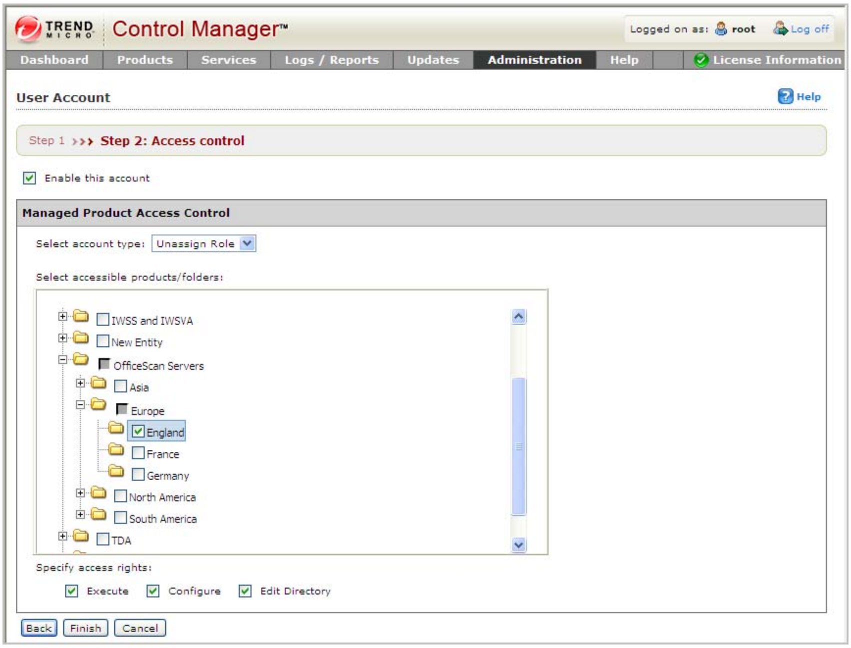
b. **Full name:** Chris

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.



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Unassign Role

Select accessible products/folders:

- □ IWSS and IWSVA
- □ New Entity
- ■ OfficeScan Servers
  - □ Asia
  - ■ Europe
    - ☑ England
    - □ France
    - □ Germany
  - □ North America
  - □ South America
- □ TDA

Specify access rights:

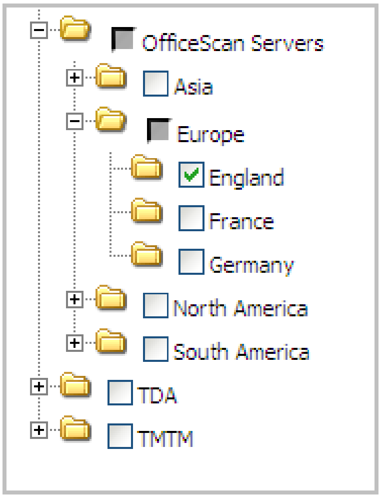
☑ Execute ☑ Configure ☑ Edit Directory

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).

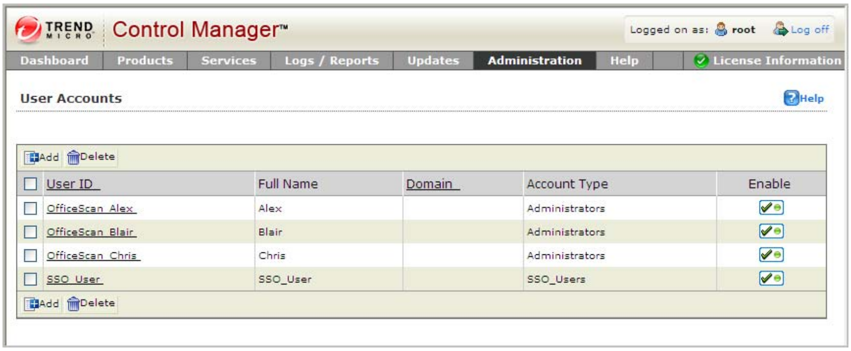


- ■ OfficeScan Servers
  - ☐ Asia
  - ■ Europe
    - ☑ England
    - ☐ France
    - ☐ Germany
  - ☐ North America
  - ☐ South America
- ☐ TDA
- ☐ TMTM

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.



User Accounts

☐	User ID	Full Name	Domain	Account Type	Enable
☐	OfficeScan_Alex	Alex		Administrators	✓
☐	OfficeScan_Blair	Blair		Administrators	✓
☐	OfficeScan_Chris	Chris		Administrators	✓
☐	SSO_User	SSO_User		SSO_Users	✓

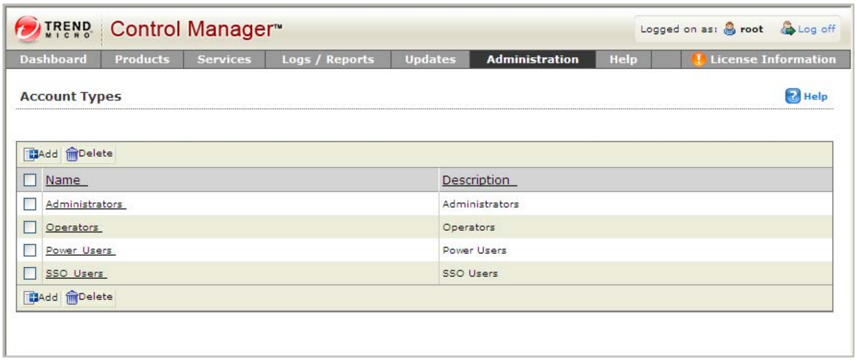
Adding a User Account for Dana (Manager)

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:

Path: Administration > Account Management > Account Types

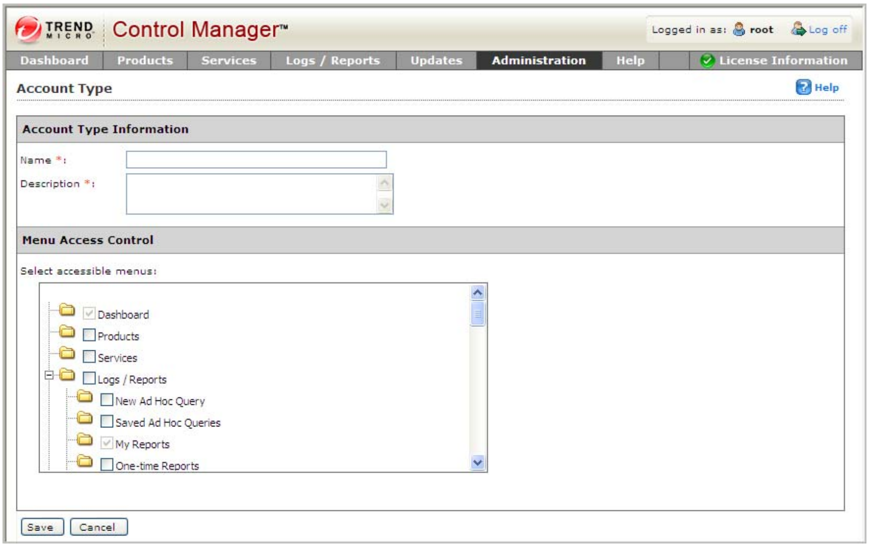
1. Navigate to the Account Types screen.



Account Types

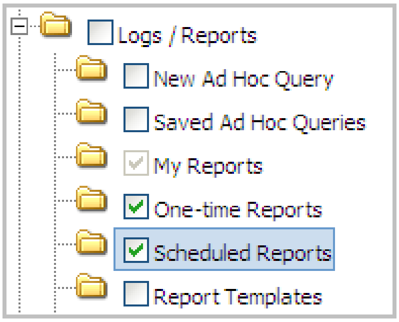
□ Name	Description
□ Administrators	Administrators
□ Operators	Operators
□ Power Users	Power Users
□ SSO Users	SSO Users

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



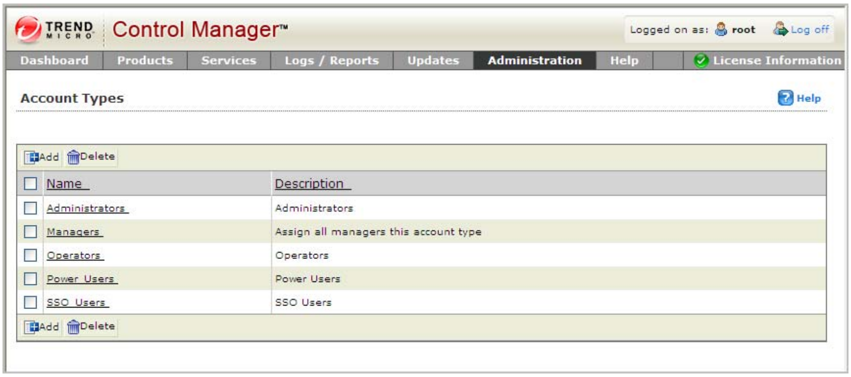
3. Provide the following information for the account type:
   - **Name:** Managers
   - **Description:** Assign all managers this account type
4. Select only the following from the **Select available menus** list:
   - **One-time Reports**
   - **Scheduled Reports**

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.



- □ Logs / Reports
  - □ New Ad Hoc Query
  - □ Saved Ad Hoc Queries
  - ☑ My Reports
  - ☑ One-time Reports
  - ☑ Scheduled Reports
  - □ Report Templates

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



Account Types

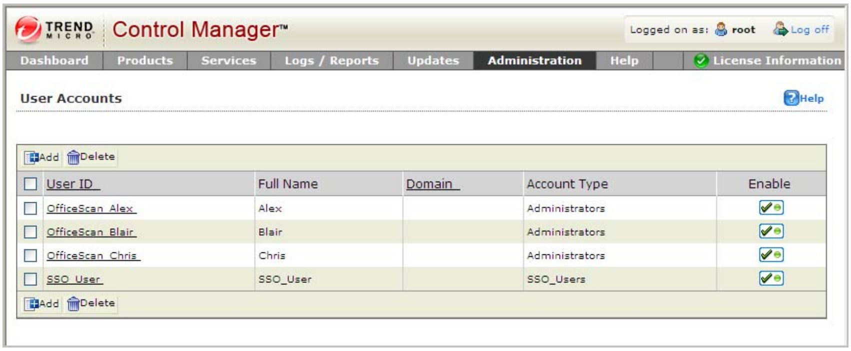
□	Name	Description
□	Administrators	Administrators
□	Managers	Assign all managers this account type
□	Operators	Operators
□	Power Users	Power Users
□	SSO Users	SSO Users

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

To add a user account for Dana:

Path: Administration > Account Management > User Accounts

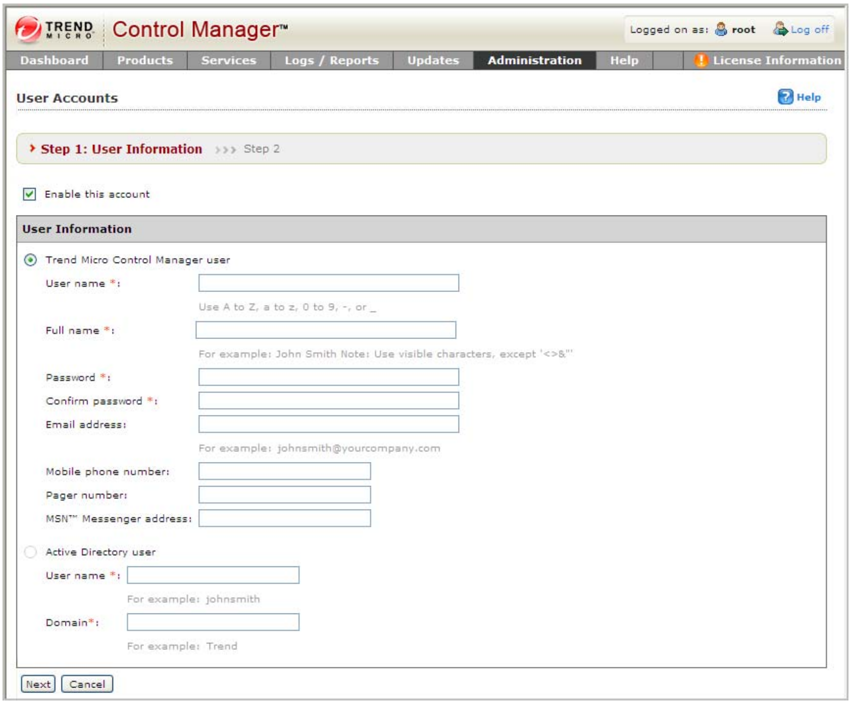
1. Navigate to the User Accounts screen.



User Accounts

□	User ID	Full Name	Domain	Account Type	Enable
□	OfficeScan_Alex	Alex		Administrators	✓
□	OfficeScan_Blair	Blair		Administrators	✓
□	OfficeScan_Chris	Chris		Administrators	✓
□	SSO_User	SSO_User		SSO_Users	✓

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



User Accounts

› Step 1: User Information ››› Step 2

☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:

Use A to Z, a to z, 0 to 9, -, or _

Full name *:

For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:

For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

User name *:

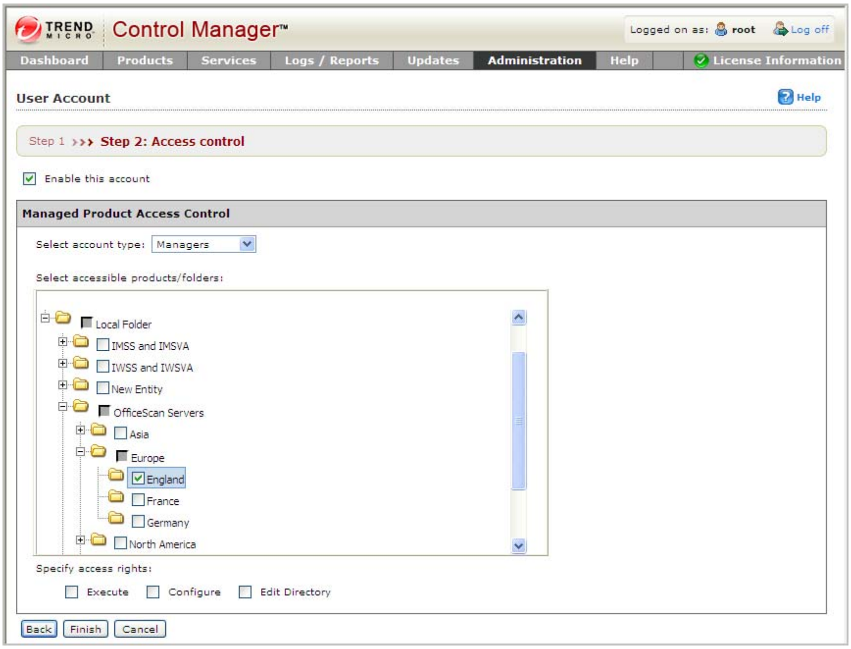
For example: johnsmith

Domain*:

For example: Trend

3. Select **Enable this account** to enable the user.
4. Select **Trend Micro Control Manager user**.
5. 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.

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



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Managers

Select accessible products/folders:

- ▪ Local Folder
  - □ IMSS and IMSVA
  - □ IWSS and IWSVA
  - □ New Entity
  - ▪ OfficeScan Servers
    - □ Asia
    - ▪ Europe
      - ☑ England
      - □ France
      - □ Germany
    - □ North America

Specify access rights:

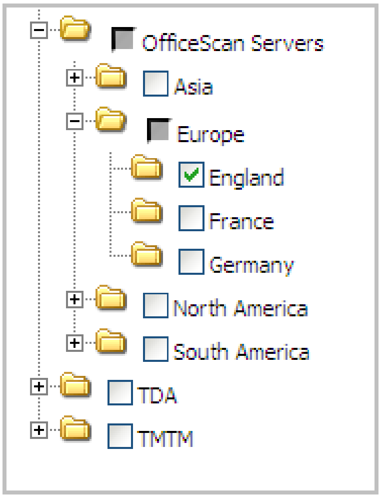
□ Execute □ Configure □ Edit Directory

7. Select **Managers** from the Account Type list.

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

9. 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.

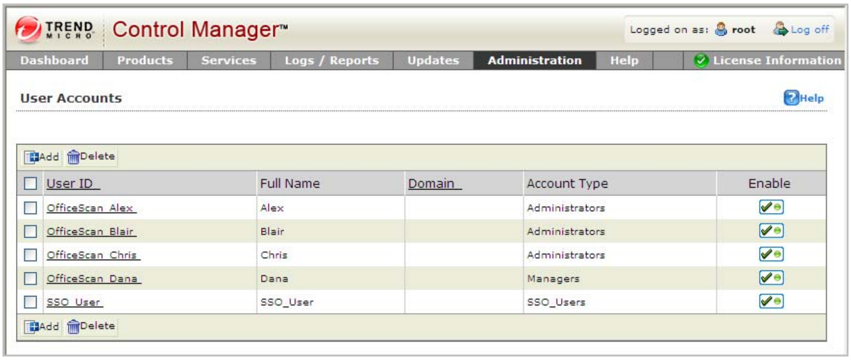


- ■ OfficeScan Servers
  - ☐ Asia
  - ■ Europe
    - ☑ England
    - ☐ France
    - ☐ Germany
  - ☐ North America
  - ☐ South America
- ☐ TDA
- ☐ TMTM

10. 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.

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



User Accounts

☐ User ID	Full Name	Domain	Account Type	Enable
☐ OfficeScan_Alex	Alex		Administrators	✓
☐ OfficeScan_Blair	Blair		Administrators	✓
☐ OfficeScan_Chris	Chris		Administrators	✓
☐ OfficeScan_Dana	Dana		Managers	✓
☐ SSO_User	SSO_User		SSO_Users	✓

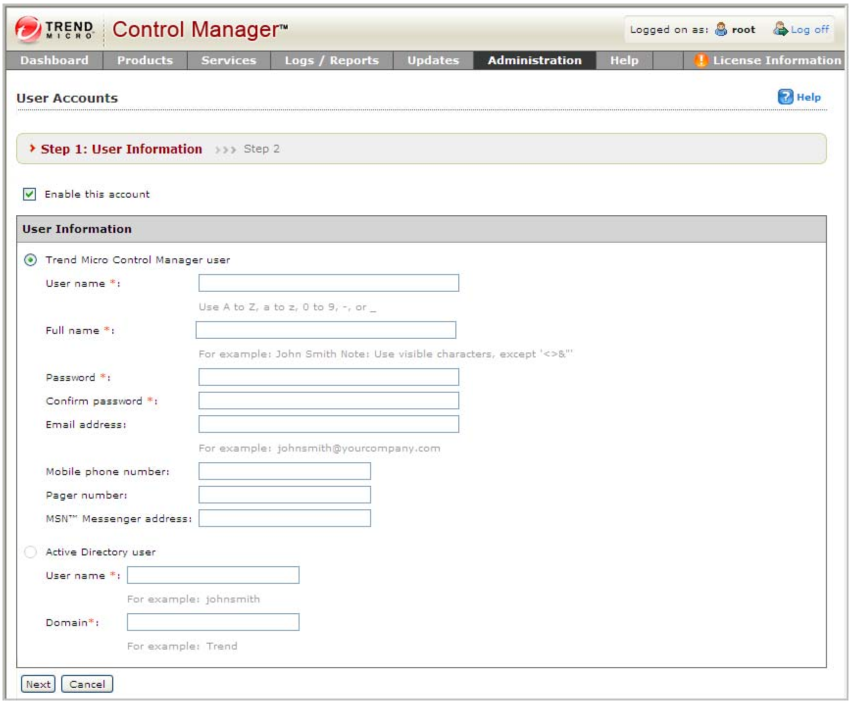
Adding a User Account for Erin (Control Manager Administrator)

You can add all of the user accounts from *Table 3-4* on page 3-12. 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.



☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:

Use A to Z, a to z, 0 to 9, -, or _

Full name *:

For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:

For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

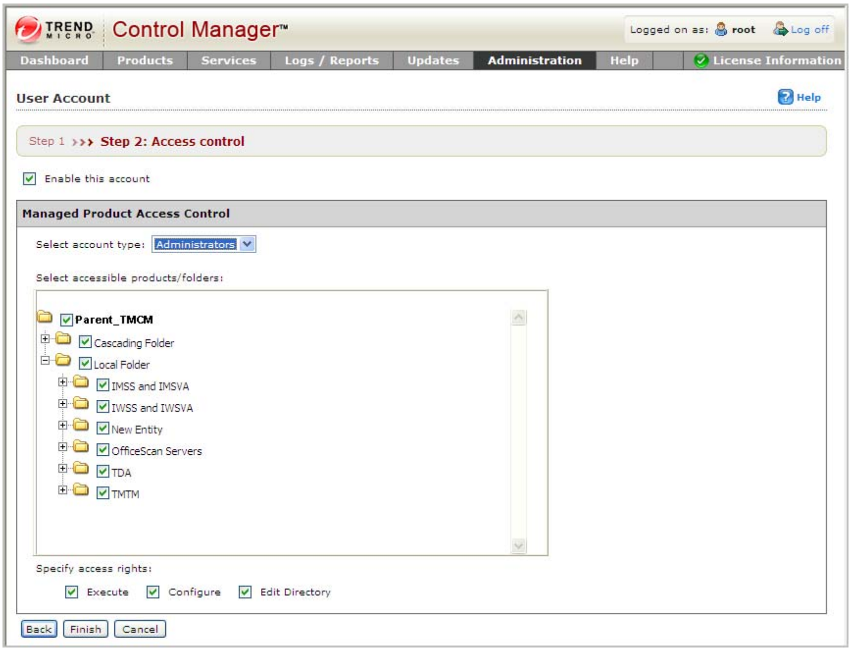
User name *:

For example: johnsmith

Domain*:

For example: Trend

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.



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Administrators

Select accessible products/folders:

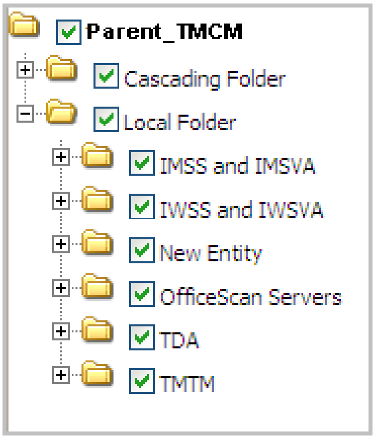
- ☑ Parent_TMCM
  - ☑ Cascading Folder
  - ☑ Local Folder
    - ☑ IMSS and IMSVA
    - ☑ IWSS and IWSVA
    - ☑ New Entity
    - ☑ OfficeScan Servers
    - ☑ TDA
    - ☑ TMTM

Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

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.

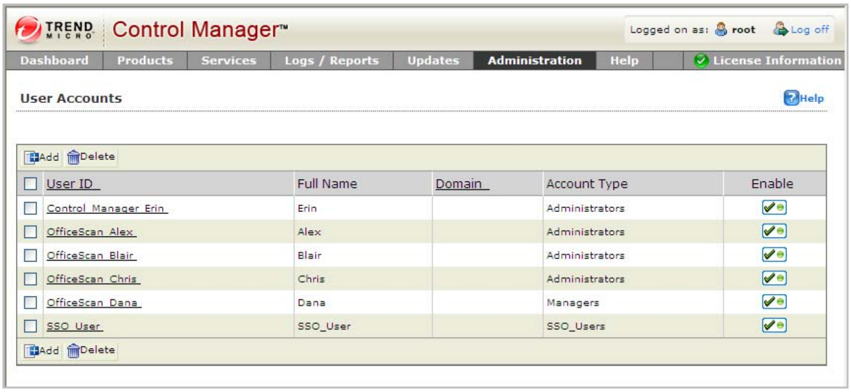


- ☑ **Parent_TMCM**
  - ☑ Cascading Folder
  - ☑ Local Folder
    - ☑ IMSS and IMSVA
    - ☑ IWSS and IWSVA
    - ☑ New Entity
    - ☑ OfficeScan Servers
    - ☑ TDA
    - ☑ TMTM

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.



User Accounts

□	User ID	Full Name	Domain	Account Type	Enable
□	Control_Manager_Erin	Erin		Administrators	✓
□	OfficeScan_Alex	Alex		Administrators	✓
□	OfficeScan_Blair	Blair		Administrators	✓
□	OfficeScan_Chris	Chris		Administrators	✓
□	OfficeScan_Dana	Dana		Managers	✓
□	SSO_User	SSO_User		SSO_Users	✓

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.

TABLE 3-5. User Access (Continued)

USER	DESCRIPTION
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

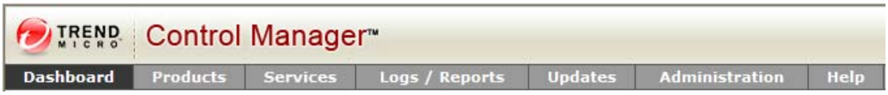
After logging on Alex, Blair, Chris, and Erin see the full main menu for the Control Manager Web console. This is because the users have access to every feature due to their account type (**Administrators**).

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.

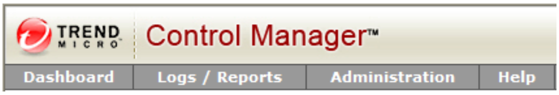
After logging on Dana does not see the complete main menu. Dana's access to the Web console is restricted by her account type (**Managers**).

FIGURE 3-1. Main Menu

MAIN MENU FOR ALEX, BLAIR, CHRIS, AND ERIN



MAIN MENU FOR DANA

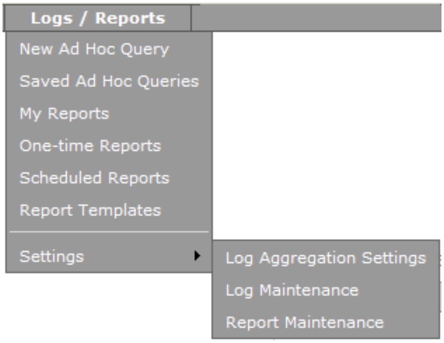
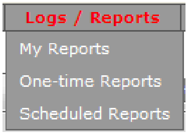


Drop-Down Menus

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
 Logs / Reports New Ad Hoc Query Saved Ad Hoc Queries My Reports One-time Reports Scheduled Reports Report Templates Settings Log Aggregation Settings Log Maintenance Report Maintenance	 Logs / Reports My Reports One-time Reports Scheduled Reports

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

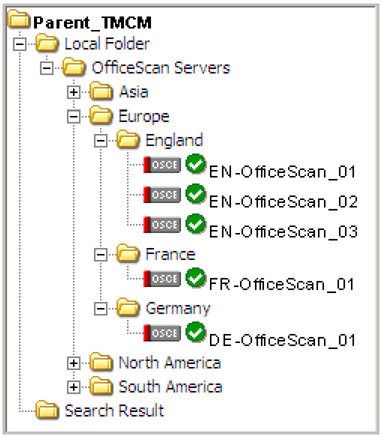
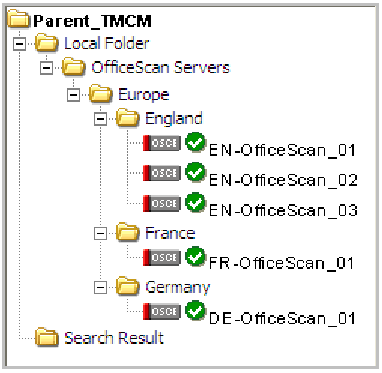
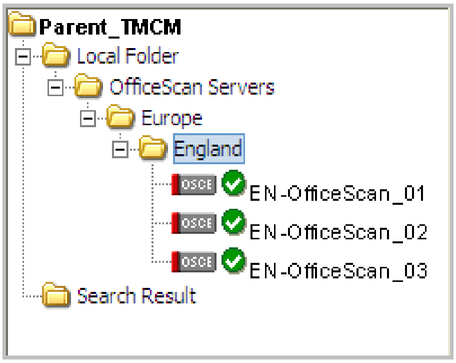
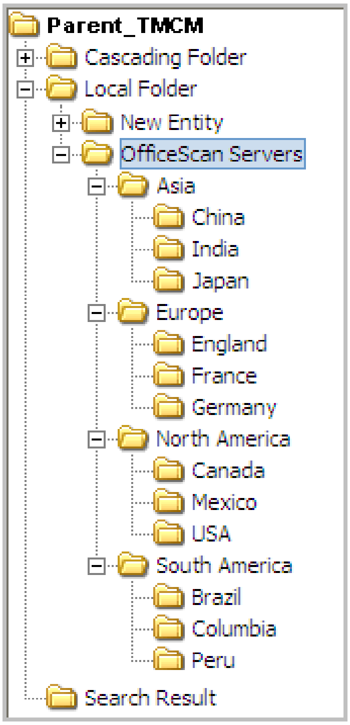
ALEX	BLAIR
Parent_TMCM Local Folder OfficeScan Servers Asia Europe England OSCE ✓ EN-OfficeScan_01 OSCE ✓ EN-OfficeScan_02 OSCE ✓ EN-OfficeScan_03 France OSCE ✓ FR-OfficeScan_01 Germany OSCE ✓ DE-OfficeScan_01 North America South America Search Result Alex has access to all managed products under the 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	Parent_TMCM Local Folder OfficeScan Servers Europe England OSCE ✓ EN-OfficeScan_01 OSCE ✓ EN-OfficeScan_02 OSCE ✓ EN-OfficeScan_03 France OSCE ✓ FR-OfficeScan_01 Germany OSCE ✓ DE-OfficeScan_01 Search Result 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
 Parent_TMCM Local Folder OfficeScan Servers Europe England OSCE EN-OfficeScan_01 OSCE EN-OfficeScan_02 OSCE EN-OfficeScan_03 Search Result 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.	 Parent_TMCM Cascading Folder Local Folder New Entity OfficeScan Servers Asia China India Japan Europe England France Germany North America Canada Mexico USA South America Brazil Columbia Peru Search Result Erin can view the entire Product Directory or Product Directory structure on any of the applicable screens.

Dashboard and Summary Screens

All users can access the Dashboard 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.

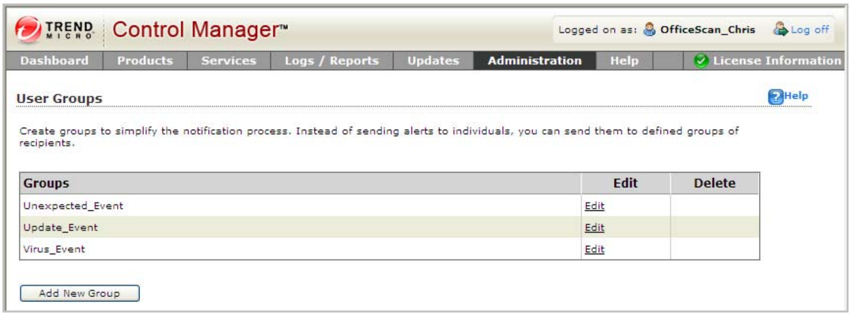
Configuring User Groups

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. Navigate to the User Groups screen: **Administration > Account Management > User Groups**

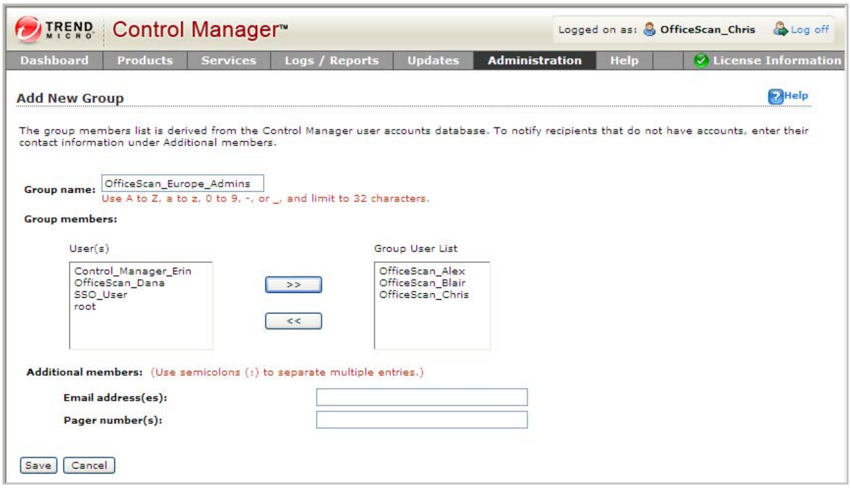


User Groups

Create groups to simplify the notification process. Instead of sending alerts to individuals, you can send them to defined groups of recipients.

Groups	Edit	Delete
Unexpected_Event	Edit	
Update_Event	Edit	
Virus_Event	Edit	

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



Add New Group

The group members list is derived from the Control Manager user accounts database. To notify recipients that do not have accounts, enter their contact information under Additional members.

Group name: OfficeScan_Europe_Admins
Use A to Z, a to z, 0 to 9, -, or _, and limit to 32 characters.

Group members:

User(s): Control_Manager_Erin, OfficeScan_Dana, SSO_User, root

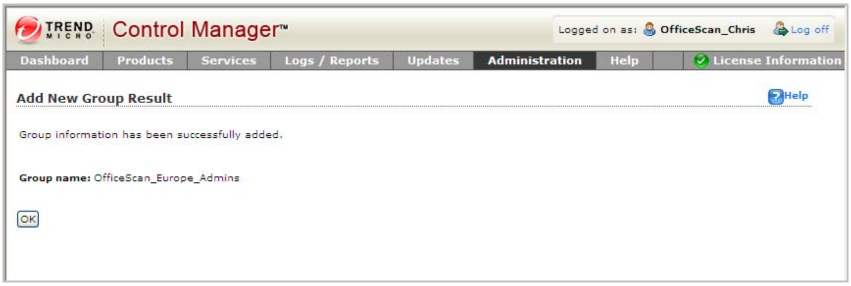
Group User List: OfficeScan_Alex, OfficeScan_Blair, OfficeScan_Chris

Additional members: (Use semicolons (;) to separate multiple entries.)

Email address(es):

Pager number(s):

4. Type the following in the **Group name** field:
   OfficeScan_Europe_Admins
5. Under Group Members, add the following users to the group list:
   - **OfficeScan_Alex**
   - **OfficeScan_Blair**
   - **OfficeScan_Chris**
6. Click **Save**. The Add New Users Result screen appears with the details of the new group.

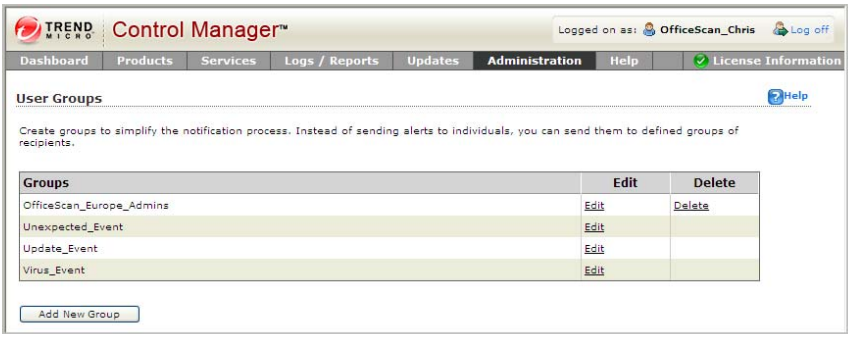


Add New Group Result

Group information has been successfully added.

Group name: OfficeScan_Europe_Admins

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



User Groups

Create groups to simplify the notification process. Instead of sending alerts to individuals, you can send them to defined groups of recipients.

Groups	Edit	Delete
OfficeScan_Europe_Admins	Edit	Delete
Unexpected_Event	Edit	
Update_Event	Edit	
Virus_Event	Edit	

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.

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

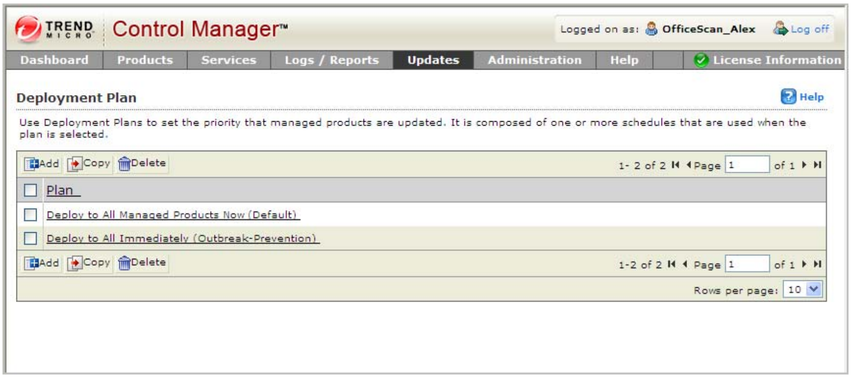
To manually download components:

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

Step 1: Configure a Deployment Plan for your components

Path: Updates > Deployment Plan

1. Navigate to the Deployment Plan screen.

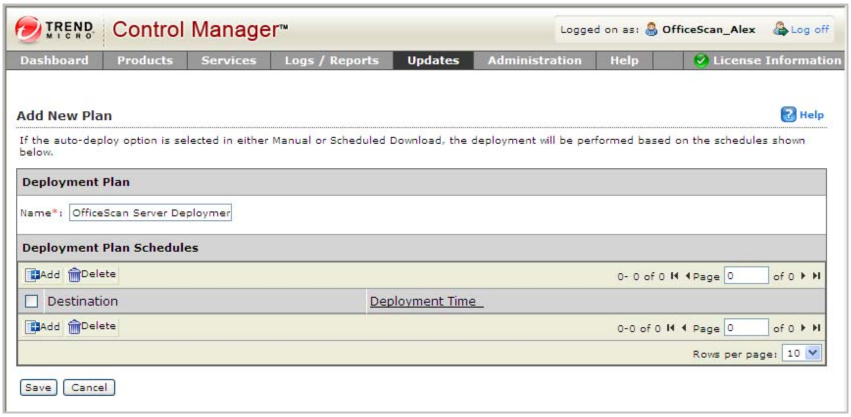


Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

□	Plan
□	Deploy to All Managed Products Now (Default)
□	Deploy to All Immediately (Outbreak-Prevention)

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



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

Name*: OfficeScan Server Deploymer

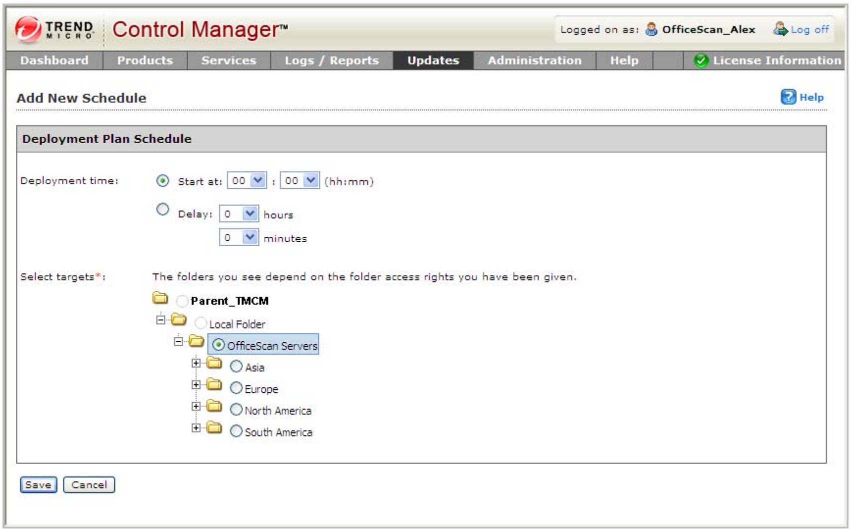
Deployment Plan Schedules

□	Destination	Deployment Time

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

   OfficeScan Server Deployment Plan

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



Add New Schedule

Deployment Plan Schedule

Deployment time: ● Start at: 00 : 00 (hh:mm)

○ Delay: 0 hours

0 minutes

Select targets*: The folders you see depend on the folder access rights you have been given.

- ○ Parent_TMCM
  - ○ Local Folder
    - ● OfficeScan Servers
      - ○ Asia
      - ○ Europe
      - ○ North America
      - ○ South America

Deployment time has the following options:

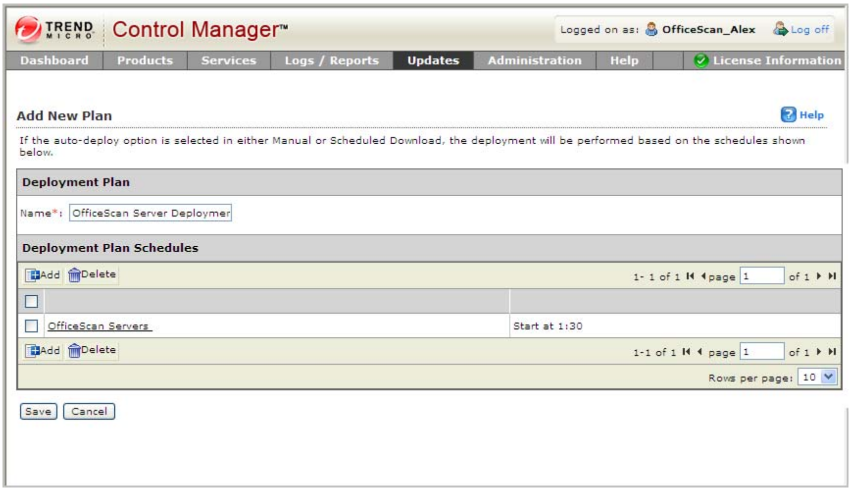
- **Start at:** Performs the deployment at a specific time
- **Delay:** after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

5. Specify the following for Deployment time:
   - Start at: **01:30**

6. 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.

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



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

Name*: OfficeScan Server Deploymer

Deployment Plan Schedules

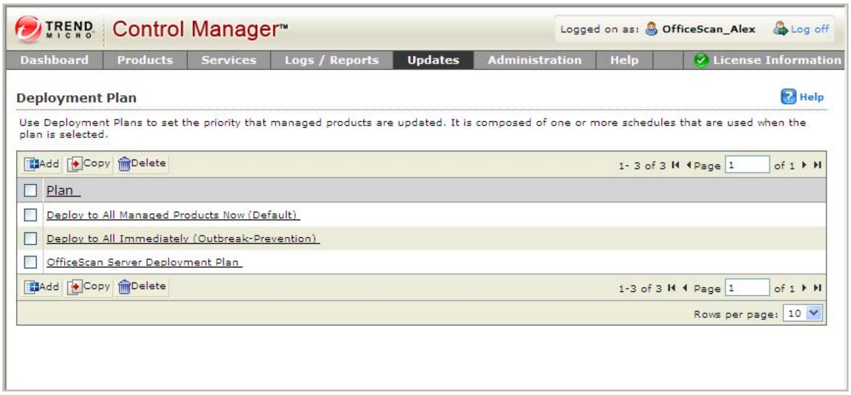
1- 1 of 1 page 1 of 1

□		
□	OfficeScan Servers	Start at 1:30

1-1 of 1 page 1 of 1

Rows per page: 10

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



Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

1- 3 of 3 Page 1 of 1

□	Plan
□	Deploy to All Managed Products Now (Default)
□	Deploy to All Immediately (Outbreak-Prevention)
□	OfficeScan Server Deployment Plan

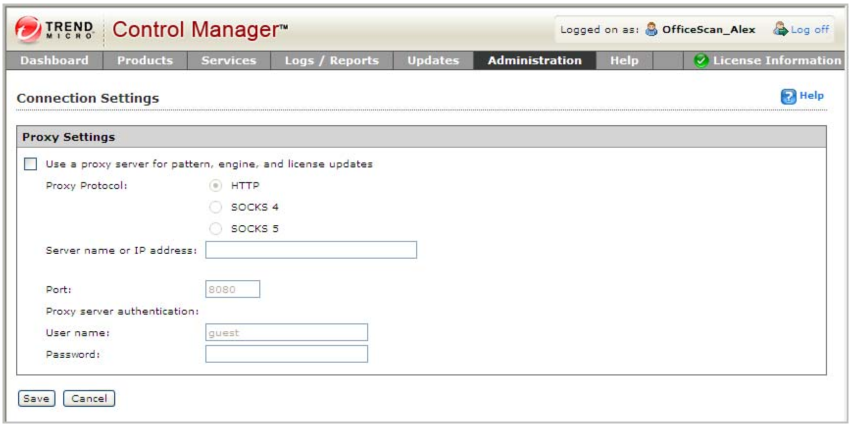
1-3 of 3 Page 1 of 1

Rows per page: 10

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

Path: Administration > Settings > Proxy Settings

1. Navigate to the Connection Settings screen.



Connection Settings

Proxy Settings

□ Use a proxy server for pattern, engine, and license updates

Proxy Protocol: ● HTTP ○ SOCKS 4 ○ SOCKS 5

Server name or IP address:

Port: 8080

Proxy server authentication:

User name: guest

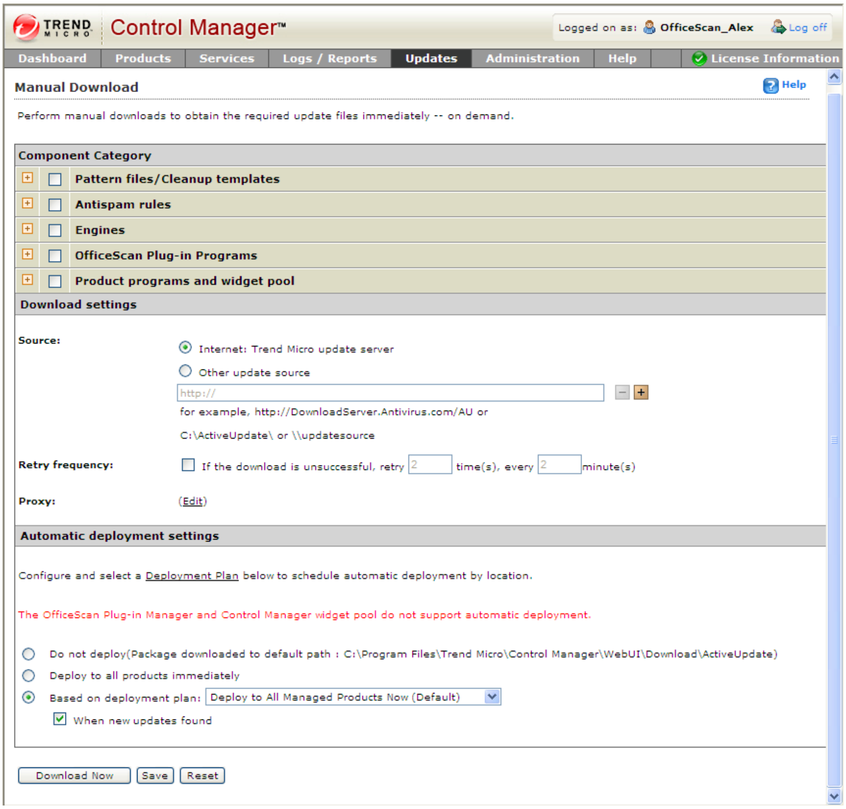
Password:

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

Step 3: Select the components to update

Path: Updates > Manual Download

1. Navigate to the Manual Download screen.



Manual Download

Perform manual downloads to obtain the required update files immediately -- on demand.

Component Category

- ⊞ □ **Pattern files/Cleanup templates**
- ⊞ □ **Antispam rules**
- ⊞ □ **Engines**
- ⊞ □ **OfficeScan Plug-in Programs**
- ⊞ □ **Product programs and widget pool**

Download settings

Source: ● Internet: Trend Micro update server
○ Other update source
http://
for example, http://DownloadServer.Antivirus.com/AU or
C:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

The OfficeScan Plug-in Manager and Control Manager widget pool do not support automatic deployment.

○ Do not deploy(Package downloaded to default path : C:\Program Files\Trend Micro\Control Manager\WebUI\Download\ActiveUpdate)
○ Deploy to all products immediately
● Based on deployment plan: Deploy to All Managed Products Now (Default)
☑ When new updates found

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

3. Alex is only interested in downloading OfficeScan components, so verify the following are selected from the Pattern files/Cleanup templates list:

TABLE 3-7. OfficeScan Pattern files/Cleanup templates

- Virus Pattern File
- Virus Cleanup Template
- Common Firewall Pattern
- Spyware Active-monitoring Pattern
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
- Spyware Pattern V6
- Smart Scan Agent Pattern
- Digital Signature Pattern
- Behavior Monitoring Configuration Pattern
- Policy Enforcement Pattern
- Policy Enforcement Pattern Description
- Behavior Monitoring Detection Pattern

4. Click the + icon to expand the Engines list.

5. Alex is only interested in downloading OfficeScan components, so verify that the following are selected from the Engines list:

TABLE 3-8. OfficeScan Scan Engines

- NTKD
- Common Firewall Driver (64-bit) V5
- Scan Engine for Windows on x64 architecture
- Virus Cleanup Engine (Digitally signed, 32-bit)
- Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)
- Spyware Scan Engine (32-bit) V6
- Spyware Scan Engine (64-bit) V6
- Behavior Monitoring Driver
- Behavior Monitor Core Service
- Common Firewall Driver (32-bit) V5

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:

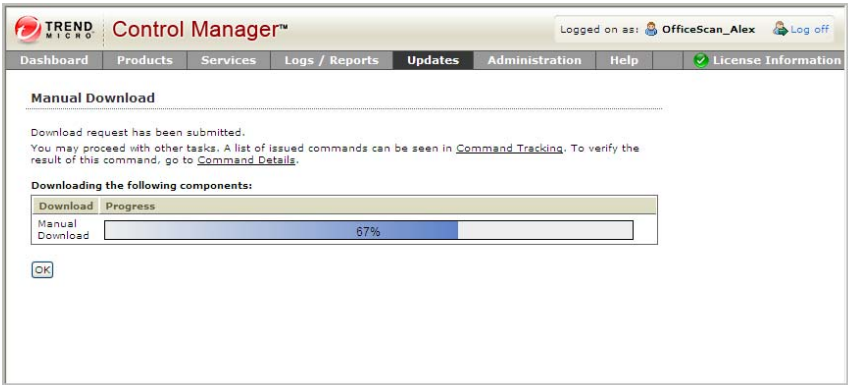
- Deploying to the managed products individually
- Testing the updated components before deployment

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.



Manual Download

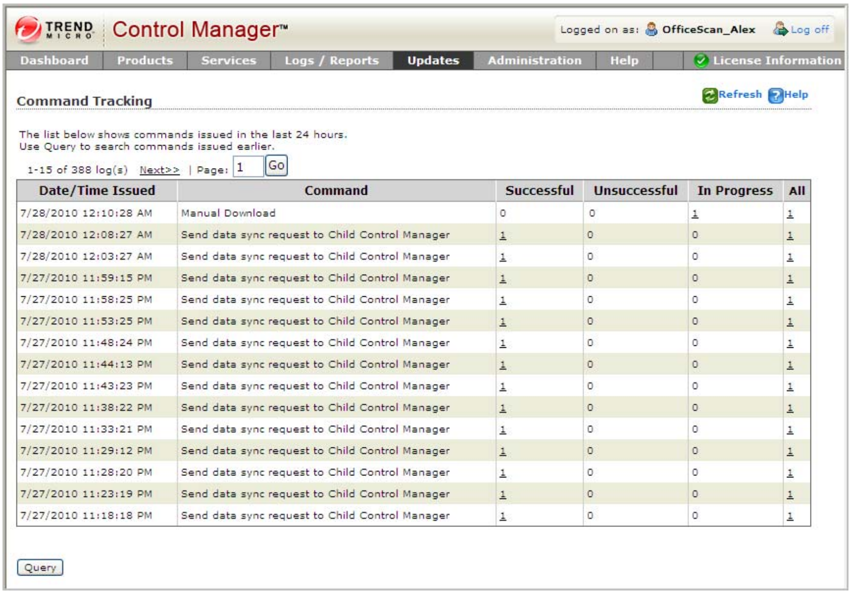
Download request has been submitted.

You may proceed with other tasks. A list of issued commands can be seen in Command Tracking. To verify the result of this command, go to Command Details.

Downloading the following components:

Download	Progress
Manual Download	67%

2. Click the **Command Tracking** to view details of the download.



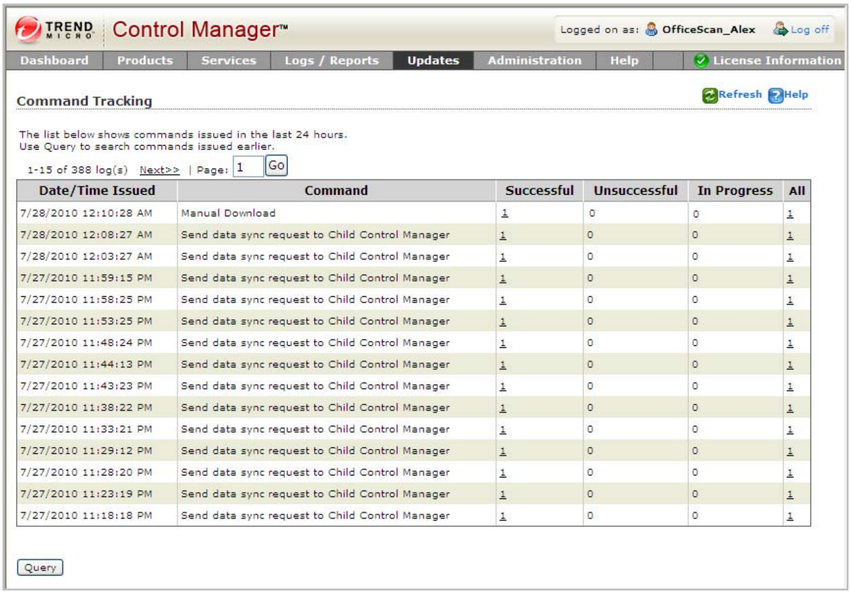
Command Tracking

The list below shows commands issued in the last 24 hours.
Use Query to search commands issued earlier.

1-15 of 388 log(s) Next>> | Page: 1 Go

Date/Time Issued	Command	Successful	Unsuccessful	In Progress	All
7/28/2010 12:10:28 AM	Manual Download	0	0	1	1
7/28/2010 12:08:27 AM	Send data sync request to Child Control Manager	1	0	0	1
7/28/2010 12:03:27 AM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:59:15 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:58:25 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:53:25 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:48:24 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:44:13 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:43:23 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:38:22 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:33:21 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:29:12 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:28:20 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:23:19 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:18:18 PM	Send data sync request to Child Control Manager	1	0	0	1

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



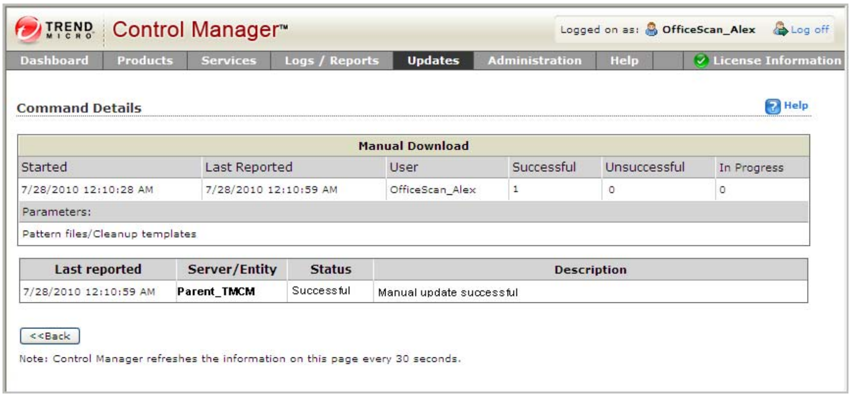
Command Tracking

The list below shows commands issued in the last 24 hours.
Use Query to search commands issued earlier.

1-15 of 388 log(s) Next>> | Page: 1

Date/Time Issued	Command	Successful	Unsuccessful	In Progress	All
7/28/2010 12:10:28 AM	Manual Download	1	0	0	1
7/28/2010 12:08:27 AM	Send data sync request to Child Control Manager	1	0	0	1
7/28/2010 12:03:27 AM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:59:15 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:58:25 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:53:25 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:48:24 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:44:13 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:43:23 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:38:22 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:33:21 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:29:12 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:28:20 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:23:19 PM	Send data sync request to Child Control Manager	1	0	0	1
7/27/2010 11:18:18 PM	Send data sync request to Child Control Manager	1	0	0	1

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



Command Details

Manual Download					
Started	Last Reported	User	Successful	Unsuccessful	In Progress
7/28/2010 12:10:28 AM	7/28/2010 12:10:59 AM	OfficeScan_Alex	1	0	0
Parameters:					
Pattern files/Cleanup templates					

Last reported	Server/Entity	Status	Description
7/28/2010 12:10:59 AM	Parent_TMCM	Successful	Manual update successful

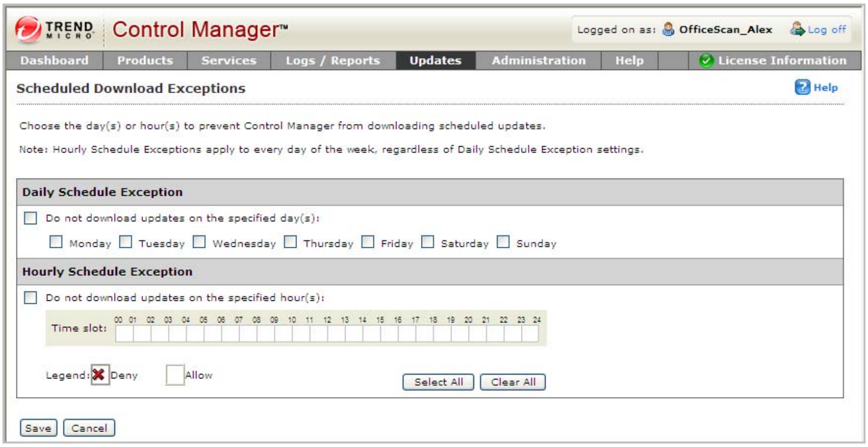
Note: Control Manager refreshes the information on this page every 30 seconds.

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.



Scheduled Download Exceptions

Choose the day(s) or hour(s) to prevent Control Manager from downloading scheduled updates.

Note: Hourly Schedule Exceptions apply to every day of the week, regardless of Daily Schedule Exception settings.

Daily Schedule Exception

☐ Do not download updates on the specified day(s):

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Hourly Schedule Exception

☐ Do not download updates on the specified hour(s):

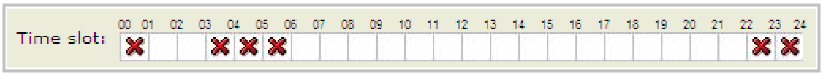
Time slot: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Legend: ☒ Deny ☐ Allow

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

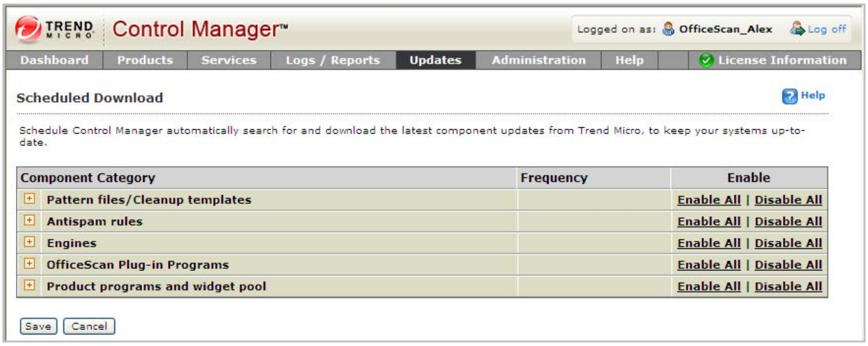
Step 7: Enable the schedule and save settings

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.



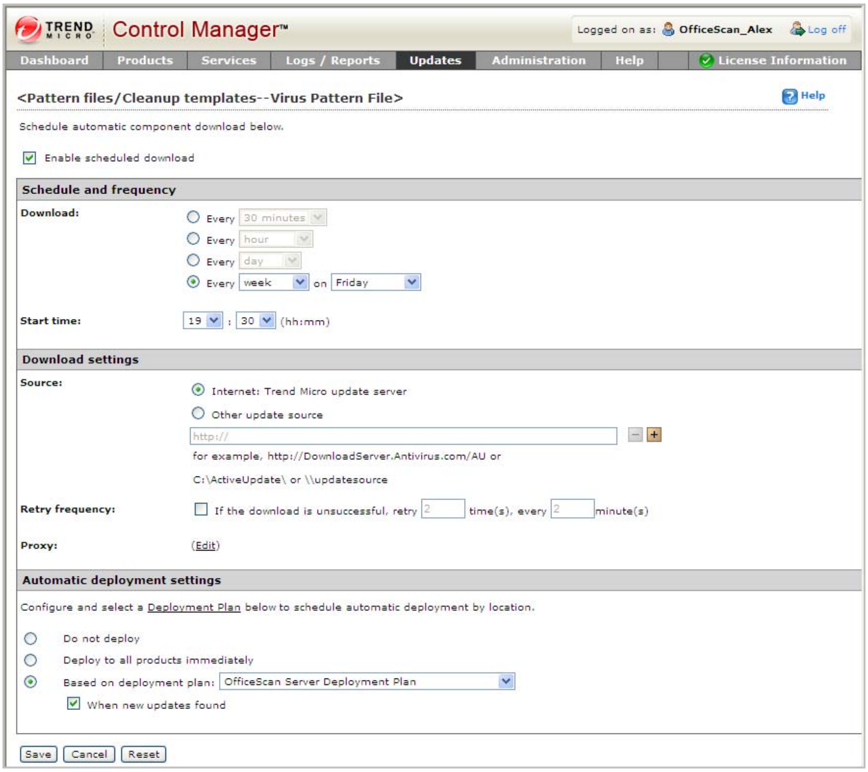
Scheduled Download

Schedule Control Manager automatically search for and download the latest component updates from Trend Micro, to keep your systems up-to-date.

Component Category	Frequency	Enable
⊞ Pattern files/Cleanup templates		Enable All | Disable All
⊞ Antispam rules		Enable All | Disable All
⊞ Engines		Enable All | Disable All
⊞ OfficeScan Plug-in Programs		Enable All | Disable All
⊞ Product programs and widget pool		Enable All | Disable All

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.



<Pattern files/Cleanup templates--Virus Pattern File>

Schedule automatic component download below.

☑ Enable scheduled download

Schedule and frequency

Download:

○ Every 30 minutes
○ Every hour
○ Every day
● Every week on Friday

Start time: 19 : 30 (hh:mm)

Download settings

Source:

● Internet: Trend Micro update server
○ Other update source

http://

for example, http://DownloadServer.Antivirus.com/AU or C:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

○ Do not deploy
○ Deploy to all products immediately
● Based on deployment plan: OfficeScan Server Deployment Plan
☑ When new updates found

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 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 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 Plan** 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 for the following:

Table 3-9. OfficeScan Pattern files/Cleanup templates

- Virus Cleanup Template
- Common Firewall Pattern
- Spyware Active-monitoring Pattern
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
- Spyware Pattern V6
- Smart Scan Agent Pattern
- Digital Signature Pattern
- Behavior Monitoring Configuration Pattern
- Policy Enforcement Pattern
- Policy Enforcement Pattern Description
- Behavior Monitoring Detection Pattern

Table 3-10. OfficeScan Scan Engines

- NTKD
- Common Firewall Driver (64-bit) V5
- Scan Engine for Windows on x64 architecture
- Virus Cleanup Engine (Digitally signed, 32-bit)
- Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)
- Spyware Scan Engine (32-bit) V6
- Spyware Scan Engine (64-bit) V6
- Behavior Monitoring Driver
- Behavior Monitor Core Service
- Common Firewall Driver (32-bit) V5

Chapter 4

Monitoring the Control Manager Network

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

This chapter covers the following topics:

Comparison of Monitoring Methods

Control Manager offers many options when monitoring your network. Use the following table to select the method that best fits your needs.

TABLE 4-1. Monitoring Options

SOURCE	DESCRIPTION
Dashboard	Provides at a glance information about what is happening on your network. **Pros**: • Provides information for a global view of your network • Information is easily displayed using widgets • Widgets can provide detailed information • Widgets can display data in different ways (graphs or tables) **Cons:** • Cannot monitor specific mission critical endpoints on your network • Cannot customize widgets to display only the data that you need
Logs	Provides detailed information on any security related event on your network **Pros**: • Information can be filtered so only the data you require displays. This can help you to monitor mission critical endpoints on your network • Query criteria can be saved and shared with other users **Cons:** • Requires some time to set up query criteria

TABLE 4-1. Monitoring Options

SOURCE	DESCRIPTION
Reports	Provides detailed information on any security related event on your network **Pros**: • Information can be filtered so only the data you require displays. This can help you to monitor mission critical endpoints on your network • Multiple ways to display data (bar, pie, or line charts or as dynamic or grid tables) • Reports can generate on a schedule or on demand **Cons:** • Requires some time to set up report templates

Understanding the Dashboard

The Control Manager dashboard provides at-a-glance information for the Control Manager network. The dashboard is comprised of two components:

- **Tabs:** Allow administrators to create a screen that contains one or more widgets
- **Widgets:** Provide specific information about various security-related events

Enabling Smart Feedback is required for Smart Protection Network widgets to function.

Configuring Smart Protection Network Settings

Enable Trend Micro Smart Feedback to share threat information with the Trend Micro Smart Protection Network. This provides better protection for your network because Trend Micro is able to quickly identify and address new threats.

Enabling Smart Protection Network Settings is also required for some widgets to function. This is because the widgets receive their data directly from Trend Micro Smart Protection Network.

Note: Email Reputation, File Reputation, and Web Reputation are all part of the Smart Protection Network.

To enable Smart Protection Network Settings Feedback:

Path: Administration > Settings > Smart Protection Network Settings

1. Navigate to the Smart Protection Network Settings screen.
2. Select **Enable Trend Micro Smart Feedback and Smart Protection Network widgets**.
3. Specify how often Control Manager will send completely anonymous threat information to the Smart Protection Network from the **Time interval** drop-down list.
4. Specify the industry that your company is in from the **Your industry** drop-down list.
5. Click **Save**.

Using the Dashboard

The dashboard can be customized for each user. Customizing the dashboard for one user does not affect the dashboard for other users.

Chris wants to create a tab for each OfficeScan server he administors. Each tab will have four widgets and the widgets will display only the data that relates to each specific OfficeScan server.

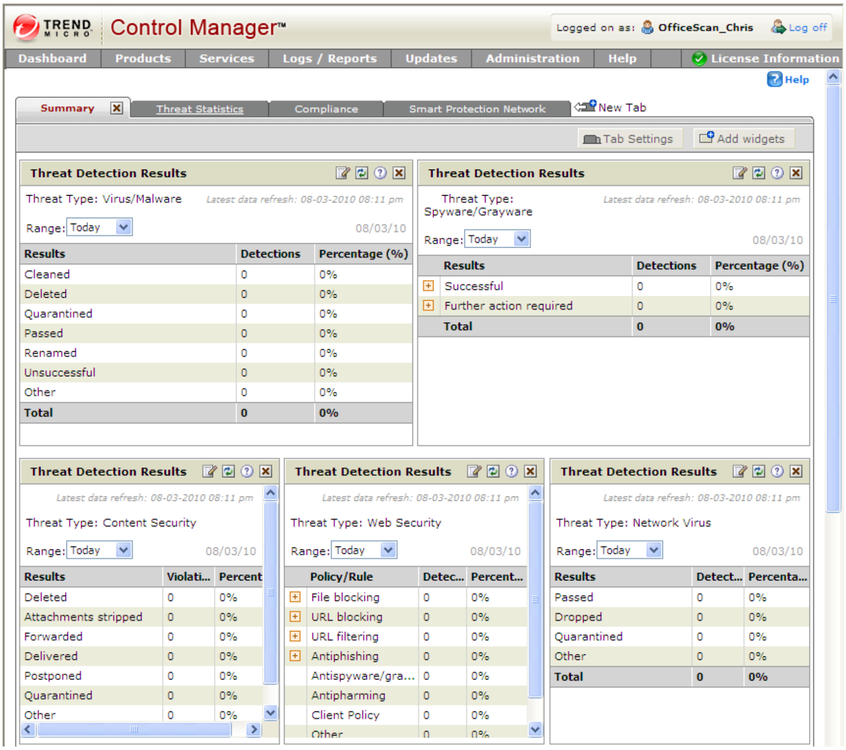
The widgets Chris wants to add to each tab are as follows.

TABLE 4-1. Widgets to add to the dashboard

WIDGET	DESCRIPTION
OfficeScan Endpoint Connection Status	Chris wants to know the connection status of the endpoints registered to each OfficeScan server.
Product Component Status	Chris wants to know which endpoints have out of date components.
Control Manager Top Threats	Chris wants to know which files have been an issue for endpoints.
Control Manager Top Threats	Chris wants to know which URLs have been an issue for endpoints.

To create a tab for each OfficeScan server:

1. Log on to the Control Manager server as **Chris**.



Threat Detection Results

Threat Type: Virus/Malware — *Latest data refresh: 08-03-2010 08:11 pm*

Range: Today — 08/03/10

Results	Detections	Percentage (%)
Cleaned	0	0%
Deleted	0	0%
Quarantined	0	0%
Passed	0	0%
Renamed	0	0%
Unsuccessful	0	0%
Other	0	0%
Total	**0**	**0%**

Threat Detection Results

Threat Type: Spyware/Grayware — *Latest data refresh: 08-03-2010 08:11 pm*

Range: Today — 08/03/10

Results	Detections	Percentage (%)
⊞ Successful	0	0%
⊞ Further action required	0	0%
Total	**0**	**0%**

Threat Detection Results

Latest data refresh: 08-03-2010 08:11 pm

Threat Type: Content Security

Range: Today — 08/03/10

Results	Violati...	Percent
Deleted	0	0%
Attachments stripped	0	0%
Forwarded	0	0%
Delivered	0	0%
Postponed	0	0%
Quarantined	0	0%
Other	0	0%

Threat Detection Results

Latest data refresh: 08-03-2010 08:11 pm

Threat Type: Web Security

Range: Today — 08/03/10

Policy/Rule	Detec...	Percent...
⊞ File blocking	0	0%
⊞ URL blocking	0	0%
⊞ URL filtering	0	0%
⊞ Antiphishing	0	0%
Antispyware/gra...	0	0%
Antipharming	0	0%
Client Policy	0	0%
Other	0	0%

Threat Detection Results

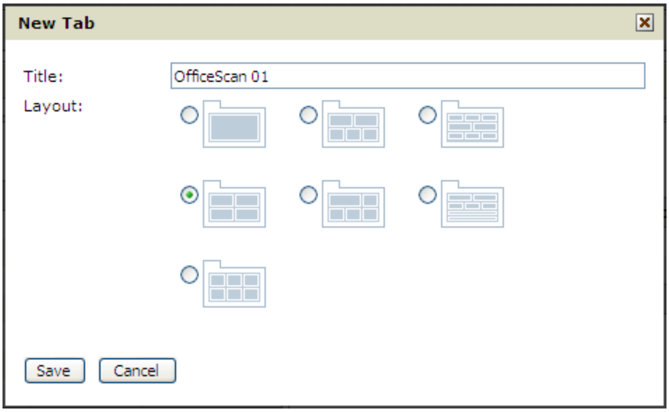
Latest data refresh: 08-03-2010 08:11 pm

Threat Type: Network Virus

Range: Today — 08/03/10

Results	Detect...	Percenta...
Passed	0	0%
Dropped	0	0%
Quarantined	0	0%
Other	0	0%
Total	**0**	**0%**

2. Click **New Tab**. The New Tab screen appears



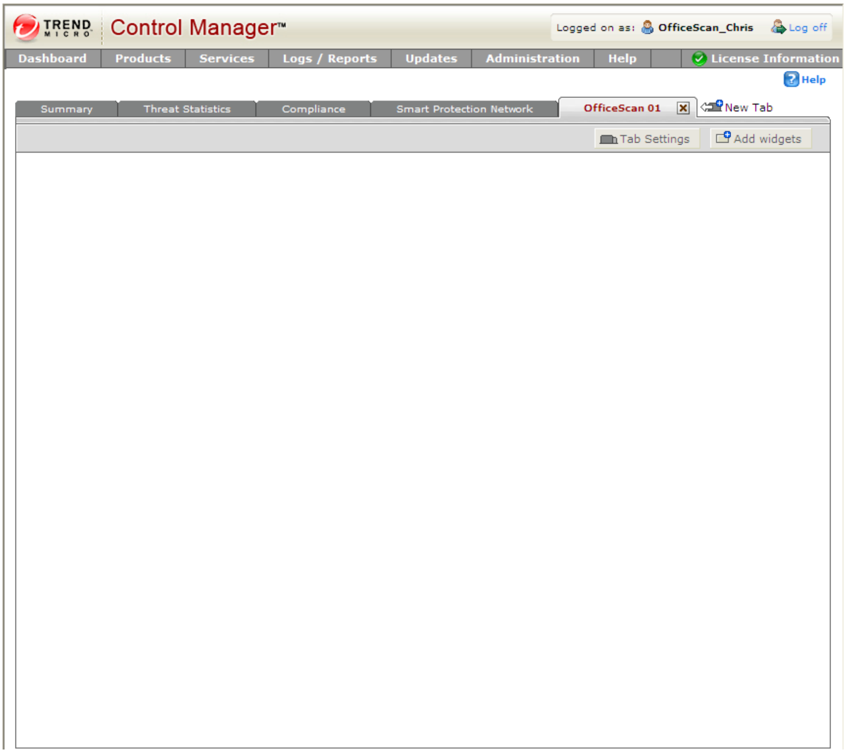
New Tab

Title: OfficeScan 01

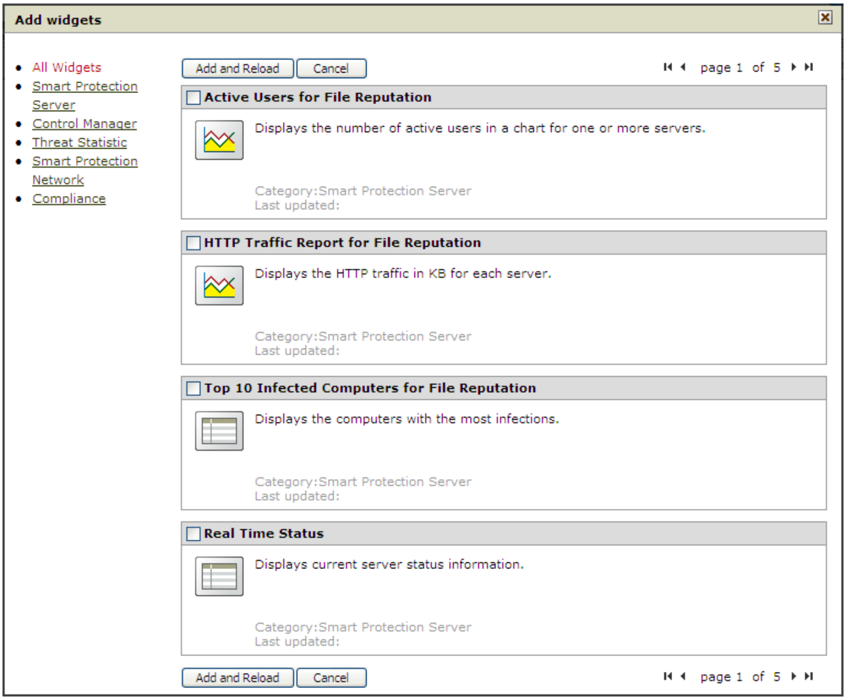
Layout:

3. Type **OfficeScan 01** for the tab title.
4. Select the 2x2 tab layout.

5. Click **Save**. The dashboard appears with the new tab.



6. Click **Add Widgets**. The Add widgets screen appears.



□ **Active Users for File Reputation**

Displays the number of active users in a chart for one or more servers.

Category:Smart Protection Server
Last updated:

□ **HTTP Traffic Report for File Reputation**

Displays the HTTP traffic in KB for each server.

Category:Smart Protection Server
Last updated:

□ **Top 10 Infected Computers for File Reputation**

Displays the computers with the most infections.

Category:Smart Protection Server
Last updated:

□ **Real Time Status**

Displays current server status information.

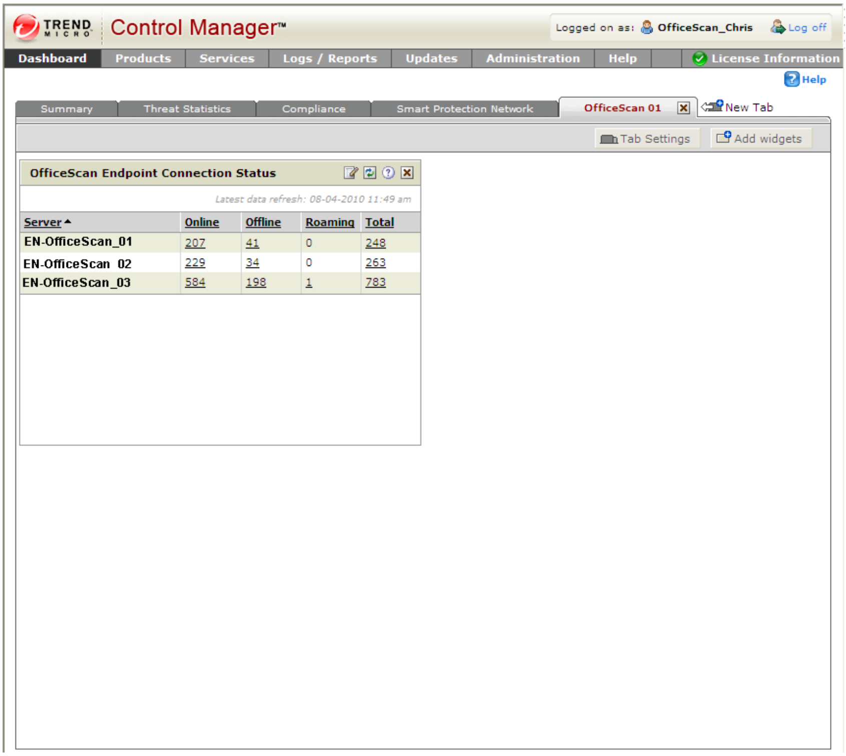
Category:Smart Protection Server
Last updated:

7. Click **Control Manager** to display only Control Manager widgets.

Tip: You can add multiple widgets to a tab by selecting the check box for each widget to add.

8. Select the **OfficeScan Endpoint Connection Status** widget.

9. Click **Add and Reload**. The widget appears in the dashboard.



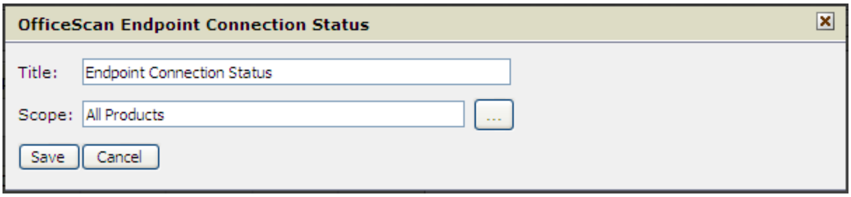
OfficeScan Endpoint Connection Status

Latest data refresh: 08-04-2010 11:49 am

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	207	41	0	248
EN-OfficeScan 02	229	34	0	263
EN-OfficeScan_03	584	198	1	783

Currently data for all three OfficeScan servers displays. Chris only wants the data for EN-OfficeScan_01 to display. Chris will need to "edit" the widget to modify the data that displays.

10. Click the **Edit** button on the widget. The edit screen for the widget appears.



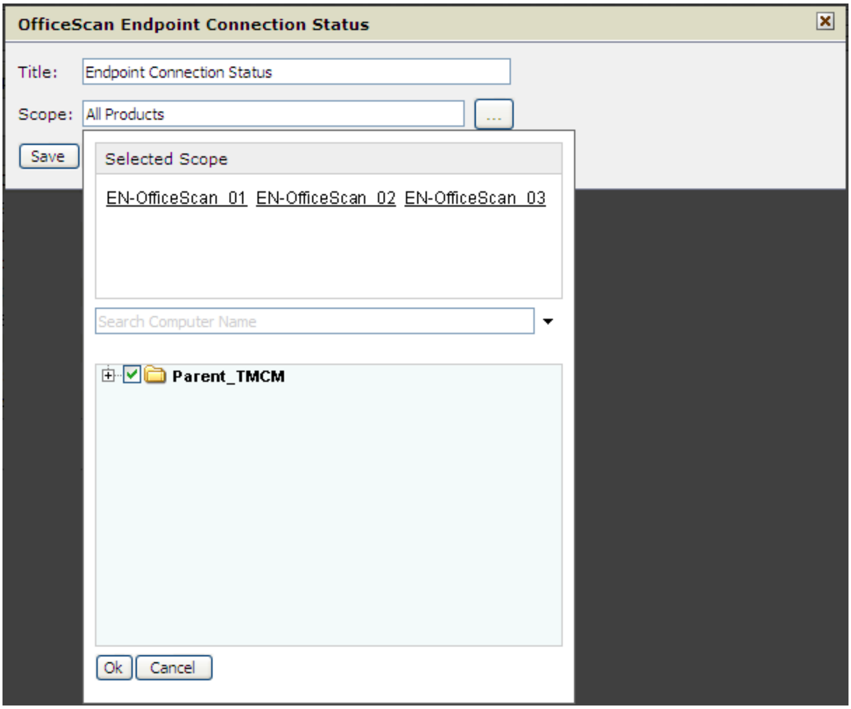
OfficeScan Endpoint Connection Status

Title: Endpoint Connection Status

Scope: All Products

11. Change the title of the widget to **Endpoint Connection Status**.

12. Click the **Browse** ... button. A Product Directory for the widget appears.



OfficeScan Endpoint Connection Status

Title: Endpoint Connection Status

Scope: All Products

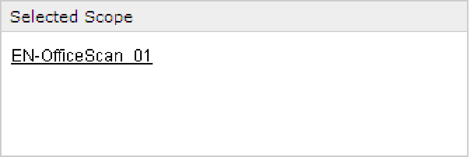
Selected Scope

EN-OfficeScan_01 EN-OfficeScan_02 EN-OfficeScan_03

☑ Parent_TMCM

13. Expand the Product Directory and clear the check boxes for **EN-OfficeScan_02** and **EN-OfficeScan_03**.

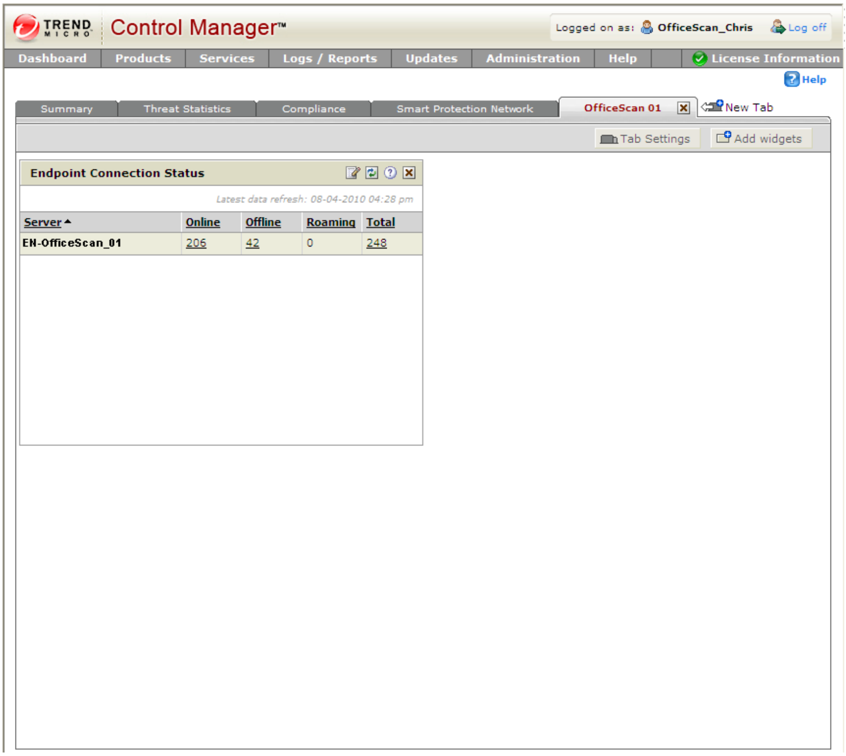
    EN-OfficeScan_01 is the only manage product that appears in the **Selected Scope** area.



Selected Scope

EN-OfficeScan_01

14. Click **Ok**. The dashboard appears with the modified widget in the OfficeScan 01 tab.

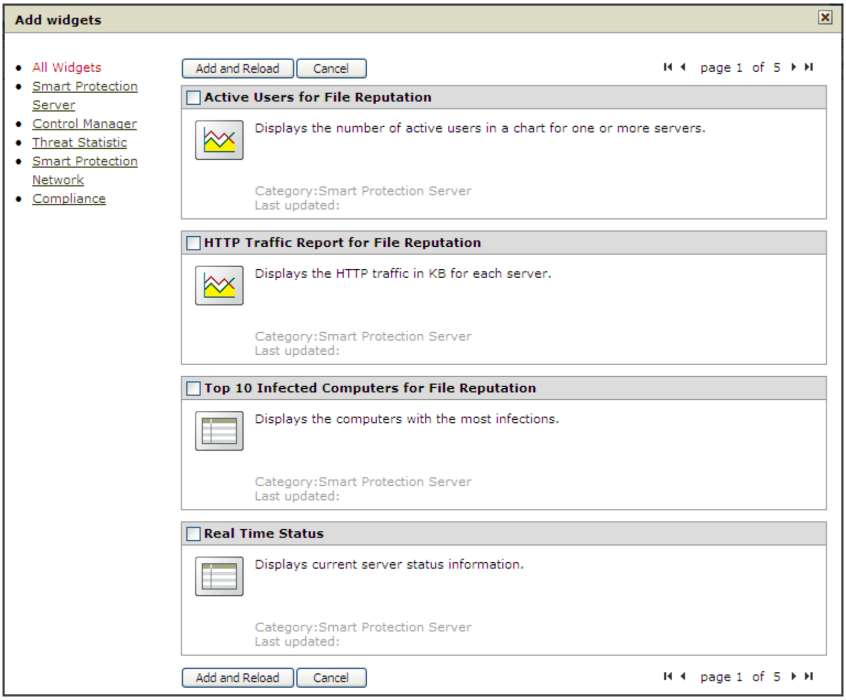


Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

15. Click **Add Widgets**. The Add widgets screen appears.



Add widgets

- All Widgets
- Smart Protection Server
- Control Manager
- Threat Statistic
- Smart Protection Network
- Compliance

□ **Active Users for File Reputation**

Displays the number of active users in a chart for one or more servers.

Category:Smart Protection Server
Last updated:

□ **HTTP Traffic Report for File Reputation**

Displays the HTTP traffic in KB for each server.

Category:Smart Protection Server
Last updated:

□ **Top 10 Infected Computers for File Reputation**

Displays the computers with the most infections.

Category:Smart Protection Server
Last updated:

□ **Real Time Status**

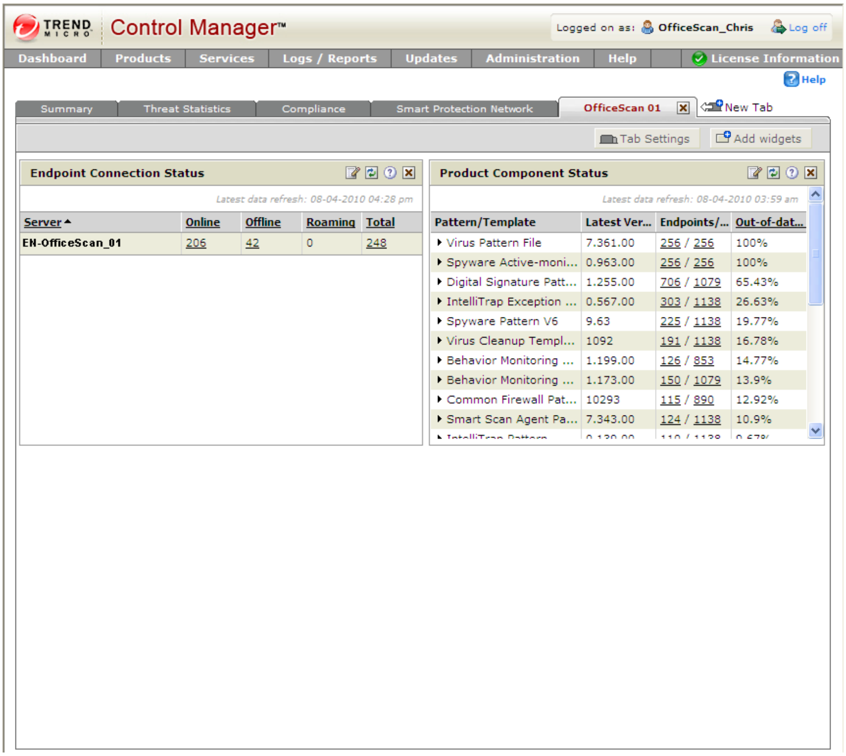
Displays current server status information.

Category:Smart Protection Server
Last updated:

16. Click **Control Manager** to display only Control Manager widgets.

17. Select the **Product Component Status** widget.

18. Click **Add and Reload**. The widget appears in the dashboard.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

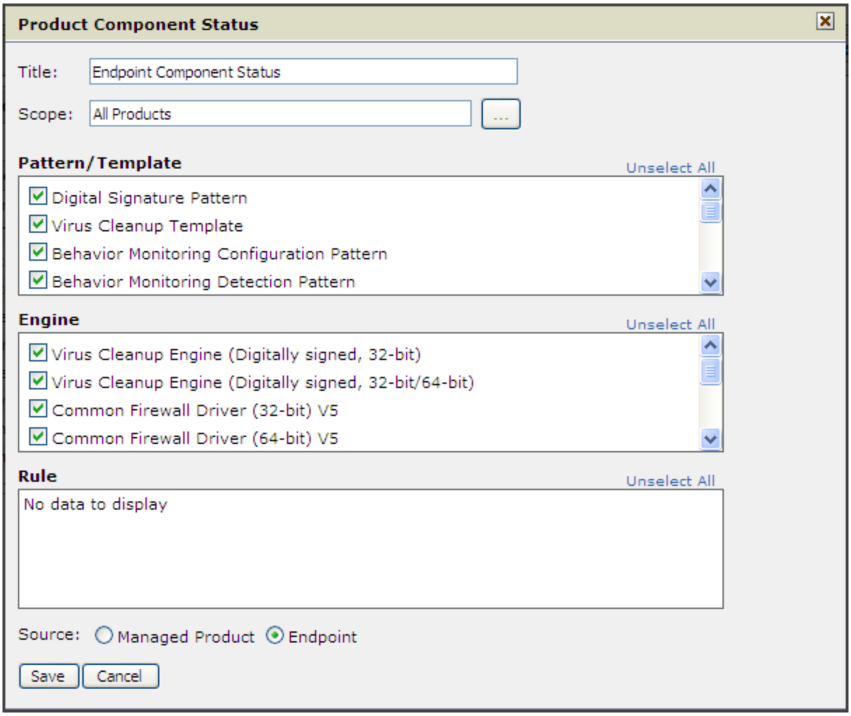
Product Component Status

Latest data refresh: 08-04-2010 03:59 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	256 / 256	100%
Spyware Active-moni...	0.963.00	256 / 256	100%
Digital Signature Patt...	1.255.00	706 / 1079	65.43%
IntelliTrap Exception ...	0.567.00	303 / 1138	26.63%
Spyware Pattern V6	9.63	225 / 1138	19.77%
Virus Cleanup Templ...	1092	191 / 1138	16.78%
Behavior Monitoring ...	1.199.00	126 / 853	14.77%
Behavior Monitoring ...	1.173.00	150 / 1079	13.9%
Common Firewall Pat...	10293	115 / 890	12.92%
Smart Scan Agent Pa...	7.343.00	124 / 1138	10.9%
IntelliTrap Pattern	0.130.00	110 / 1138	9.67%

The data the widget currently displays is for the OfficeScan servers, not for the endpoints registered to the OfficeScan servers. For this tab Chris wants only the data for endpoints registered to EN-OfficeScan_01.

19. Click the **Edit** button on the widget. The edit screen for the widget appears.



Product Component Status

Title: Endpoint Component Status

Scope: All Products

Pattern/Template

- ☑ Digital Signature Pattern
- ☑ Virus Cleanup Template
- ☑ Behavior Monitoring Configuration Pattern
- ☑ Behavior Monitoring Detection Pattern

Engine

- ☑ Virus Cleanup Engine (Digitally signed, 32-bit)
- ☑ Virus Cleanup Engine (Digitally signed, 32-bit/64-bit)
- ☑ Common Firewall Driver (32-bit) V5
- ☑ Common Firewall Driver (64-bit) V5

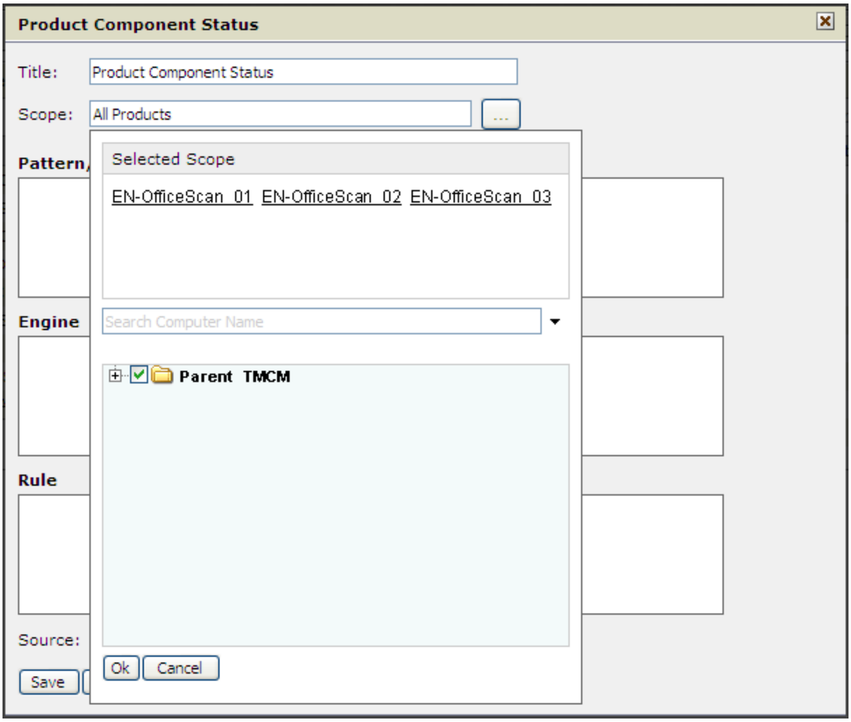
Rule

No data to display

Source: ○ Managed Product ● Endpoint

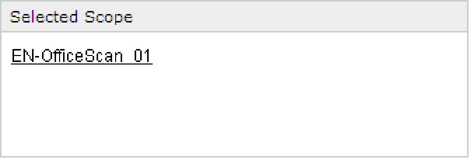
20. Change the title to **Endpoint Component Status**.

21. Click the **Browse** [...] button. A Product Directory for the widget appears.

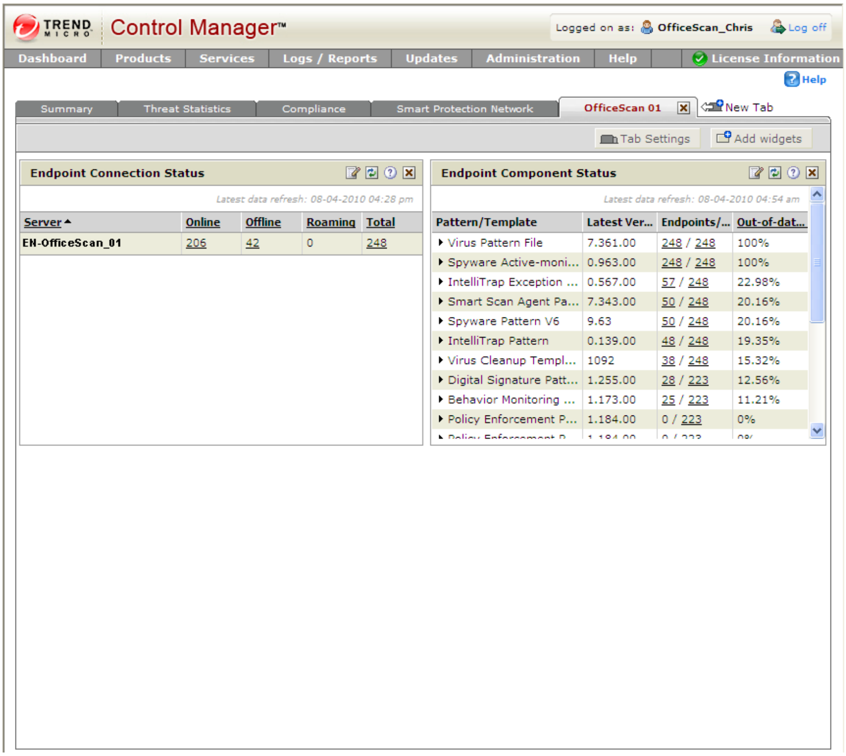


22. Expand the Product Directory and clear the check boxes for **EN-OfficeScan_02** and **EN-OfficeScan_03**.

    EN-OfficeScan_01 is the only manage product that appears in the **Selected Scope** area.



23. Click **Ok**.
24. Select **Endpoint** next to Source.
25. Click **Save**. The widget appears in the OfficeScan 01 tab, and only diplays endpoint component data from EN-OfficeScan_01.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

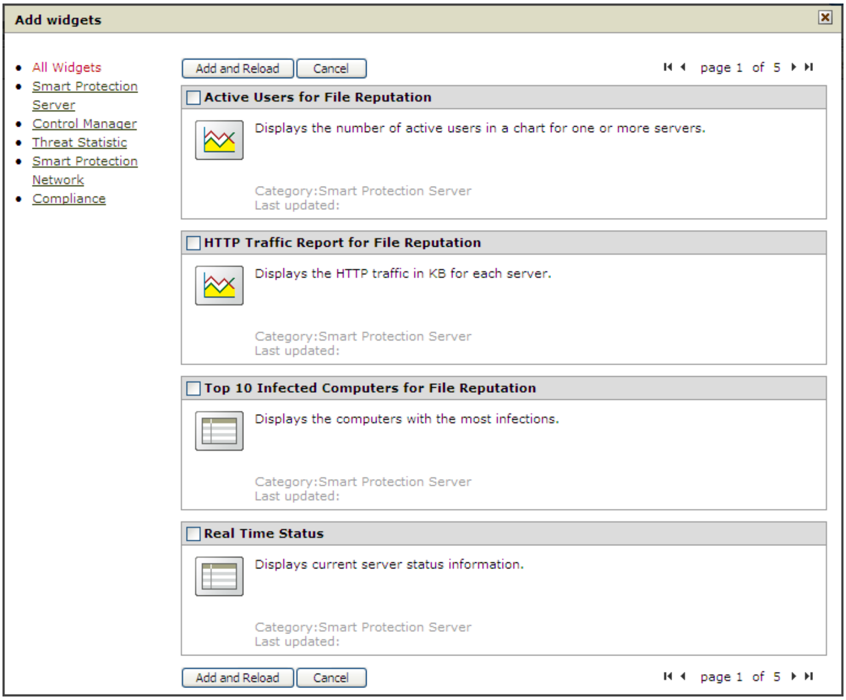
Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%
Policy Enforcement P...	1.184.00	0 / 223	0%

Chris now wants to add widgets that will let him know the top threats his endpoints are facing.

26. Click **Add Widgets**. The Add widgets screen appears.



Add widgets

- All Widgets
- Smart Protection Server
- Control Manager
- Threat Statistic
- Smart Protection Network
- Compliance

□ **Active Users for File Reputation**

Displays the number of active users in a chart for one or more servers.

Category:Smart Protection Server
Last updated:

□ **HTTP Traffic Report for File Reputation**

Displays the HTTP traffic in KB for each server.

Category:Smart Protection Server
Last updated:

□ **Top 10 Infected Computers for File Reputation**

Displays the computers with the most infections.

Category:Smart Protection Server
Last updated:

□ **Real Time Status**

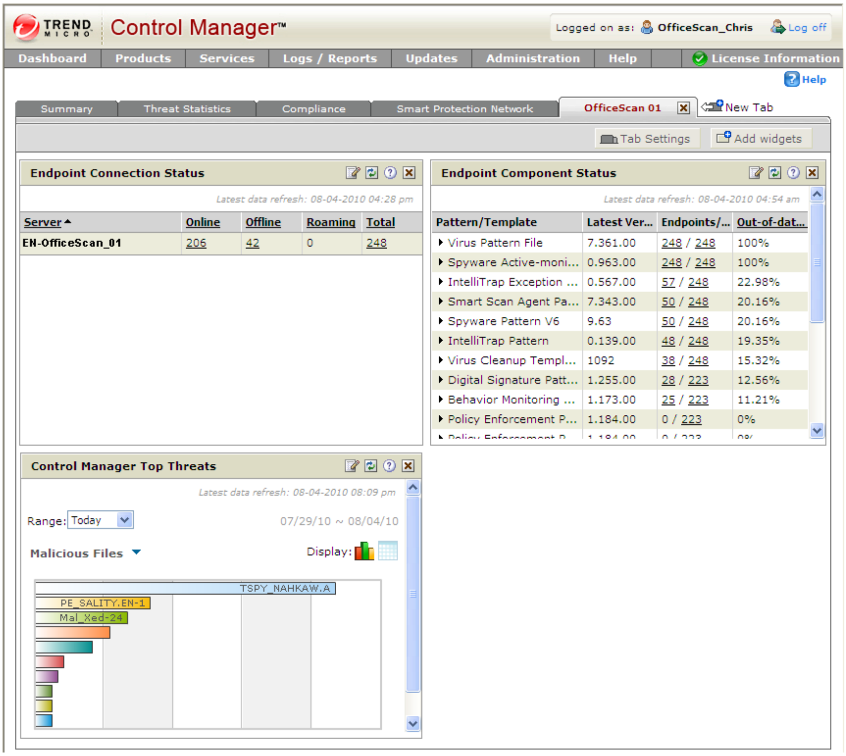
Displays current server status information.

Category:Smart Protection Server
Last updated:

27. Click **Control Manager** to display only Control Manager widgets.

28. Select the **Control Manager Top Threats** widget.

29. Click **Add and Reload**. The widget appears in the dashboard.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%
Policy Enforcement P...	1.184.00	0 / 223	0%

Control Manager Top Threats

Latest data refresh: 08-04-2010 08:09 pm

Range: Today

07/29/10 ~ 08/04/10

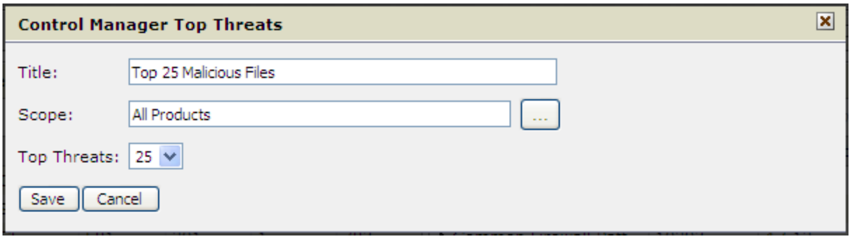
Malicious Files

Display:

Currently data for all three OfficeScan servers displays. Chris only wants the data for EN-OfficeScan_01 to display. Chris will need to "edit" the widget to modify the data that displays.

The **Control Manager Top Threats** widget displays 10 entires by default, but can display upto 50 entries. Chris wants to display more than 10 entries.

30. Click the **Edit** button on the widget. The edit screen for the widget appears.



Control Manager Top Threats

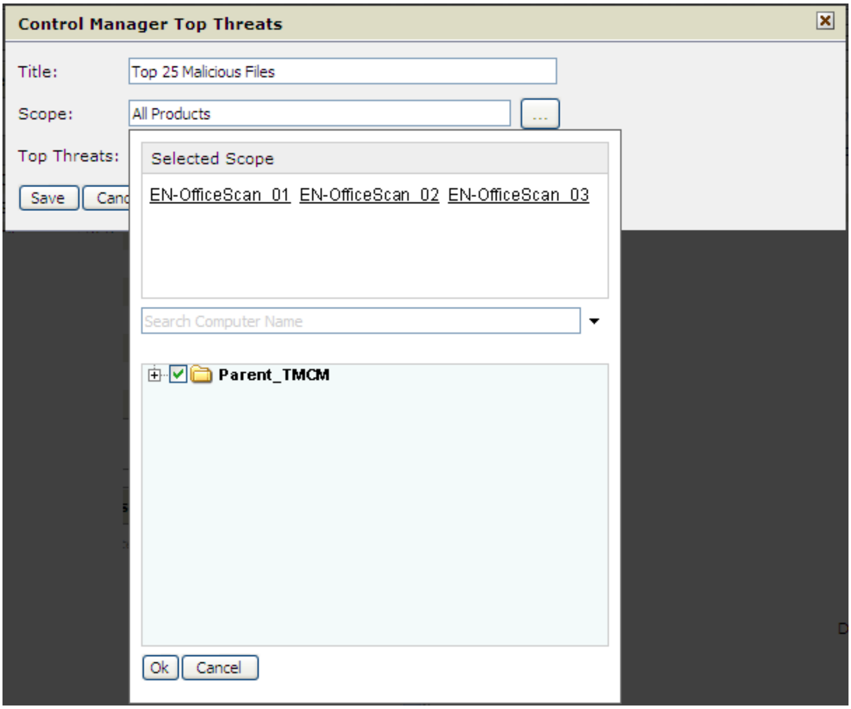
Title: Top 25 Malicious Files

Scope: All Products ...

Top Threats: 25

31. Change the title of the widget to **Top 25 Malicious Files**.

32. Click the **Browse** ... button. A Product Directory for the widget appears.



Control Manager Top Threats

Title: Top 25 Malicious Files

Scope: All Products ...

Top Threats:

Selected Scope

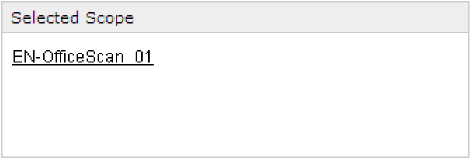
EN-OfficeScan_01 EN-OfficeScan_02 EN-OfficeScan_03

Search Computer Name

☑ **Parent_TMCM**

33. Expand the Product Directory and clear the check boxes for **EN-OfficeScan_02** and **EN-OfficeScan_03**.

    EN-OfficeScan_01 is the only manage product that appears in the **Selected Scope** area.

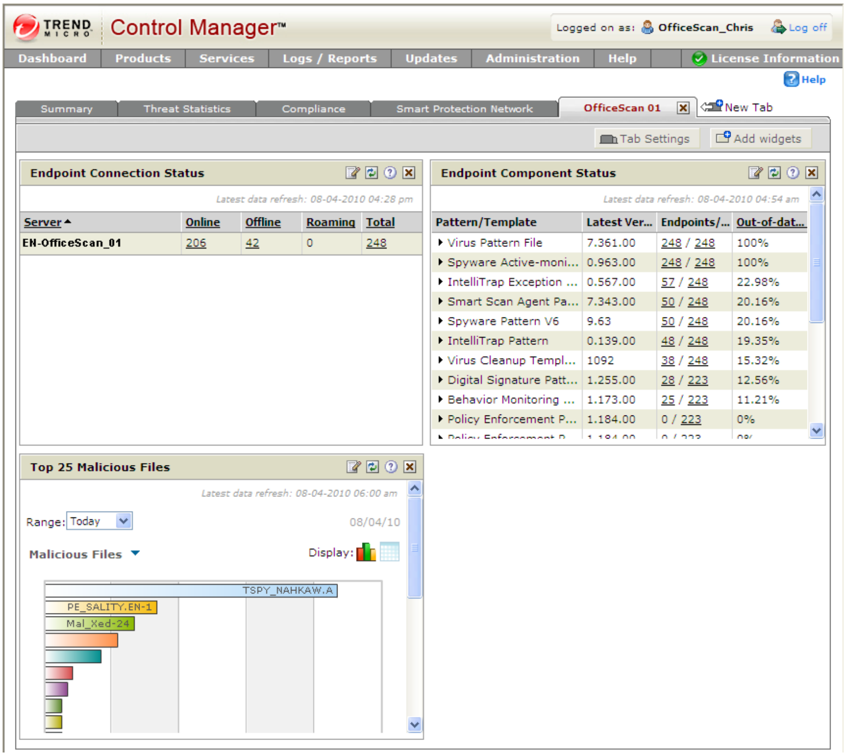


Selected Scope

EN-OfficeScan_01

34. Click **Ok**.
35. Select **25** from the **Top Threats** list.

36. Click **Save**. The dashboard appears with the modified widget in the OfficeScan 01 tab.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%
Policy Enforcement P...	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:00 am

Range: Today

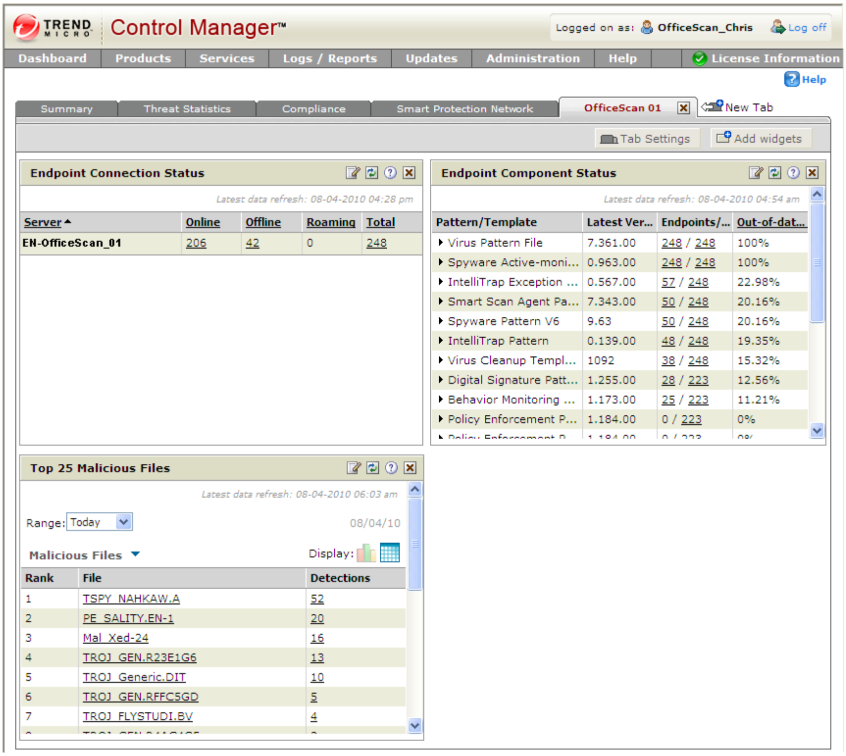
08/04/10

Malicious Files

Display:

While a bar chart is visually appealing, Chris wants the widget to display the data in a table.

37. Click the **Graph** icon in the widget. The widget reloads and displays the data in a table.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
▸ Virus Pattern File	7.361.00	248 / 248	100%
▸ Spyware Active-moni...	0.963.00	248 / 248	100%
▸ IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
▸ Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
▸ Spyware Pattern V6	9.63	50 / 248	20.16%
▸ IntelliTrap Pattern	0.139.00	48 / 248	19.35%
▸ Virus Cleanup Templ...	1092	38 / 248	15.32%
▸ Digital Signature Patt...	1.255.00	28 / 223	12.56%
▸ Behavior Monitoring ...	1.173.00	25 / 223	11.21%
▸ Policy Enforcement P...	1.184.00	0 / 223	0%
▸ Policy Enforcement P...	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:03 am

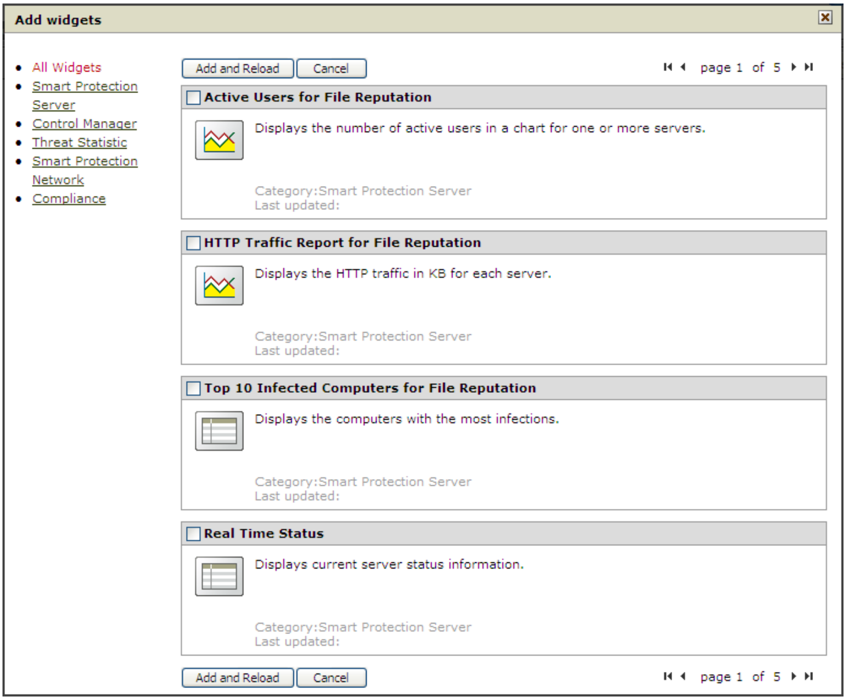
Range: Today 08/04/10

Malicious Files ▾ Display:

Rank	File	Detections
1	TSPY_NAHKAW.A	52
2	PE_SALITY.EN-1	20
3	Mal_Xed-24	16
4	TROJ_GEN.R23E1G6	13
5	TROJ_Generic.DIT	10
6	TROJ_GEN.RFFC5GD	5
7	TROJ_FLYSTUDI.BV	4

Chris also wants a widget that displays the top URLs that are dangerous to his endpoints.

38. Click **Add Widgets**. The Add widgets screen appears.



Add widgets

- All Widgets
- Smart Protection Server
- Control Manager
- Threat Statistic
- Smart Protection Network
- Compliance

☐ **Active Users for File Reputation**

Displays the number of active users in a chart for one or more servers.

Category:Smart Protection Server
Last updated:

☐ **HTTP Traffic Report for File Reputation**

Displays the HTTP traffic in KB for each server.

Category:Smart Protection Server
Last updated:

☐ **Top 10 Infected Computers for File Reputation**

Displays the computers with the most infections.

Category:Smart Protection Server
Last updated:

☐ **Real Time Status**

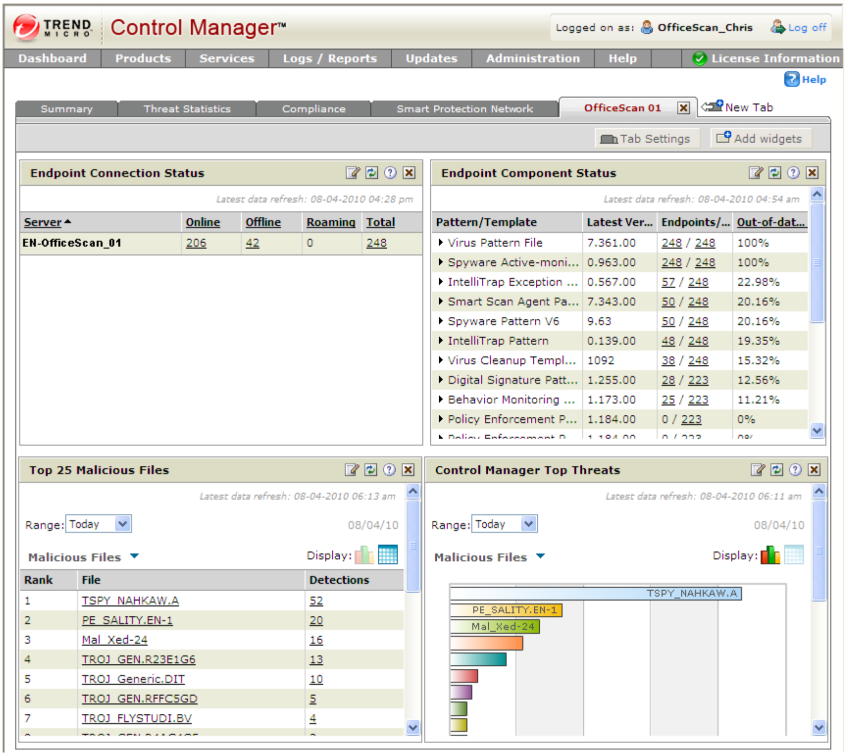
Displays current server status information.

Category:Smart Protection Server
Last updated:

39. Click **Control Manager** to display only Control Manager widgets.

40. Select the **Control Manager Top Threats** widget.

41. Click **Add and Reload**. The widget appears in the dashboard.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:13 am

Range: Today 08/04/10

Malicious Files Display:

Rank	File	Detections
1	TSPY_NAHKAW.A	52
2	PE_SALITY.EN-1	20
3	Mal_Xed-24	16
4	TROJ_GEN.R23E1G6	13
5	TROJ_Generic.DIT	10
6	TROJ_GEN.RFFC5GD	5
7	TROJ_FLYSTUDI.BV	4

Control Manager Top Threats

Latest data refresh: 08-04-2010 06:11 am

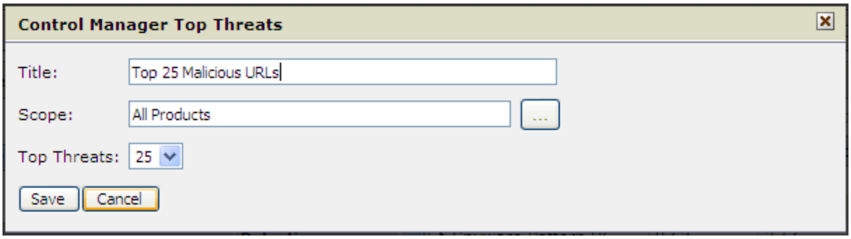
Range: Today 08/04/10

Malicious Files Display:

Currently data for all three OfficeScan servers displays. Chris only wants the data for EN-OfficeScan_01 to display. Chris will need to "edit" the widget to modify the data that displays.

The **Control Manager Top Threats** widget displays 10 entires by default, but can display upto 50 entries. Chris wants to display more than 10 entries.

42. Click the **Edit** button on the widget. The edit screen for the widget appears.



Control Manager Top Threats

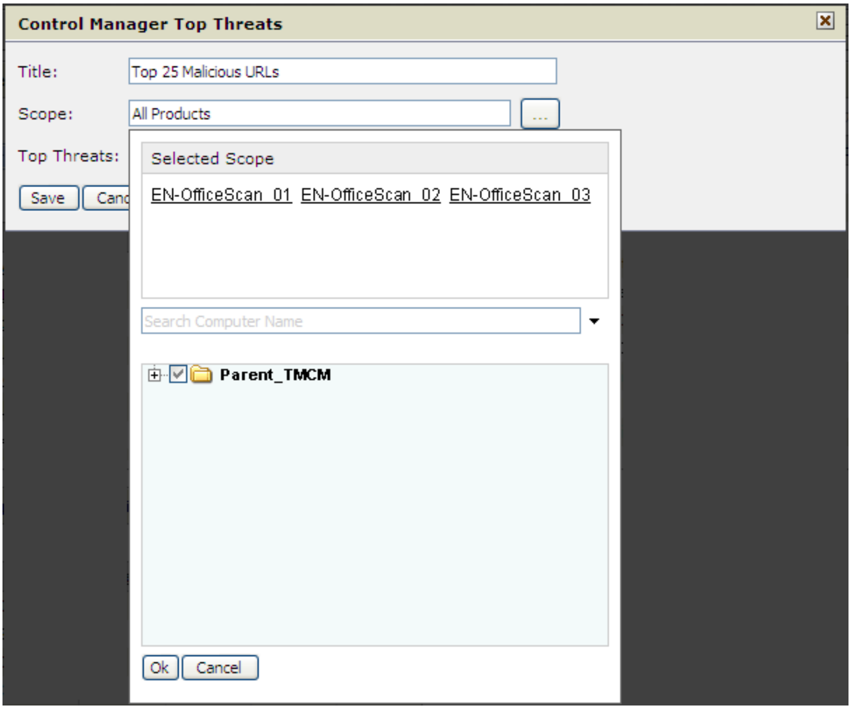
Title: Top 25 Malicious URLs

Scope: All Products

Top Threats: 25

43. Change the title of the widget to **Top 25 Malicious URLs**.

44. Click the **Browse** button. A Product Directory for the widget appears.



Control Manager Top Threats

Title: Top 25 Malicious URLs

Scope: All Products

Top Threats:

Selected Scope

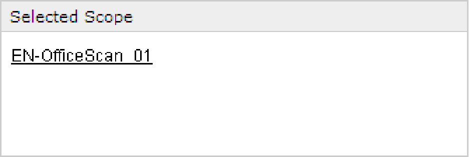
EN-OfficeScan_01 EN-OfficeScan_02 EN-OfficeScan_03

Search Computer Name

☑ Parent_TMCM

45. Expand the Product Directory and clear the check boxes for **EN-OfficeScan_02** and **EN-OfficeScan_03**.

    EN-OfficeScan_01 is the only manage product that appears in the **Selected Scope** area.

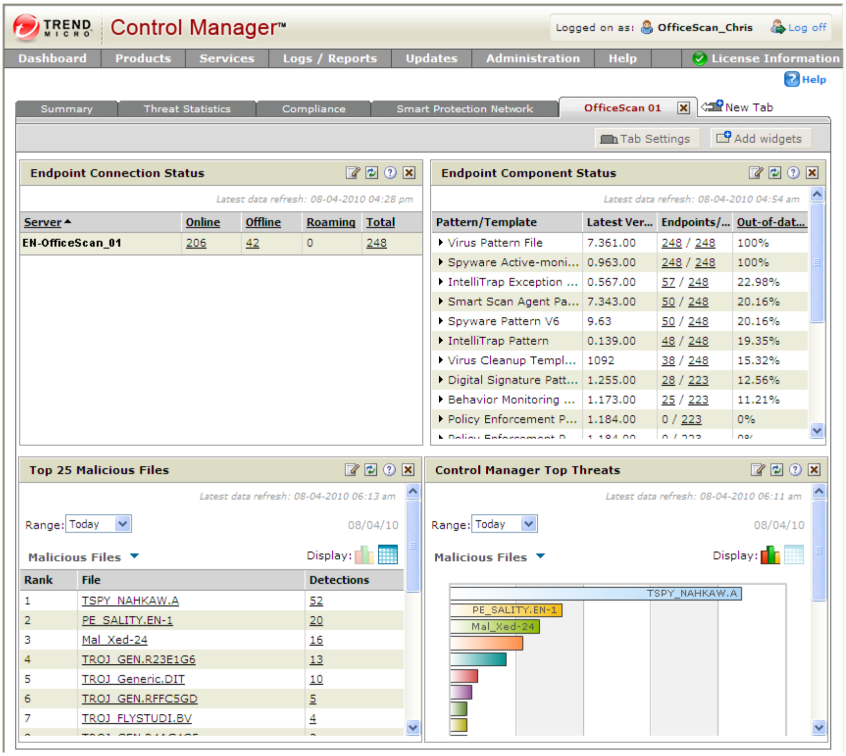
    

    Selected Scope

    EN-OfficeScan_01

46. Click **Ok**.
47. Select **25** from the **Top Threats** list.

48. Click **Save**. The dashboard appears with the modified widget in the OfficeScan 01 tab.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%
Policy Enforcement P...	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:13 am

Range: Today 08/04/10

Malicious Files Display:

Rank	File	Detections
1	TSPY_NAHKAW.A	52
2	PE_SALITY.EN-1	20
3	Mal_Xed-24	16
4	TROJ_GEN.R23E1G6	13
5	TROJ_Generic.DIT	10
6	TROJ_GEN.RFFC5GD	5
7	TROJ_FLYSTUDI.BV	4

Control Manager Top Threats

Latest data refresh: 08-04-2010 06:11 am

Range: Today 08/04/10

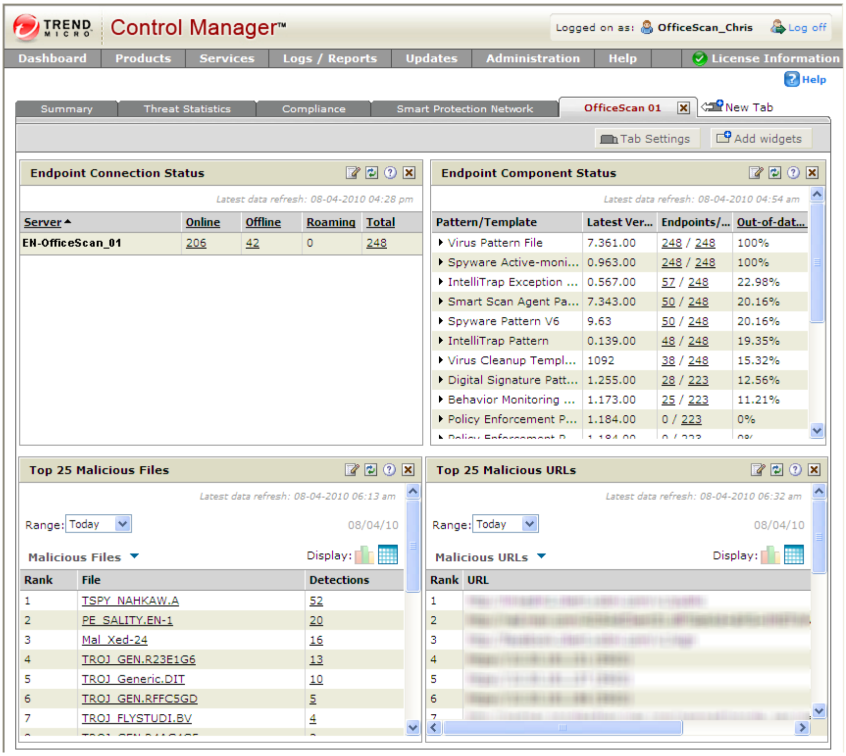
Malicious Files Display:

Chris wants this widget to display the top 25 malicious URLs. The data that the widget currently displays is not for URLs.

49. Move the cursor over **Malicious Files** and select **Malicious URLs** from the list on the widget.

While a bar chart is visually appealing, Chris wants the widget to display the data in a table.

50. Click the **Graph** ▦ icon in the widget. The widget reloads and displays the data in a table.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
Virus Pattern File	7.361.00	248 / 248	100%
Spyware Active-moni...	0.963.00	248 / 248	100%
IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
Spyware Pattern V6	9.63	50 / 248	20.16%
IntelliTrap Pattern	0.139.00	48 / 248	19.35%
Virus Cleanup Templ...	1092	38 / 248	15.32%
Digital Signature Patt...	1.255.00	28 / 223	12.56%
Behavior Monitoring ...	1.173.00	25 / 223	11.21%
Policy Enforcement P...	1.184.00	0 / 223	0%
Policy Enforcement P	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:13 am

Range: Today 08/04/10

Malicious Files ▼ Display:

Rank	File	Detections
1	TSPY_NAHKAW.A	52
2	PE_SALITY.EN-1	20
3	Mal_Xed-24	16
4	TROJ_GEN.R23E1G6	13
5	TROJ_Generic.DIT	10
6	TROJ_GEN.RFFC5GD	5
7	TROJ_FLYSTUDI.BV	4

Top 25 Malicious URLs

Latest data refresh: 08-04-2010 06:32 am

Range: Today 08/04/10

Malicious URLs ▼ Display:

Rank	URL
1	[redacted]
2	[redacted]
3	[redacted]
4	[redacted]
5	[redacted]
6	[redacted]
7	[redacted]

51. Add two more tabs (**OfficeScan 02** and **OfficeScan 03**) for the other OfficeScan servers.

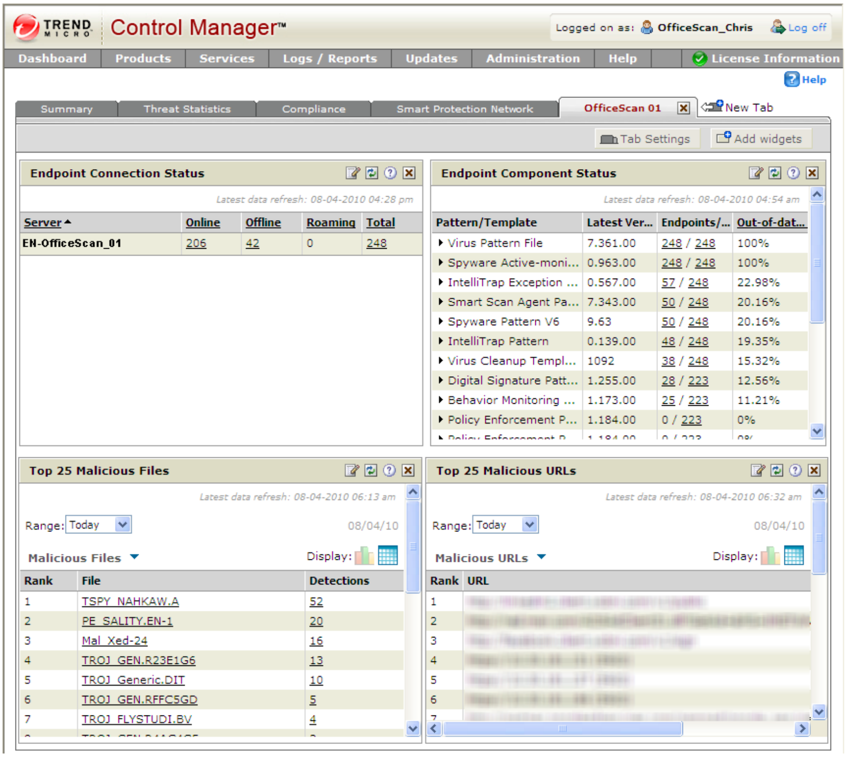
52. Add widgets to the other tabs and "edit" and "configure" the widgets to display data for their respective servers.

Using Widgets

After adding the widgets to the dashboard, Chris wants to view detailed information about the data a widget displays.

To view detailed widget information:

1. Log on to the Control Manager web console as **Chris**. The dashboard appears.
2. Click the **OfficeScan 01** tab.



Endpoint Connection Status

Latest data refresh: 08-04-2010 04:28 pm

Server ▲	Online	Offline	Roaming	Total
EN-OfficeScan_01	206	42	0	248

Endpoint Component Status

Latest data refresh: 08-04-2010 04:54 am

Pattern/Template	Latest Ver...	Endpoints/...	Out-of-dat...
▸ Virus Pattern File	7.361.00	248 / 248	100%
▸ Spyware Active-moni...	0.963.00	248 / 248	100%
▸ IntelliTrap Exception ...	0.567.00	57 / 248	22.98%
▸ Smart Scan Agent Pa...	7.343.00	50 / 248	20.16%
▸ Spyware Pattern V6	9.63	50 / 248	20.16%
▸ IntelliTrap Pattern	0.139.00	48 / 248	19.35%
▸ Virus Cleanup Templ...	1092	38 / 248	15.32%
▸ Digital Signature Patt...	1.255.00	28 / 223	12.56%
▸ Behavior Monitoring ...	1.173.00	25 / 223	11.21%
▸ Policy Enforcement P...	1.184.00	0 / 223	0%

Top 25 Malicious Files

Latest data refresh: 08-04-2010 06:13 am

Range: Today 08/04/10

Malicious Files ▼ Display:

Rank	File	Detections
1	TSPY_NAHKAW.A	52
2	PE_SALITY.EN-1	20
3	Mal_Xed-24	16
4	TROJ_GEN.R23E1G6	13
5	TROJ_Generic.DIT	10
6	TROJ_GEN.RFFC5GD	5
7	TROJ_FLYSTUDI.BV	4

Top 25 Malicious URLs

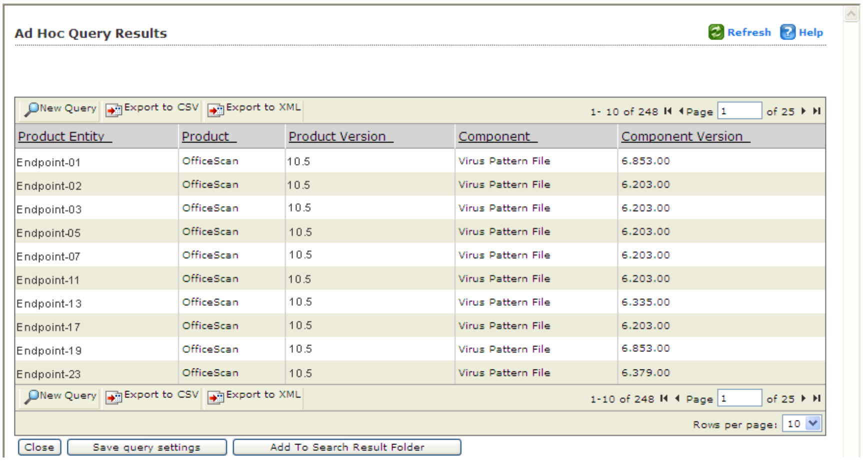
Latest data refresh: 08-04-2010 06:32 am

Range: Today 08/04/10

Malicious URLs ▼ Display:

Rank	URL
1	[redacted]
2	[redacted]
3	[redacted]
4	[redacted]
5	[redacted]
6	[redacted]

3. Click the data under **Endpoints/All** for the **Virus Pattern File** row on the **Endpoint Component Status** widget. An Ad Hoc Query screen appears with results for the data.



Product Entity	Product	Product Version	Component	Component Version
Endpoint-01	OfficeScan	10.5	Virus Pattern File	6.853.00
Endpoint-02	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-03	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-05	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-07	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-11	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-13	OfficeScan	10.5	Virus Pattern File	6.335.00
Endpoint-17	OfficeScan	10.5	Virus Pattern File	6.203.00
Endpoint-19	OfficeScan	10.5	Virus Pattern File	6.853.00
Endpoint-23	OfficeScan	10.5	Virus Pattern File	6.379.00

The query results display which endpoints have out of date components and the name of the components.

Display more results on a screen by selecting the number of rows that appear on a screen.

Sort the columns by clicking on the column heading.

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 4-2. Command Tracking Details

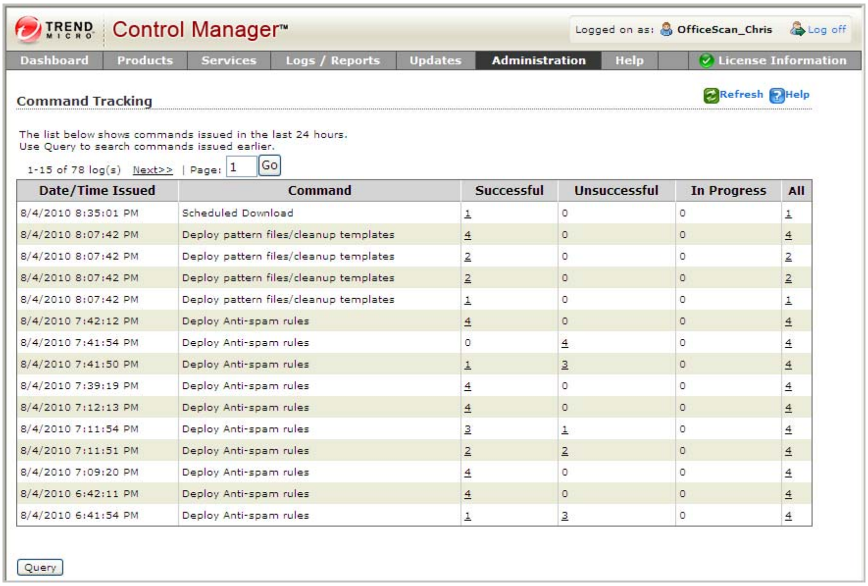
INFORMATION	DESCRIPTION
Date/Time Issued	The date and time when the Control Manager server issued the command to the managed product or child server
Command	The type of command issued
Successful	The number of managed products or child servers that completed the command
Unsuccessful	The number of managed 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.



Command Tracking

The list below shows commands issued in the last 24 hours.
Use Query to search commands issued earlier.

1-15 of 78 log(s) Next>> | Page: 1 Go

Date/Time Issued	Command	Successful	Unsuccessful	In Progress	All
8/4/2010 8:35:01 PM	Scheduled Download	1	0	0	1
8/4/2010 8:07:42 PM	Deploy pattern files/cleanup templates	4	0	0	4
8/4/2010 8:07:42 PM	Deploy pattern files/cleanup templates	2	0	0	2
8/4/2010 8:07:42 PM	Deploy pattern files/cleanup templates	2	0	0	2
8/4/2010 8:07:42 PM	Deploy pattern files/cleanup templates	1	0	0	1
8/4/2010 7:42:12 PM	Deploy Anti-spam rules	4	0	0	4
8/4/2010 7:41:54 PM	Deploy Anti-spam rules	0	4	0	4
8/4/2010 7:41:50 PM	Deploy Anti-spam rules	1	3	0	4
8/4/2010 7:39:19 PM	Deploy Anti-spam rules	4	0	0	4
8/4/2010 7:12:13 PM	Deploy Anti-spam rules	4	0	0	4
8/4/2010 7:11:54 PM	Deploy Anti-spam rules	3	1	0	4
8/4/2010 7:11:51 PM	Deploy Anti-spam rules	2	2	0	4
8/4/2010 7:09:20 PM	Deploy Anti-spam rules	4	0	0	4
8/4/2010 6:42:11 PM	Deploy Anti-spam rules	4	0	0	4
8/4/2010 6:41:54 PM	Deploy Anti-spam rules	1	3	0	4

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 4-3. 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 4-4. 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 4-5. 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	

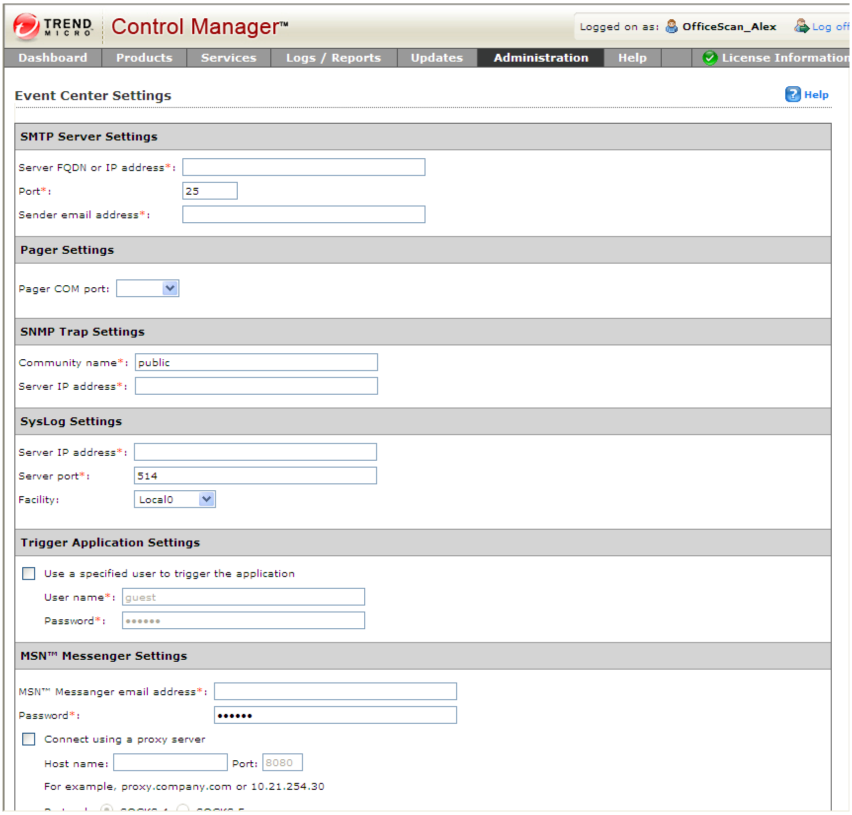
Configuring Event Notification Methods

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.



Event Center Settings

SMTP Server Settings

Server FQDN or IP address*:

Port*: 25

Sender email address*:

Pager Settings

Pager COM port:

SNMP Trap Settings

Community name*: public

Server IP address*:

SysLog Settings

Server IP address*:

Server port*: 514

Facility: Local0

Trigger Application Settings

□ Use a specified user to trigger the application

User name*: guest

Password*: ••••••

MSN™ Messenger Settings

MSN™ Messanger email address*:

Password*: •••••••

□ Connect using a proxy server

Host name: Port: 8080

For example, proxy.company.com or 10.21.254.30

Protocol: ● SOCKS 4 ○ SOCKS 5

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.

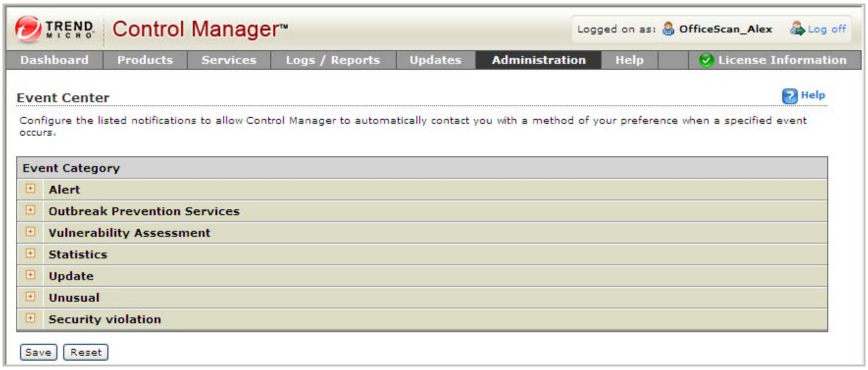
6. Click **Save**.

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.

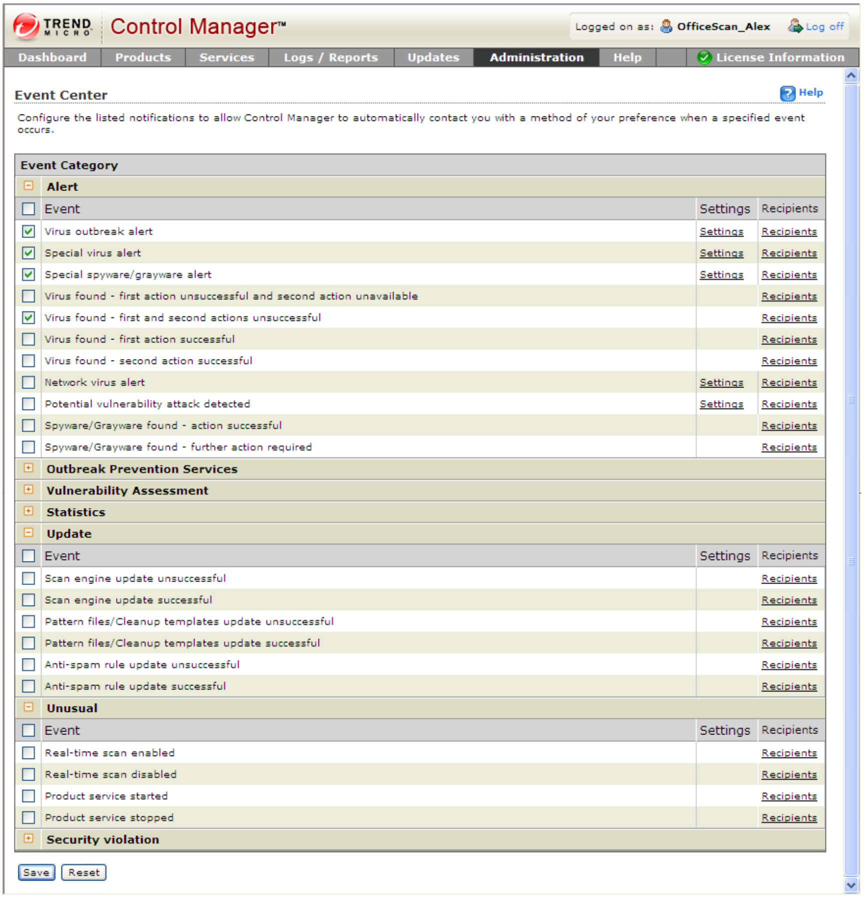


Event Center

Configure the listed notifications to allow Control Manager to automatically contact you with a method of your preference when a specified event occurs.

Event Category
⊞ Alert
⊞ Outbreak Prevention Services
⊞ Vulnerability Assessment
⊞ Statistics
⊞ Update
⊞ Unusual
⊞ Security violation

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

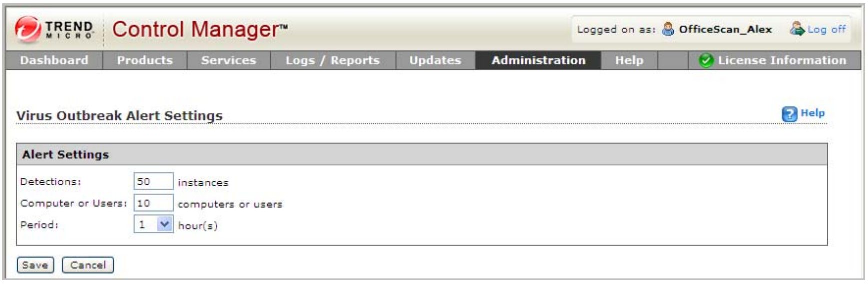


Event Center

Configure the listed notifications to allow Control Manager to automatically contact you with a method of your preference when a specified event occurs.

	Event Category		
⊟	**Alert**		
□	Event	Settings	Recipients
☑	Virus outbreak alert	Settings	Recipients
☑	Special virus alert	Settings	Recipients
☑	Special spyware/grayware alert	Settings	Recipients
□	Virus found - first action unsuccessful and second action unavailable		Recipients
☑	Virus found - first and second actions unsuccessful		Recipients
□	Virus found - first action successful		Recipients
□	Virus found - second action successful		Recipients
□	Network virus alert	Settings	Recipients
□	Potential vulnerability attack detected	Settings	Recipients
□	Spyware/Grayware found - action successful		Recipients
□	Spyware/Grayware found - further action required		Recipients
⊞	**Outbreak Prevention Services**		
⊞	**Vulnerability Assessment**		
⊞	**Statistics**		
⊟	**Update**		
□	Event	Settings	Recipients
□	Scan engine update unsuccessful		Recipients
□	Scan engine update successful		Recipients
□	Pattern files/Cleanup templates update unsuccessful		Recipients
□	Pattern files/Cleanup templates update successful		Recipients
□	Anti-spam rule update unsuccessful		Recipients
□	Anti-spam rule update successful		Recipients
⊟	**Unusual**		
□	Event	Settings	Recipients
□	Real-time scan enabled		Recipients
□	Real-time scan disabled		Recipients
□	Product service started		Recipients
□	Product service stopped		Recipients
⊞	**Security violation**		

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



Virus Outbreak Alert Settings

Alert Settings

Detections:	50	instances
Computer or Users:	10	computers or users
Period:	1	hour(s)

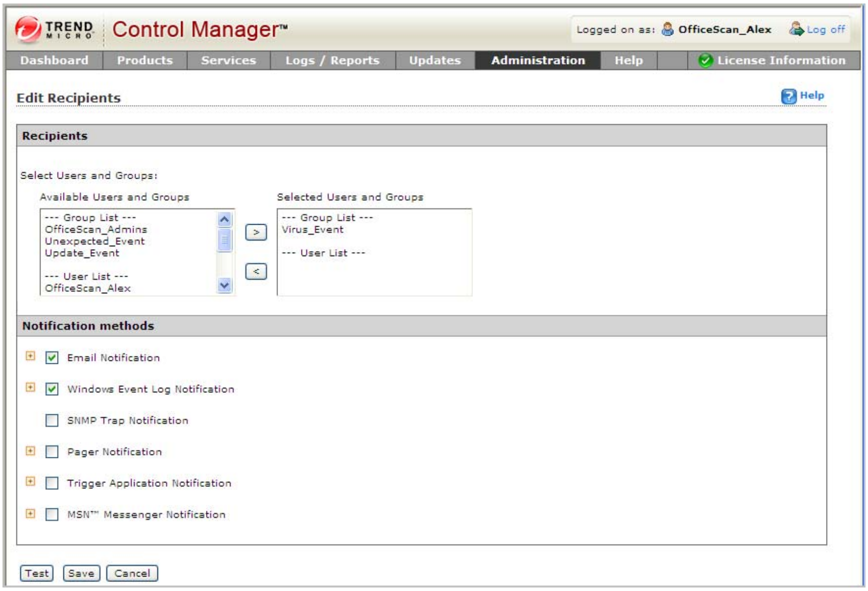
6. Under Alert Settings, provide the following:

   - 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.



Edit Recipients

Recipients

Select Users and Groups:

Available Users and Groups

--- Group List ---
OfficeScan_Admins
Unexpected_Event
Update_Event

--- User List ---
OfficeScan_Alex

Selected Users and Groups

--- Group List ---
Virus_Event

--- User List ---

Notification methods

☑ Email Notification

☑ Windows Event Log Notification

☐ SNMP Trap Notification

☐ Pager Notification

☐ Trigger Application Notification

☐ MSN™ Messenger Notification

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.

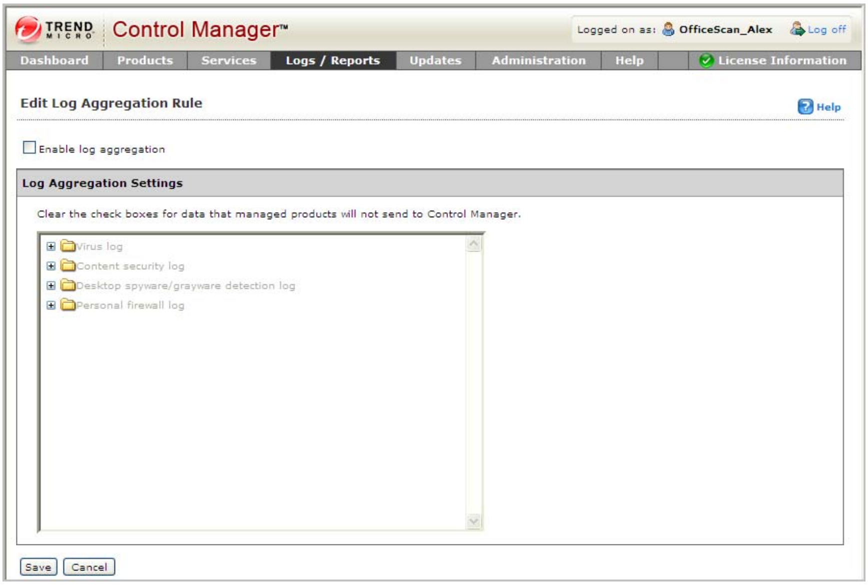
WARNING! **Log aggregation comes at a cost. Information that managed products do not send to Control Manager is lost. Control Manager cannot create reports or queries for information the server does not have. This can raise issues if information that seems unimportant, and managed products drop, later 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.



Edit Log Aggregation Rule

□ Enable log aggregation

Log Aggregation Settings

Clear the check boxes for data that managed products will not send to Control Manager.

- Virus log
- Content security log
- Desktop spyware/grayware detection log
- Personal firewall log

Save Cancel

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

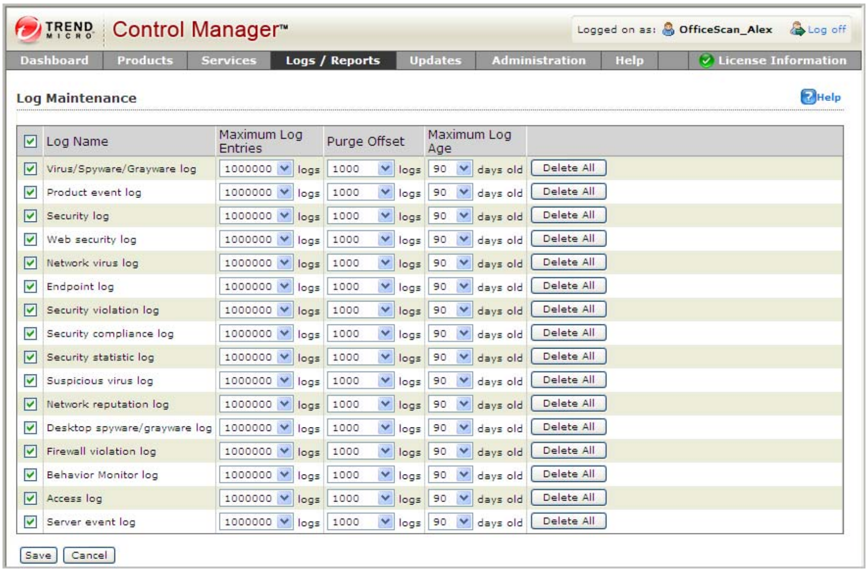
The Log Maintenance screen provides two methods for deleting logs automatically:

- 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.



Log Maintenance

☑	Log Name	Maximum Log Entries	Purge Offset	Maximum Log Age	
☑	Virus/Spyware/Grayware log	1000000 logs	1000 logs	90 days old	Delete All
☑	Product event log	1000000 logs	1000 logs	90 days old	Delete All
☑	Security log	1000000 logs	1000 logs	90 days old	Delete All
☑	Web security log	1000000 logs	1000 logs	90 days old	Delete All
☑	Network virus log	1000000 logs	1000 logs	90 days old	Delete All
☑	Endpoint log	1000000 logs	1000 logs	90 days old	Delete All
☑	Security violation log	1000000 logs	1000 logs	90 days old	Delete All
☑	Security compliance log	1000000 logs	1000 logs	90 days old	Delete All
☑	Security statistic log	1000000 logs	1000 logs	90 days old	Delete All
☑	Suspicious virus log	1000000 logs	1000 logs	90 days old	Delete All
☑	Network reputation log	1000000 logs	1000 logs	90 days old	Delete All
☑	Desktop spyware/grayware log	1000000 logs	1000 logs	90 days old	Delete All
☑	Firewall violation log	1000000 logs	1000 logs	90 days old	Delete All
☑	Behavior Monitor log	1000000 logs	1000 logs	90 days old	Delete All
☑	Access log	1000000 logs	1000 logs	90 days old	Delete All
☑	Server event log	1000000 logs	1000 logs	90 days old	Delete All

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

Querying Log Data

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). Ad Hoc Queries provide 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 format 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 a CSV or XML file

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 clusters of related data cells. Data views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager 5.5 allows direct queries to the Control Manager database. Data views are available to Control Manager 5 report templates and to Ad Hoc Query requests.

Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example, the Virus/Malware Action/Result Summary data view has the following headings:

- Action Result

- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

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

TABLE 4-2. Sample Data View

ACTION RESULT	ACTION TAKEN	UNIQUE ENDPOINTS	UNIQUE SOURCES	DETECTIONS

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 *Understanding Data Views* on page A-2 for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

Product Information

Product Information data views provide information about Control Manager, managed products, components, and product licenses.

TABLE 4-3. Product Information Data Views

CATEGORY	DESCRIPTION
Control Manager Information	Displays information about Control Manager user access, Command Tracking information, and Control Manager server events.

TABLE 4-3. Product Information Data Views

CATEGORY	DESCRIPTION
Managed Product Information	Displays status, detailed, and summary information about managed products or managed product endpoints.
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 4-4. Security Threat Information Data Views

CATEGORY	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 that managed products detect on your network.
Spyware/Grayware Information	Displays summary and detailed data about spyware/grayware that managed products detect on your network.
Content Violation Information	Displays summary and detailed data about prohibited content that managed products detect on your network.

TABLE 4-4. Security Threat Information Data Views

CATEGORY	DESCRIPTION
Spam Violation Information	Displays summary and detailed data about spam that managed products detect on your network.
Web Violation Information	Displays summary and detailed data about Internet violations that managed products detect on your network.
Policy/Rule Violation Information	Displays summary and detailed data about policy/rule violations that managed products detect on your network.
Suspicious Threat Information	Displays summary and detailed data about suspicious activity that managed products detect on your network.

Note: For more information about the available data views Control Manager supports, see *Understanding Data Views* on page A-2.

Data View Terminology

Control Manager uses the following terms in data views, returned queries, and generated reports.

TABLE 4-6. Data View Terminology

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of a computer.
IP	Displays the IP address of a computer.
Port	Displays the port number of an computer.
MAC	Displays the MAC address of an computer.

TABLE 4-6. Data View Terminology

DATA	DESCRIPTION
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product Host	Displays the host name of the server on which the managed product installs.
Product IP	Displays the IP address of the server on which the managed product installs.
Product MAC	Displays the MAC address of the server on which the managed product installs.
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Source Host	Displays the IP address or host name of the computer where security threats originate.
Source IP	Displays the IP address of the computer where security threats originate.
Source Port	Displays the port number of the computer where security threats originate.
Source MAC	Displays the MAC address of the computer where security threats originate.
Unique Endpoints	Displays the number of unique computers affected by security threats. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. Unique Endpoints = 3

TABLE 4-6. Data View Terminology

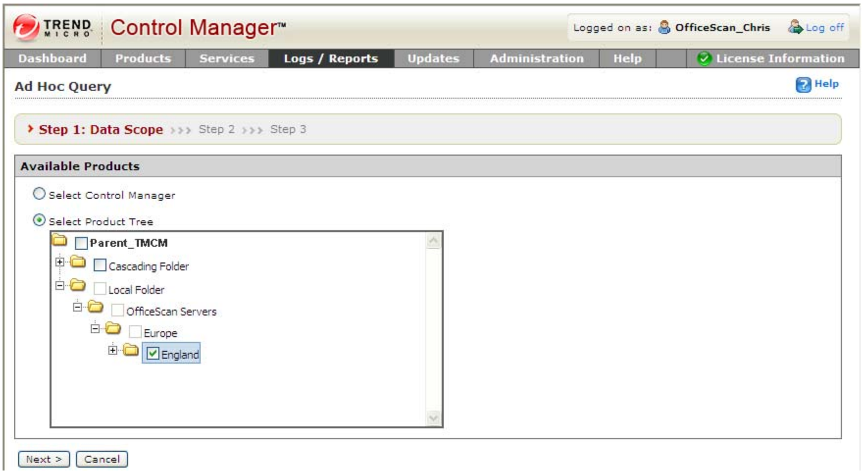
DATA	DESCRIPTION
Unique Sources	Displays the number of unique infection sources where security threats originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. Unique Sources = 2
Unique Senders/Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3
Unique Recipients	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. Unique Recipients = 2
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

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.



○ Select Control Manager

● Select Product Tree

- □ Parent_TMCM
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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:

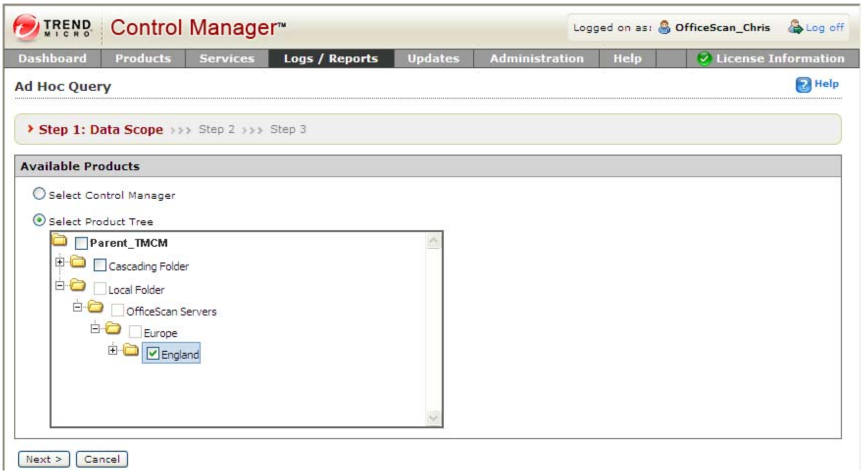
- **Select Control Manager:** Specifies that information originates from the Control Manager server to which the user is currently logged on.

  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**.

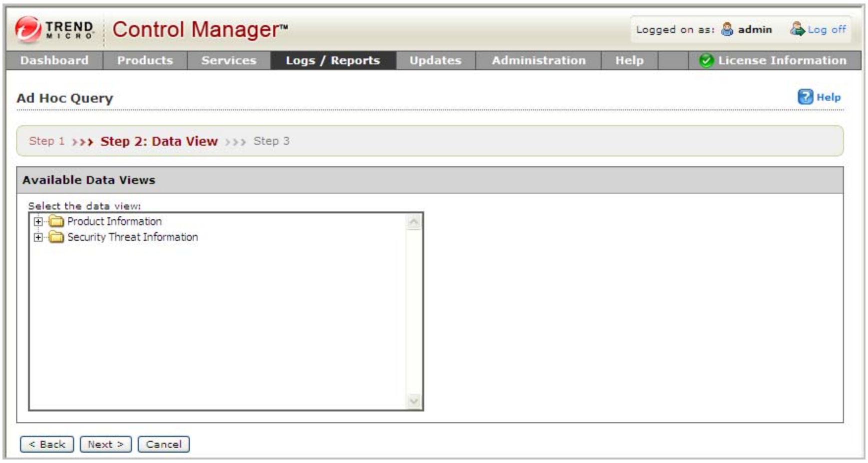


○ Select Control Manager

● Select Product Tree

- □ Parent_TMCM
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

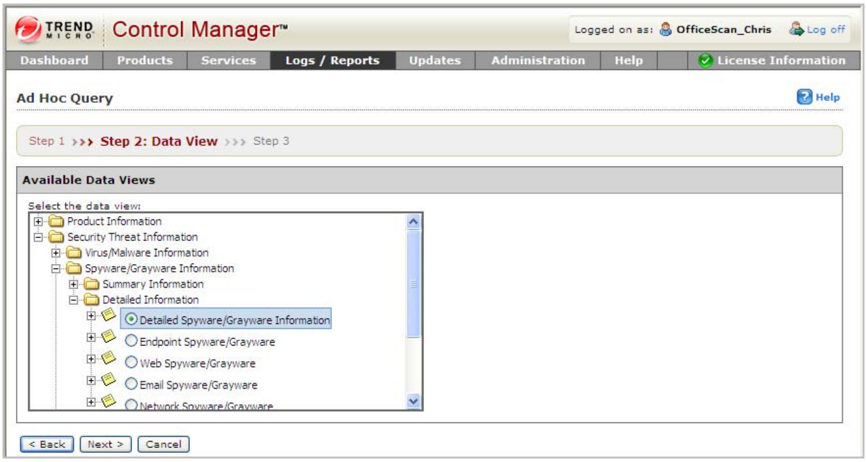
3. Click **Next**. The Select Data View screen appears.



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**

Spyware/Grayware Information. For more information on data views, see *Understanding Data Views* on page A-2.



Ad Hoc Query

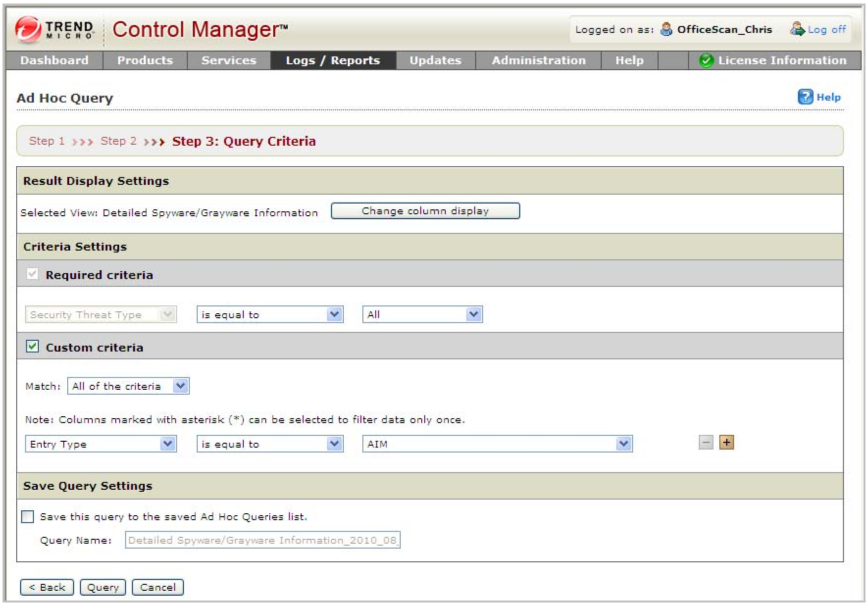
Step 1 ››› Step 2: Data View ››› Step 3

Available Data Views

Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
    - Detailed Information
      - ● Detailed Spyware/Grayware Information
      - ○ Endpoint Spyware/Grayware
      - ○ Web Spyware/Grayware
      - ○ Email Spyware/Grayware
      - ○ Network Spyware/Grayware

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



Ad Hoc Query

Step 1 ››› Step 2 ››› Step 3: Query Criteria

Result Display Settings

Selected View: Detailed Spyware/Grayware Information

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | All

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Entry Type | is equal to | AIM

Save Query Settings

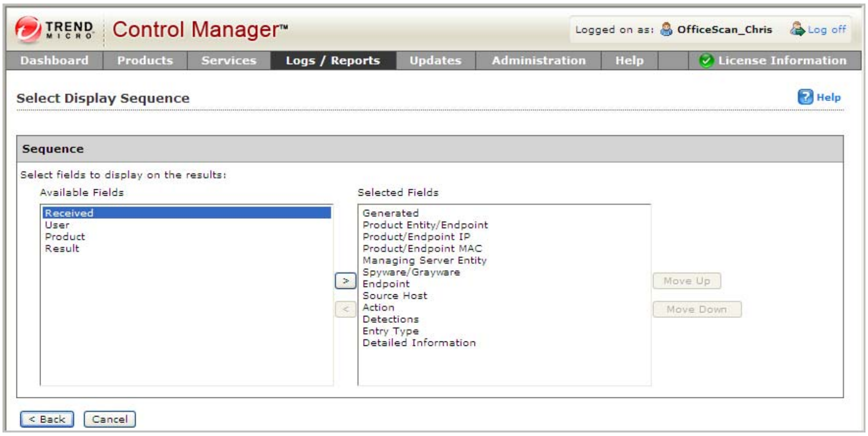
□ Save this query to the saved Ad Hoc Queries list.

Query Name: Detailed Spyware/Grayware Information_2010_08

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.



Select Display Sequence

Sequence

Select fields to display on the results:

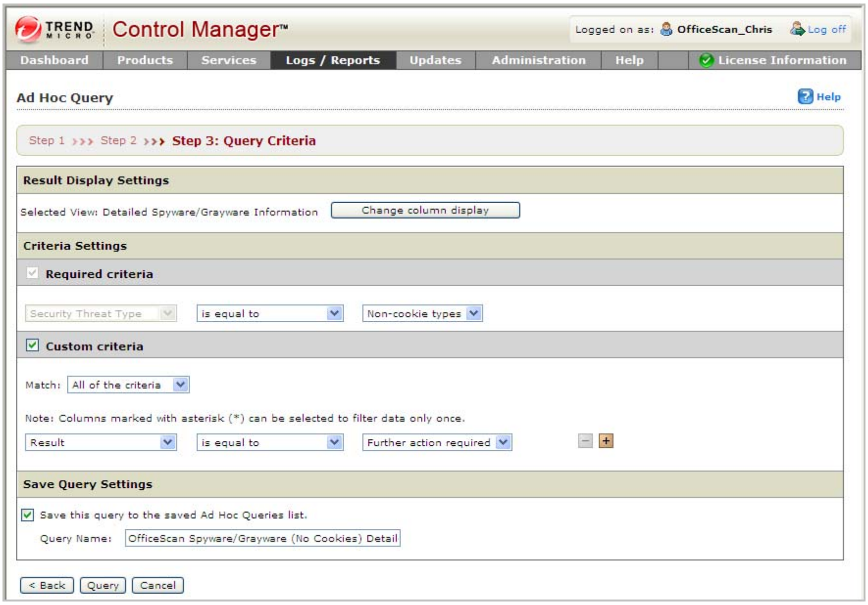
Available Fields
- Received
- User
- Product
- Result

Selected Fields
- Generated
- Product Entity/Endpoint
- Product/Endpoint IP
- Product/Endpoint MAC
- Managing Server Entity
- Spyware/Grayware
- Endpoint
- Source Host
- Action
- Detections
- Entry Type
- Detailed Information

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

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

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



Ad Hoc Query

Step 1 >>> Step 2 >>> Step 3: Query Criteria

Result Display Settings

Selected View: Detailed Spyware/Grayware Information

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | Non-cookie types

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

Save Query Settings

☑ Save this query to the saved Ad Hoc Queries list.

Query Name: OfficeScan Spyware/Grayware (No Cookies) Detail

2. Specify the filtering criteria:

Required Criteria:

d. Specify the following filtering criteria:

- **Security Threat 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:

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

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

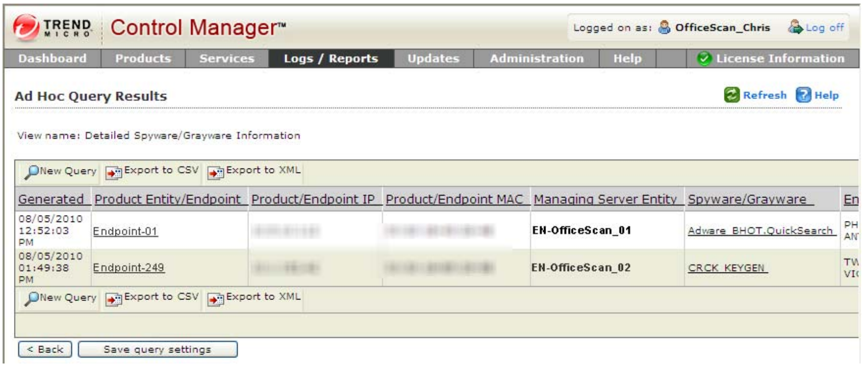
Step 4: Save and complete the query:

1. Click **Save this query to the saved Ad Hoc Queries list** under Save Query Settings to save the Ad Hoc query.
2. Specify 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.



Ad Hoc Query Results

View name: Detailed Spyware/Grayware Information

Generated	Product Entity/Endpoint	Product/Endpoint IP	Product/Endpoint MAC	Managing Server Entity	Spyware/Grayware	En
08/05/2010 12:52:03 PM	Endpoint-01	[redacted]	[redacted]	EN-OfficeScan_01	Adware_BHOT.QuickSearch	PH AN
08/05/2010 01:49:38 PM	Endpoint-249	[redacted]	[redacted]	EN-OfficeScan_02	CRCK_KEYGEN	TW VI

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

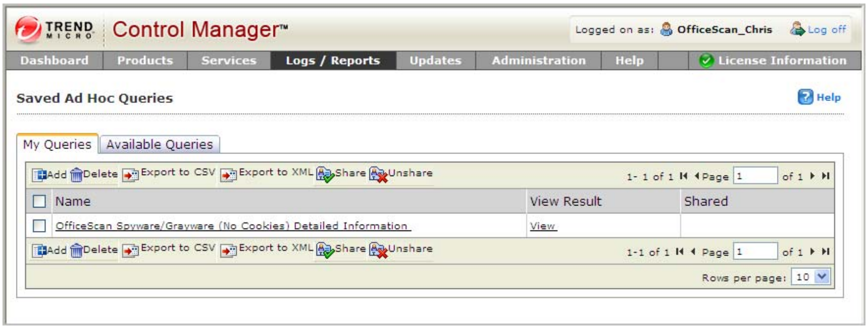
Step 3: Specify filtering criteria, and the specific information that displays

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.

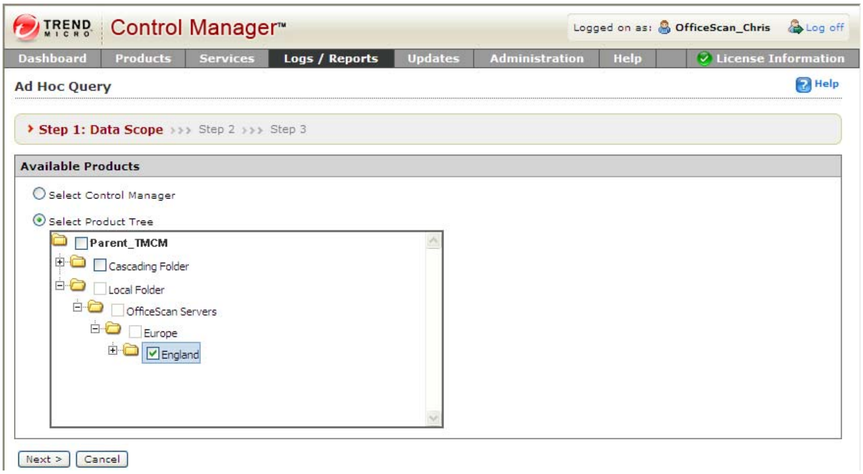
1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports** on the main menu. A drop-down menu appears.
3. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.



Saved Ad Hoc Queries

□	Name	View Result	Shared
□	OfficeScan Spyware/Grayware (No Cookies) Detailed Information	View	

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



Ad Hoc Query

› Step 1: Data Scope ››› Step 2 ››› Step 3

Available Products

○ Select Control Manager

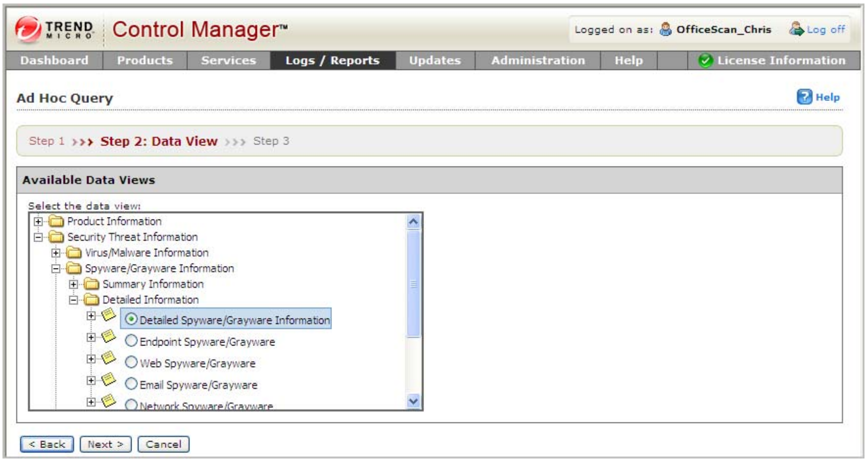
● Select Product Tree

- □ Parent_TMCM
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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.



Ad Hoc Query

Step 1 ››› **Step 2: Data View** ››› Step 3

Available Data Views

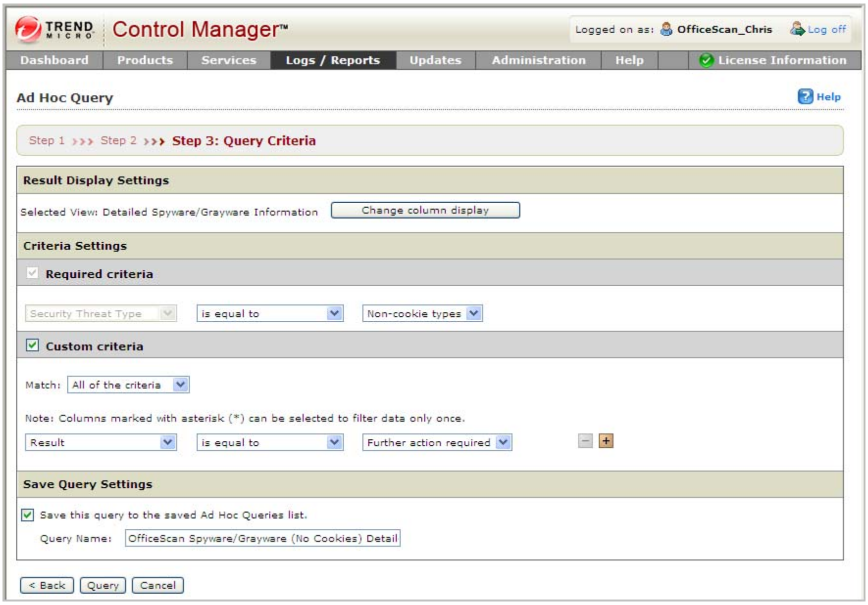
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
    - Detailed Information
      - ● Detailed Spyware/Grayware Information
      - ○ Endpoint Spyware/Grayware
      - ○ Web Spyware/Grayware
      - ○ Email Spyware/Grayware
      - ○ Network Spyware/Grayware

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.



Ad Hoc Query

Step 1 >>> Step 2 >>> Step 3: Query Criteria

Result Display Settings

Selected View: Detailed Spyware/Grayware Information

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | Non-cookie types

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

Save Query Settings

☑ Save this query to the saved Ad Hoc Queries list.

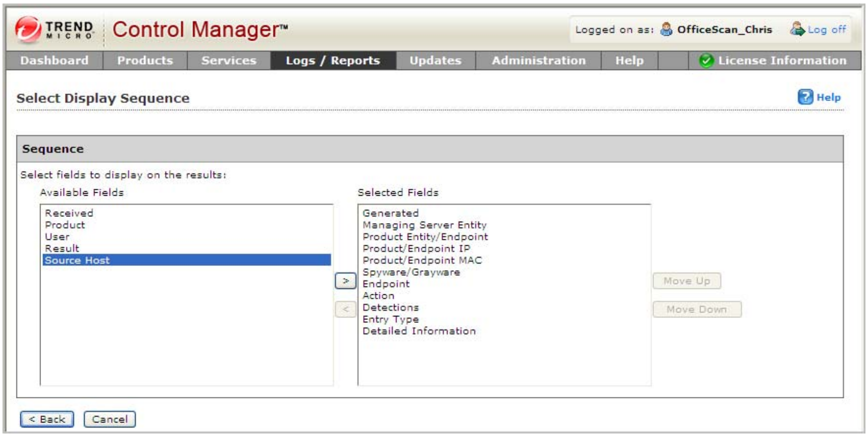
Query Name: OfficeScan Spyware/Grayware (No Cookies) Detail

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.



Select Display Sequence

Sequence

Select fields to display on the results:

Available Fields

- Received
- Product
- User
- Result
- Source Host

Selected Fields

- Generated
- Managing Server Entity
- Product Entity/Endpoint
- Product/Endpoint IP
- Product/Endpoint MAC
- Spyware/Grayware
- Endpoint
- Action
- Detections
- Entry Type
- Detailed Information

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

   - **Source Host**

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

   - **Generated**
   - **Managing Server Entity**
   - **Product Enity/Endpoint**
   - **Product Enity/Endpoint IP**
   - **Product Enity/Endpoint MAC**
   - **Spyware/Grayware**
   - **Endpoint**
   - **Action**
   - **Detections**
   - **Entry Type**

   - **Detailed Information**

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

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

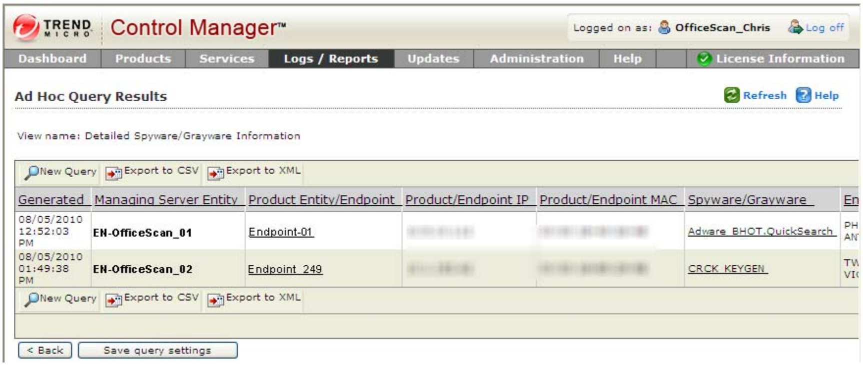
Step 4: Save and complete the query:

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.



Ad Hoc Query Results

View name: Detailed Spyware/Grayware Information

Generated	Managing Server Entity	Product Entity/Endpoint	Product/Endpoint IP	Product/Endpoint MAC	Spyware/Grayware	En
08/05/2010 12:52:03 PM	EN-OfficeScan_01	Endpoint-01	[redacted]	[redacted]	Adware_BHOT.QuickSearch	PH AN
08/05/2010 01:49:38 PM	EN-OfficeScan_02	Endpoint_249	[redacted]	[redacted]	CRCK_KEYGEN	TV VI

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.

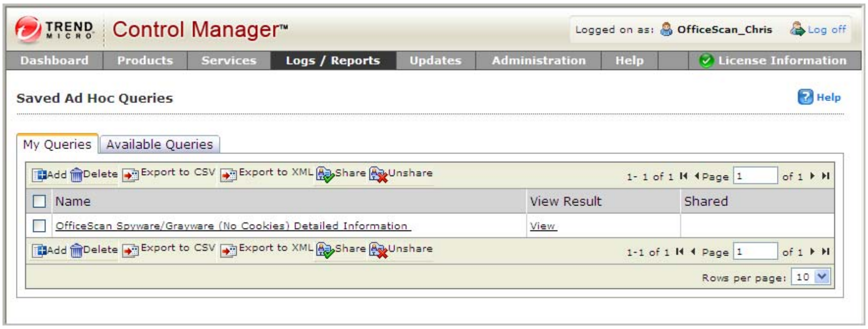
Sharing Saved Ad Hoc Queries

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:

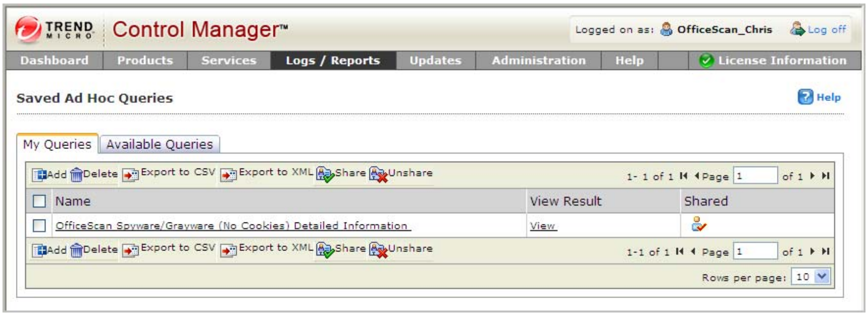
1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.



□ Name	View Result	Shared
□ OfficeScan Spyware/Grayware (No Cookies) Detailed Information	View	

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.



☐ Name	View Result	Shared
☐ OfficeScan Spyware/Grayware (No Cookies) Detailed Information	View	✓

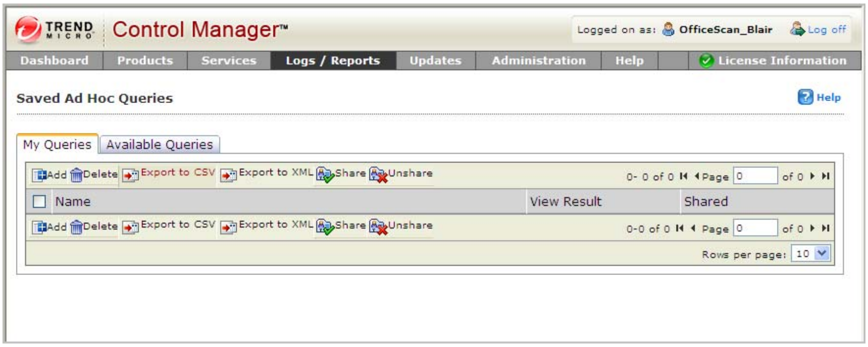
Working With Shared Ad Hoc Queries

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.

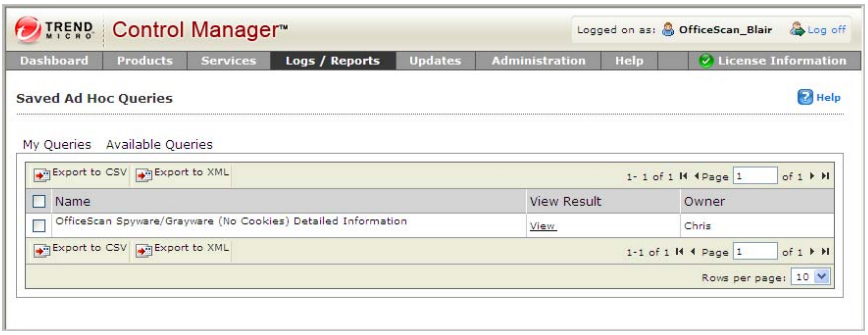
To access Available Queries:

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.



☐ Name	View Result	Shared

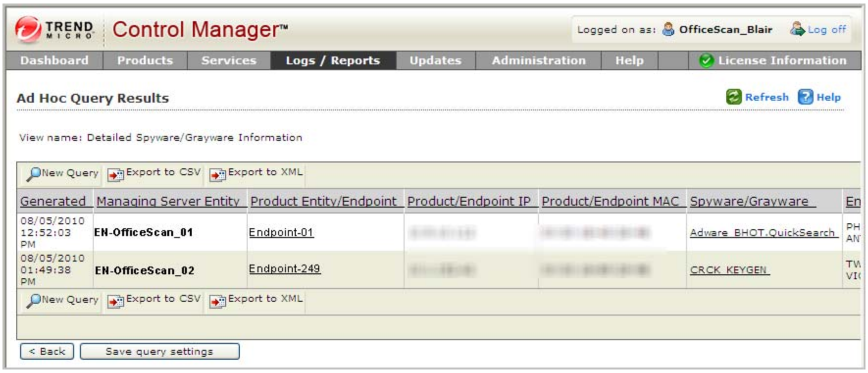
4. Click **Available Queries**. The Available Queries tab appears.



Saved Ad Hoc Queries

□	Name	View Result	Owner
□	OfficeScan Spyware/Grayware (No Cookies) Detailed Information	View	Chris

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



Ad Hoc Query Results

View name: Detailed Spyware/Grayware Information

Generated	Managing Server Entity	Product Entity/Endpoint	Product/Endpoint IP	Product/Endpoint MAC	Spyware/Grayware	En
08/05/2010 12:52:03 PM	EN-OfficeScan_01	Endpoint-01	[redacted]	[redacted]	Adware_BHOT.QuickSearch	PH AN
08/05/2010 01:49:38 PM	EN-OfficeScan_02	Endpoint-249	[redacted]	[redacted]	CRCK_KEYGEN	TW VI

Working With Reports

Understanding Control Manager Report Templates

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

- **Control Manager 5 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 templates, see the *Control Manager Administrator's Guide*.
- **Control Manager 3 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3 templates, see the *Control Manager Administrator's Guide*.

Adding Control Manager 5 Report Templates

Control Manager 5 templates allow greater flexibility for report generation than previous versions of Control Manager templates. Control Manager 5 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 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.

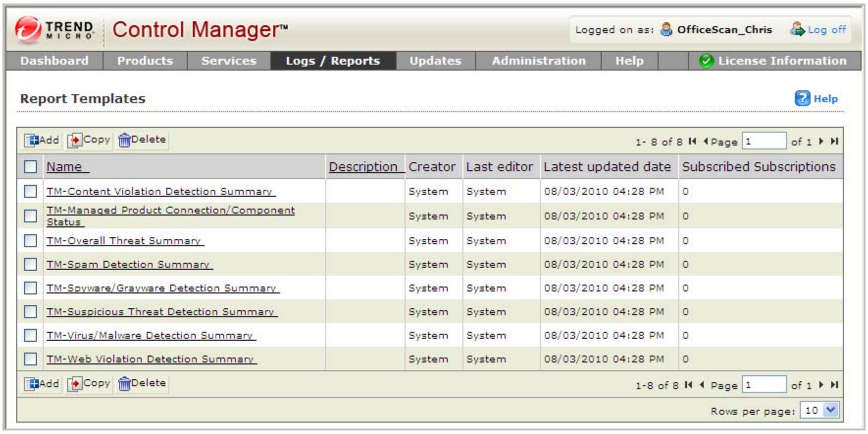
Modifying an Existing Template

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 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.

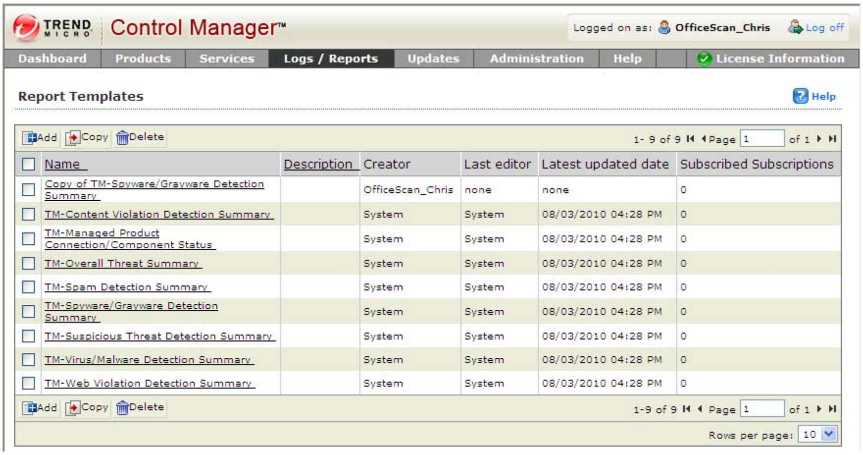


Report Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	TM-Content Violation Detection Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Managed Product Connection/Component Status		System	System	08/03/2010 04:28 PM	0
□	TM-Overall Threat Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Spam Detection Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Spyware/Grayware Detection Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Suspicious Threat Detection Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Virus/Malware Detection Summary		System	System	08/03/2010 04:28 PM	0
□	TM-Web Violation Detection Summary		System	System	08/03/2010 04:28 PM	0

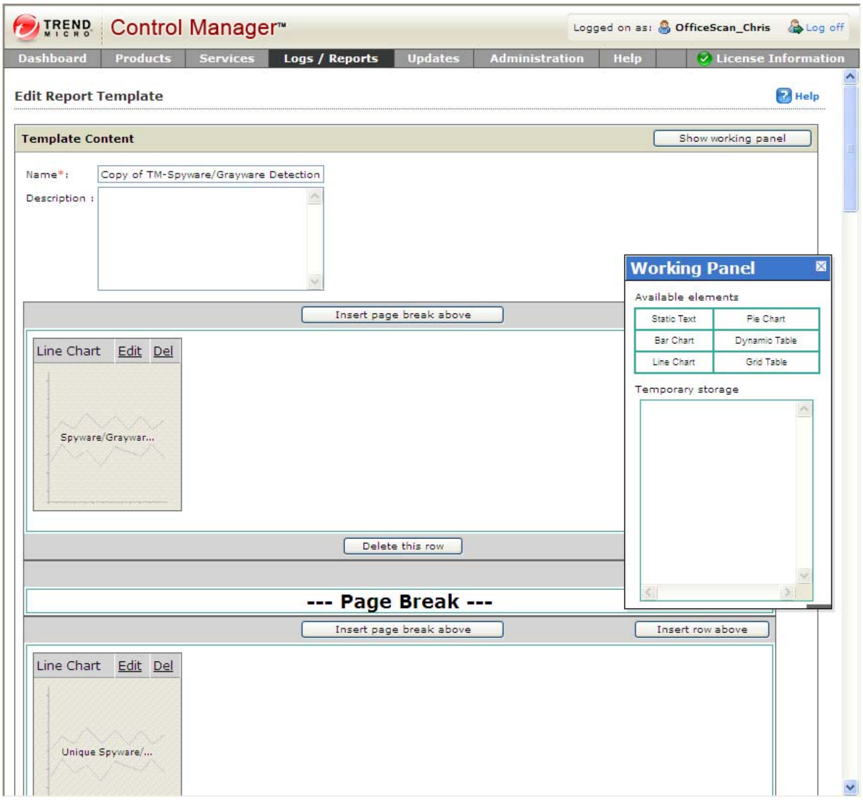
4. Select **TM-Spyware/Grayware Detection Summary**.

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



☐	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
☐	Copy of TM-Spyware/Grayware Detection Summary		OfficeScan_Chris	none	none	0
☐	TM-Content Violation Detection Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Managed Product Connection/Component Status		System	System	08/03/2010 04:28 PM	0
☐	TM-Overall Threat Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Spam Detection Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Spyware/Grayware Detection Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Suspicious Threat Detection Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Virus/Malware Detection Summary		System	System	08/03/2010 04:28 PM	0
☐	TM-Web Violation Detection Summary		System	System	08/03/2010 04:28 PM	0

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



Name*: Copy of TM-Spyware/Grayware Detection

Description :

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

   OfficeScan Spyware/Grayware Detection Summary

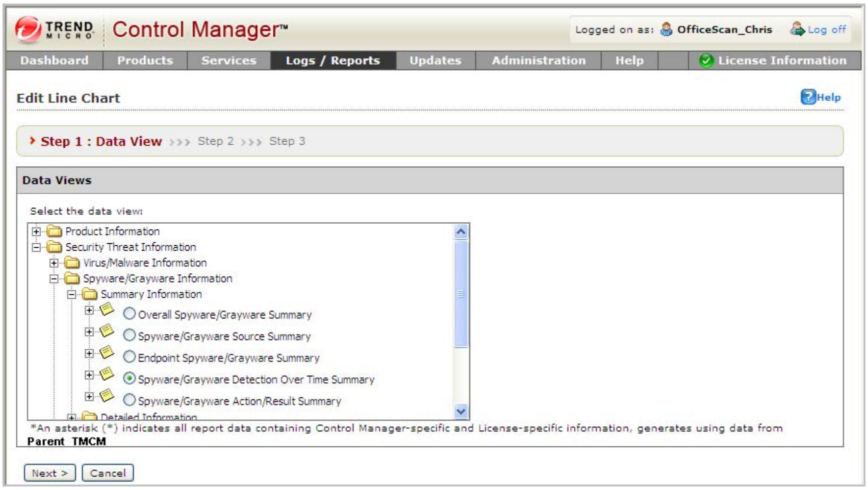
8. Type the following in the **Description** field:

   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.



Edit Line Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

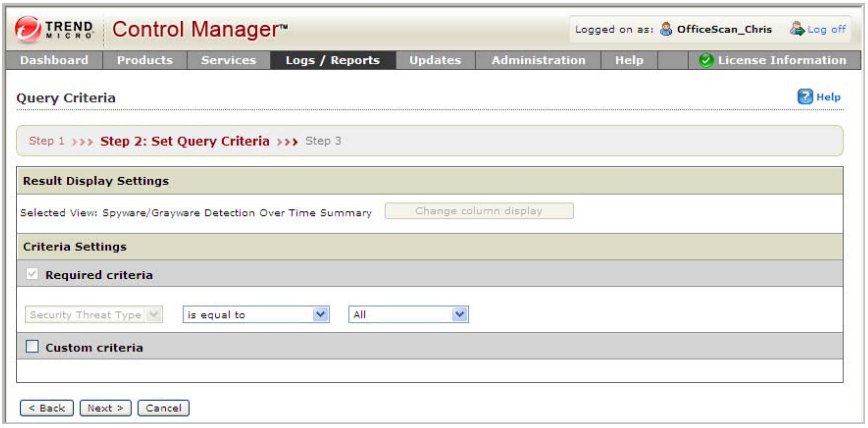
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ● Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 ››› **Step 2: Set Query Criteria** ››› Step 3

Result Display Settings

Selected View: Spyware/Grayware Detection Over Time Summary

Criteria Settings

☑ **Required criteria**

Security Threat Type | is equal to | All

□ **Custom criteria**

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.

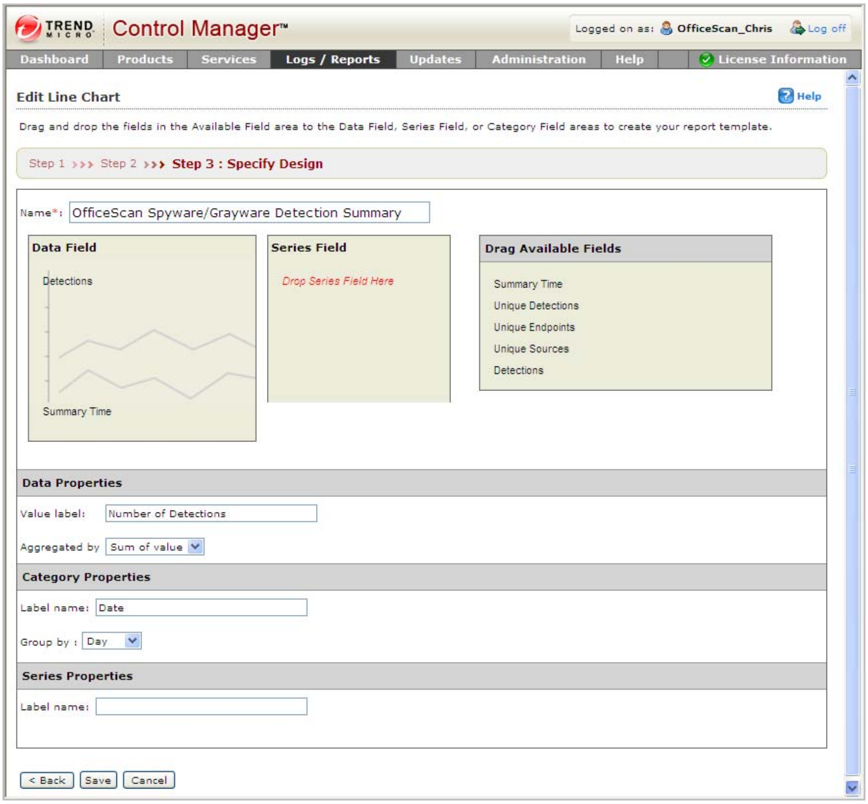
Chris does not want cookies to appear in his line chart for spyware/grayware.

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

   Security Threat 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.



Edit Line Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Name*: OfficeScan Spyware/Grayware Detection Summary

Data Field: Detections, Summary Time

Data Properties

Value label: Number of Detections

Aggregated by: Sum of value

Category Properties

Label name: Date

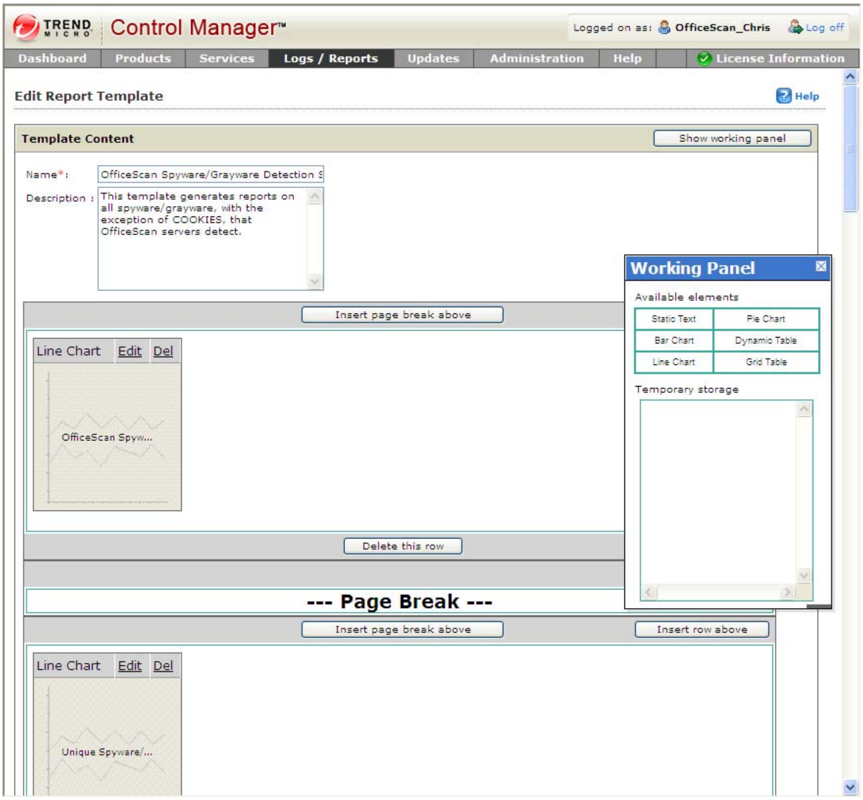
Group by : Day

Series Properties

Label name:

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 Report Template

Template Content

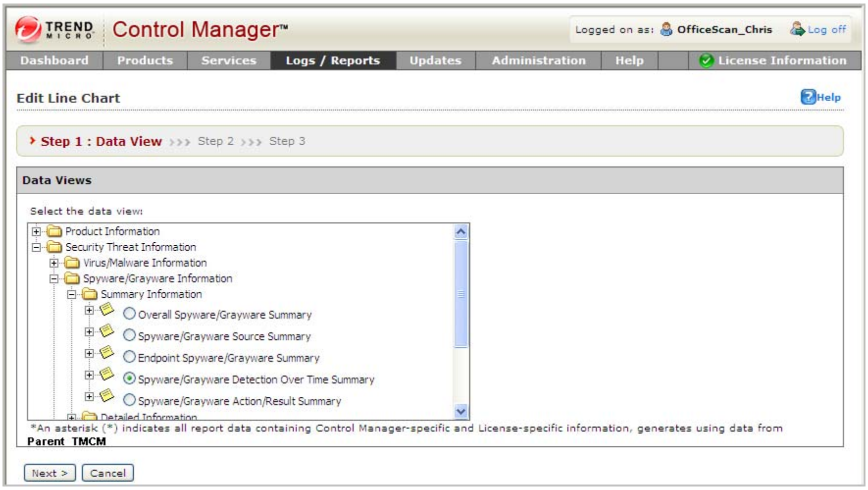
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 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.



Edit Line Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

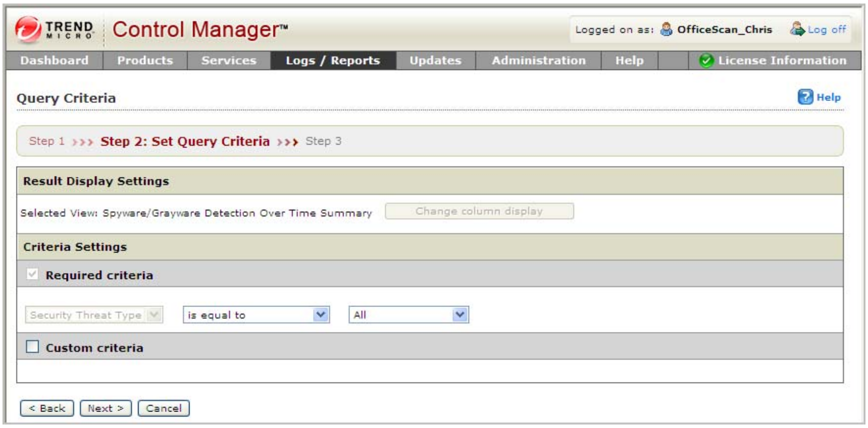
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ● Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Selected View: Spyware/Grayware Detection Over Time Summary

☑ Required criteria

Security Threat Type | is equal to | All

☐ Custom criteria

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.

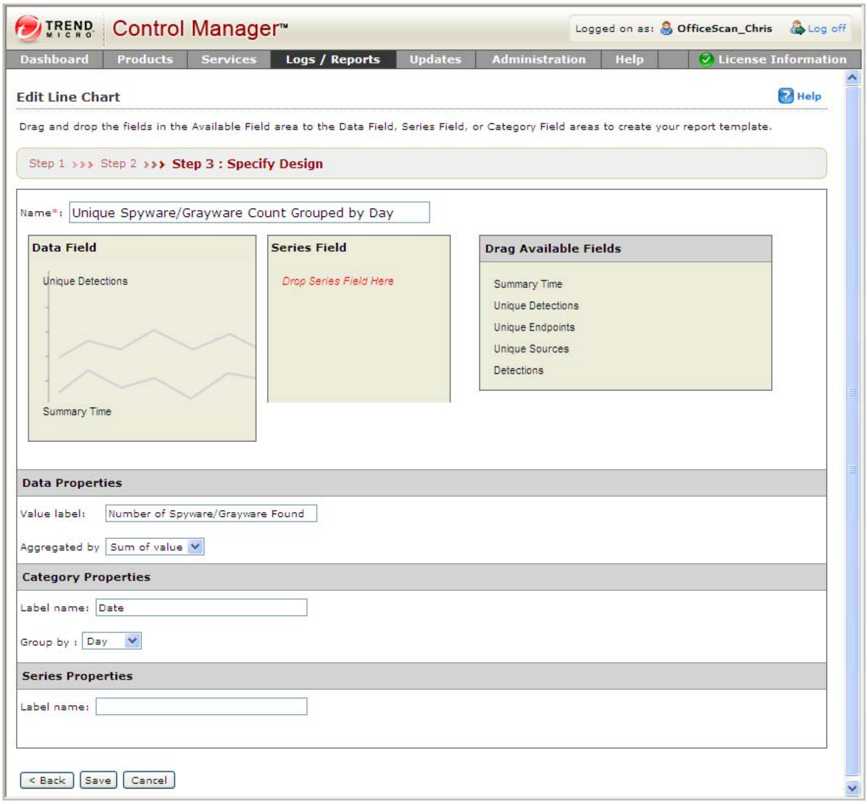
Chris does not want cookies to appear in his line chart for spyware/grayware.

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

   Security Threat 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.



Edit Line Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Name*: Unique Spyware/Grayware Count Grouped by Day

Data Properties

Value label: Number of Spyware/Grayware Found

Aggregated by Sum of value

Category Properties

Label name: Date

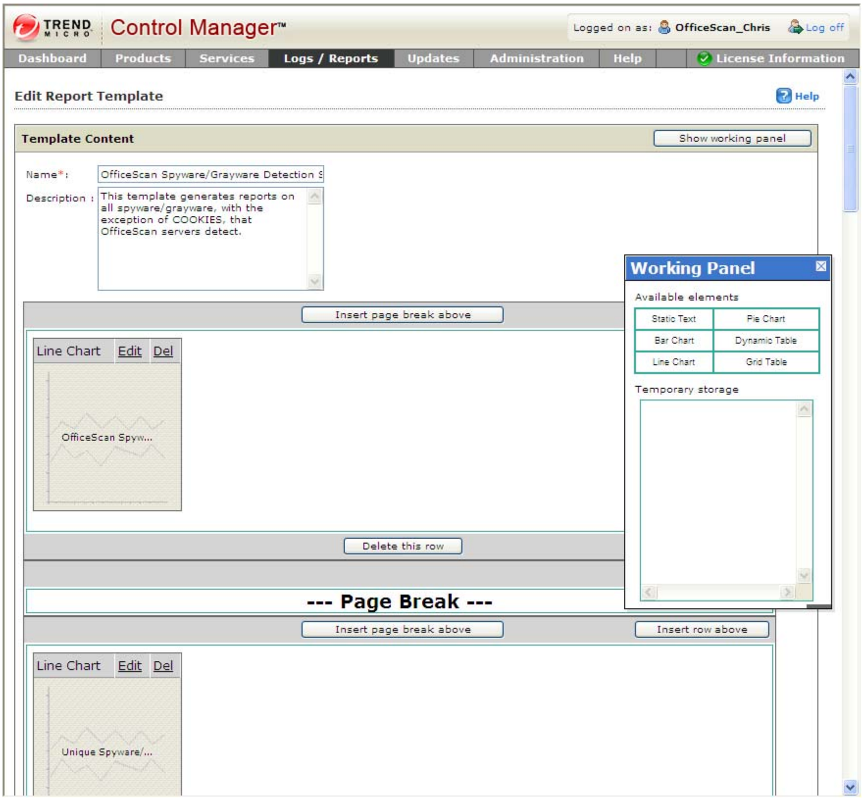
Group by : Day

Series Properties

Label name:

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 Edit Report Template screen appears.



Edit Report Template

Template Content

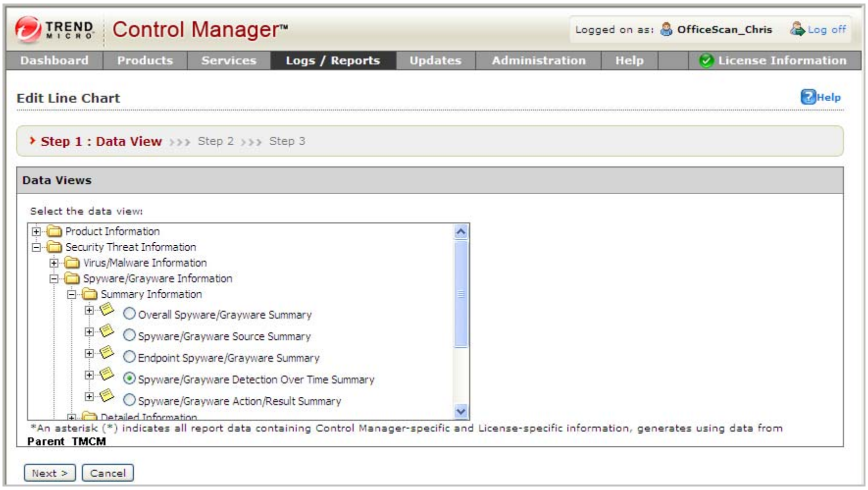
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 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.



Edit Line Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

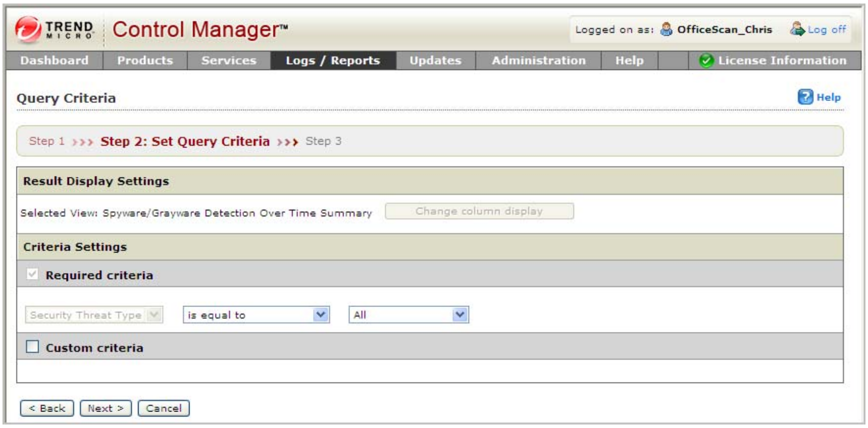
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ● Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

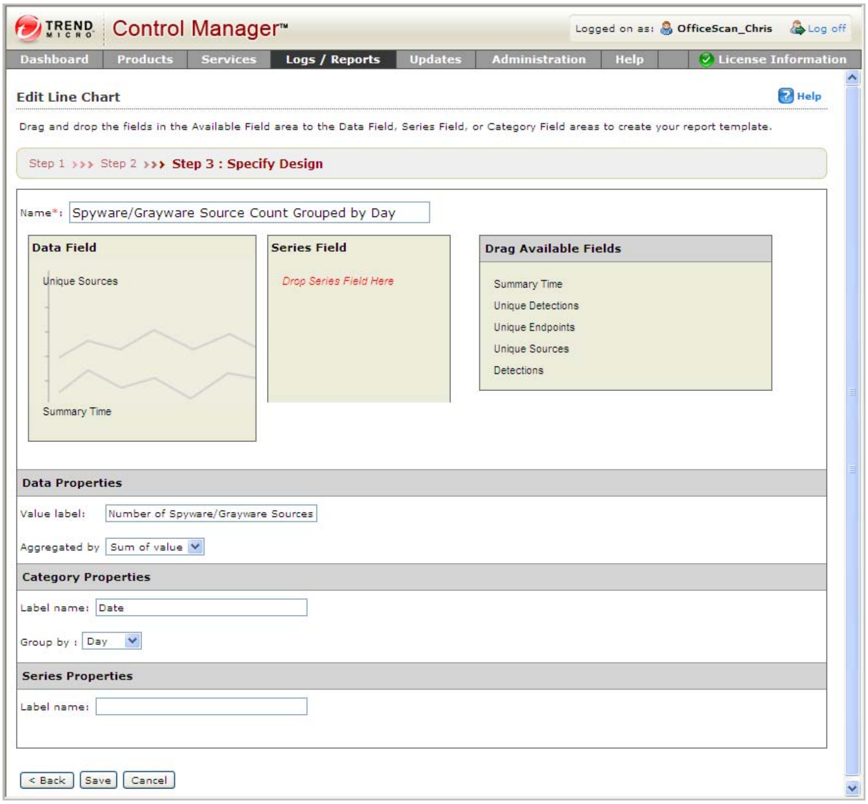
Chris does not want cookies to appear in his line chart for spyware/grayware.

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

   Security Threat 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.



Edit Line Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name*: Spyware/Grayware Source Count Grouped by Day

Data Field: Unique Sources, Summary Time

Series Field: Drop Series Field Here

Drag Available Fields: Summary Time, Unique Detections, Unique Endpoints, Unique Sources, Detections

Data Properties

Value label: Number of Spyware/Grayware Sources

Aggregated by: Sum of value

Category Properties

Label name: Date

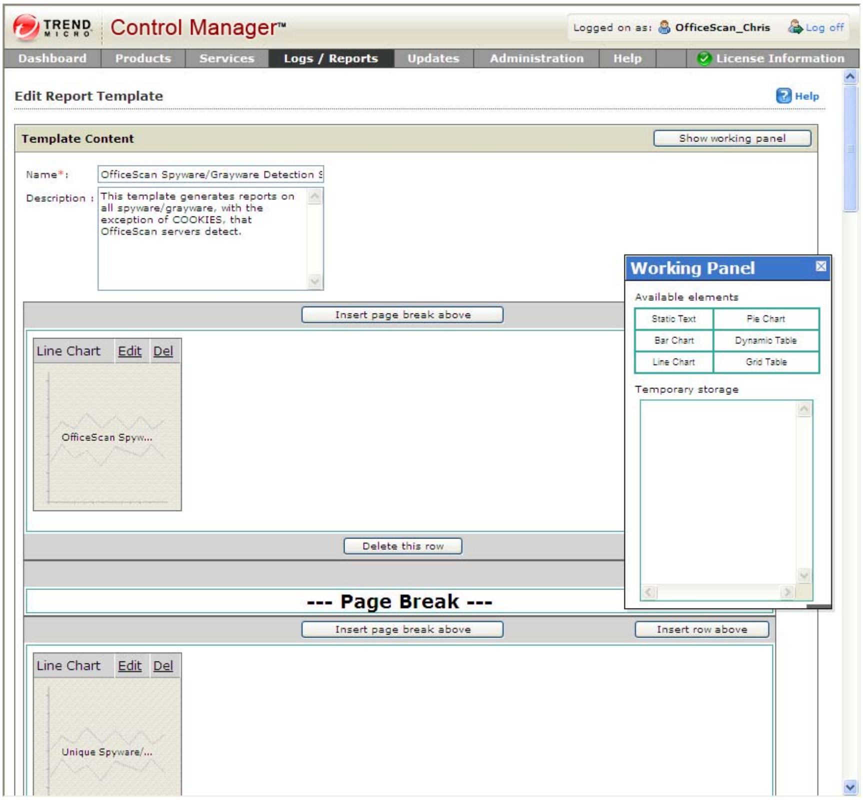
Group by : Day

Series Properties

Label name:

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 Edit Report Template screen appears.



Edit Report Template

Template Content

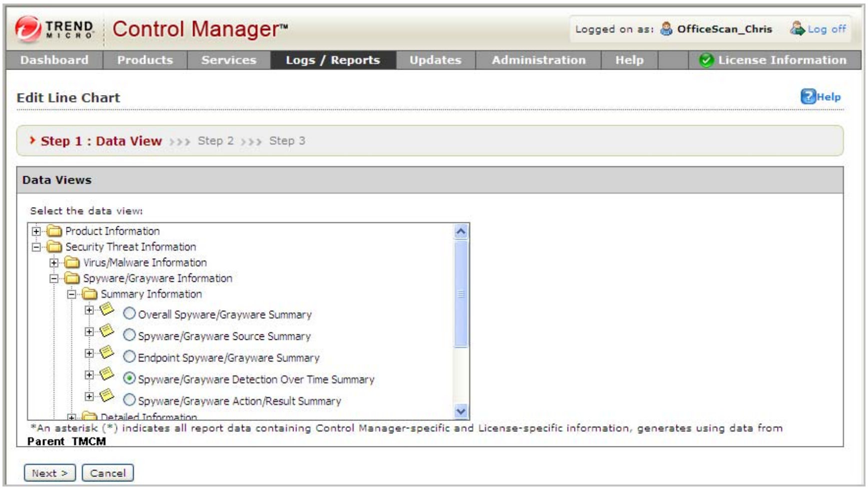
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 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.



Edit Line Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

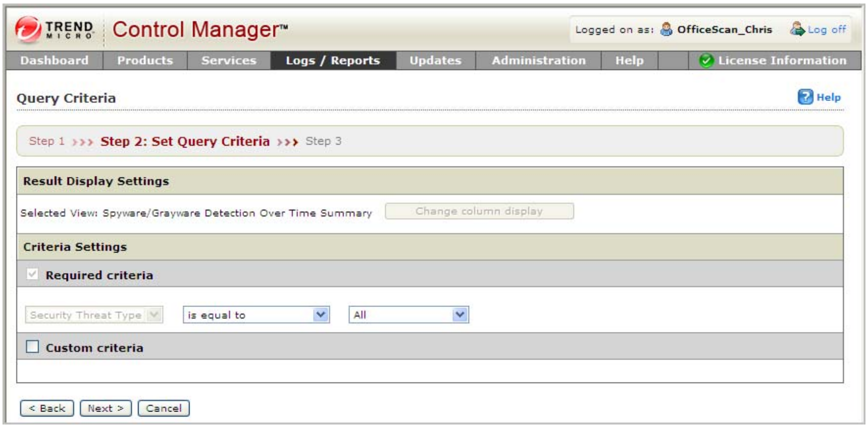
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ● Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

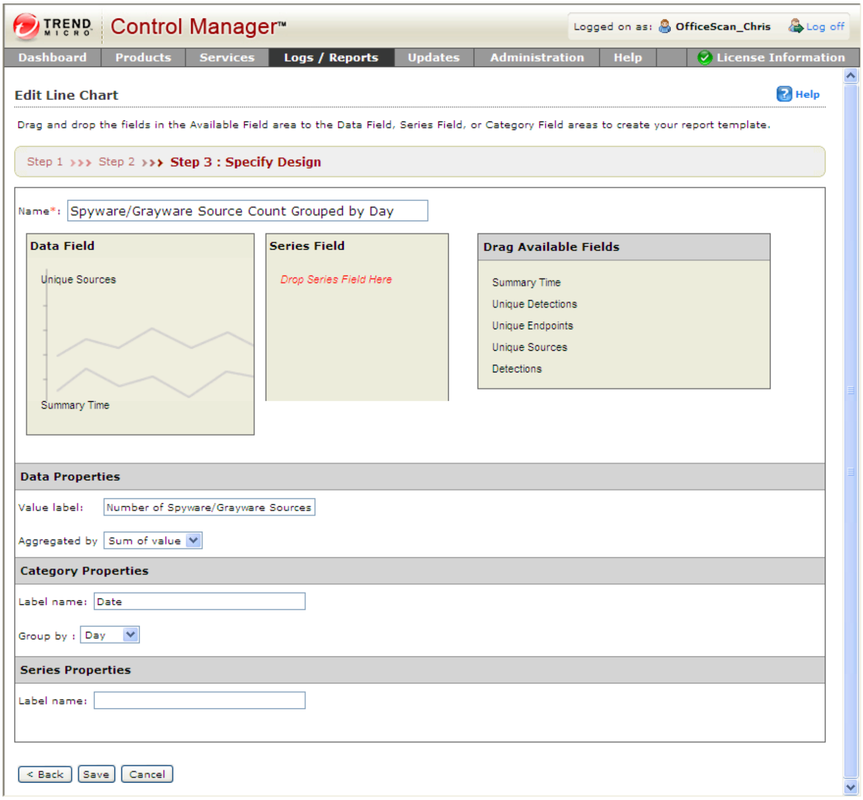
Chris does not want cookies to appear in his line chart for spyware/grayware.

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

   Security Threat 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.



Edit Line Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› Step 3 : Specify Design

Name*: Spyware/Grayware Source Count Grouped by Day

Data Properties

Value label: Number of Spyware/Grayware Sources

Aggregated by: Sum of value

Category Properties

Label name: Date

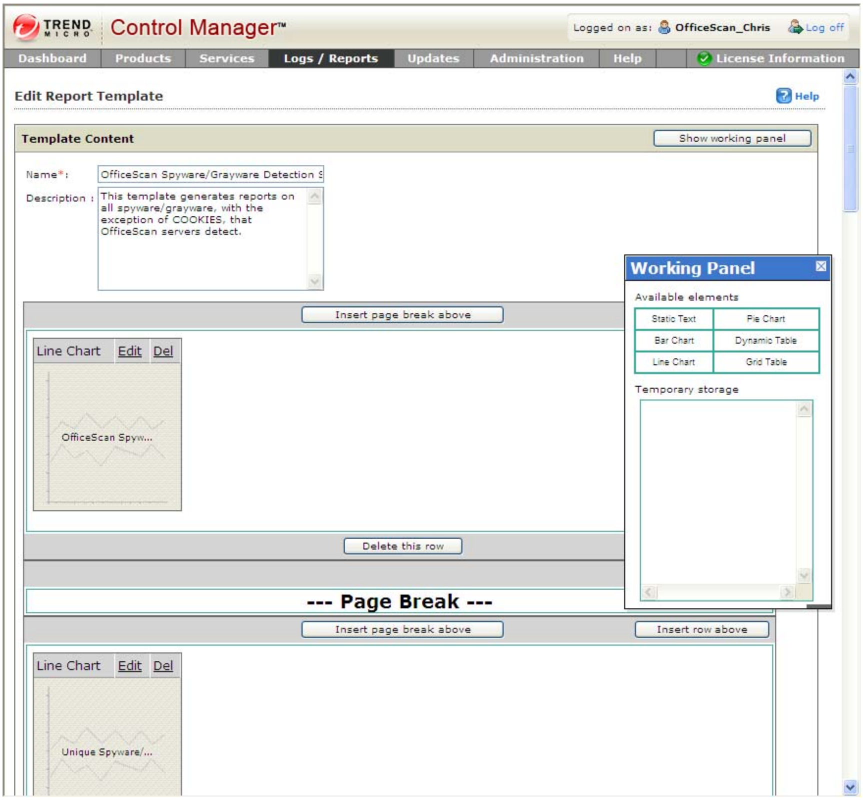
Group by : Day

Series Properties

Label name:

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 Edit Report Template screen appears.



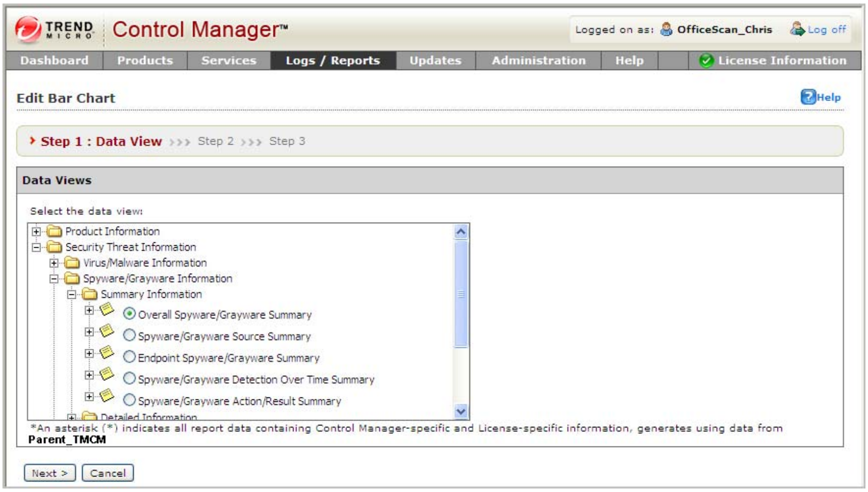
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Top 25 Spyware/Grayware bar chart:

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



Edit Bar Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

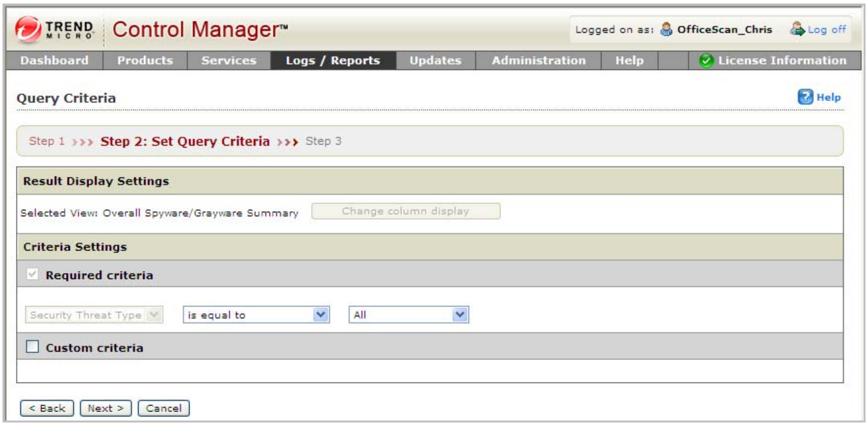
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ● Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

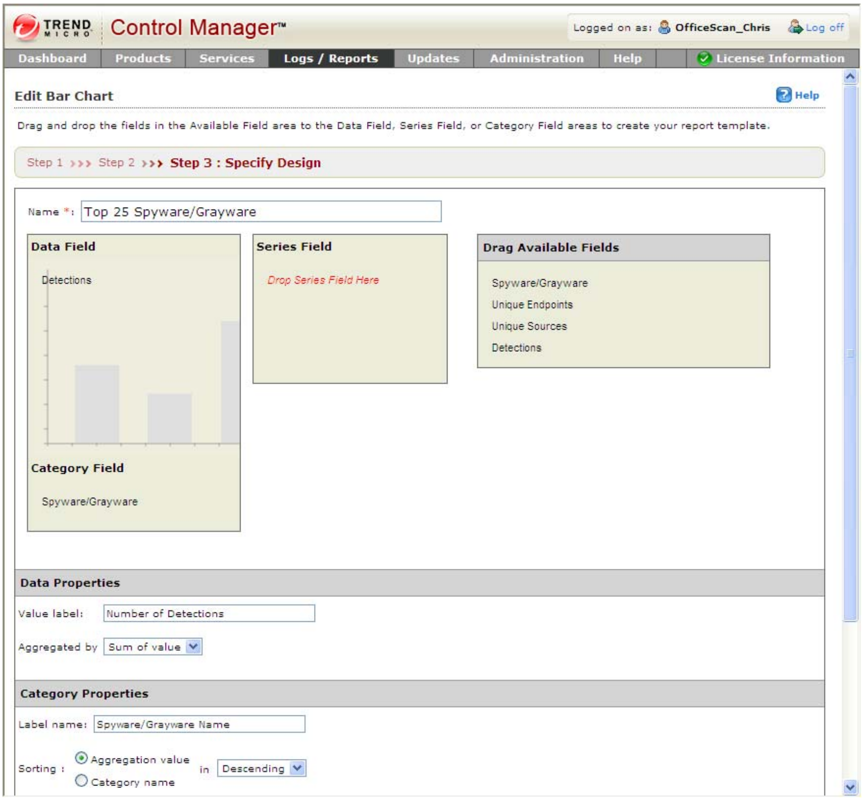
Chris does not want cookies to appear in his bar chart for spyware/grayware.

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

   Security Threat 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.



Edit Bar Chart

Help

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *: Top 25 Spyware/Grayware

Data Field

Detections

Category Field

Spyware/Grayware

Series Field

Drop Series Field Here

Drag Available Fields

Spyware/Grayware
Unique Endpoints
Unique Sources
Detections

Data Properties

Value label: Number of Detections

Aggregated by: Sum of value

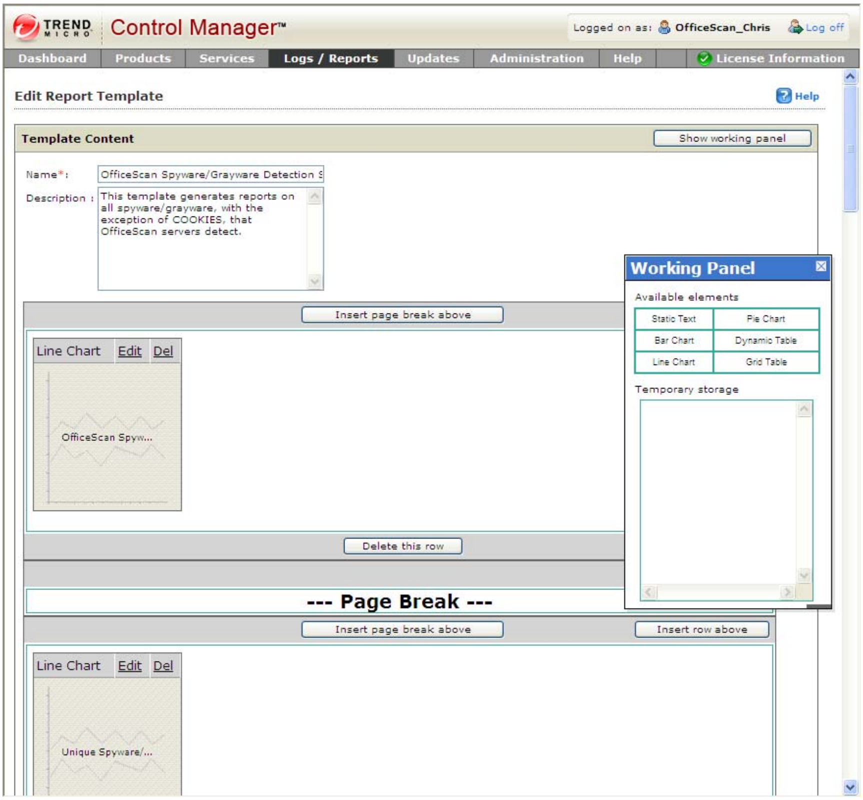
Category Properties

Label name: Spyware/Grayware Name

Sorting : ● Aggregation value ○ Category name in Descending

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

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



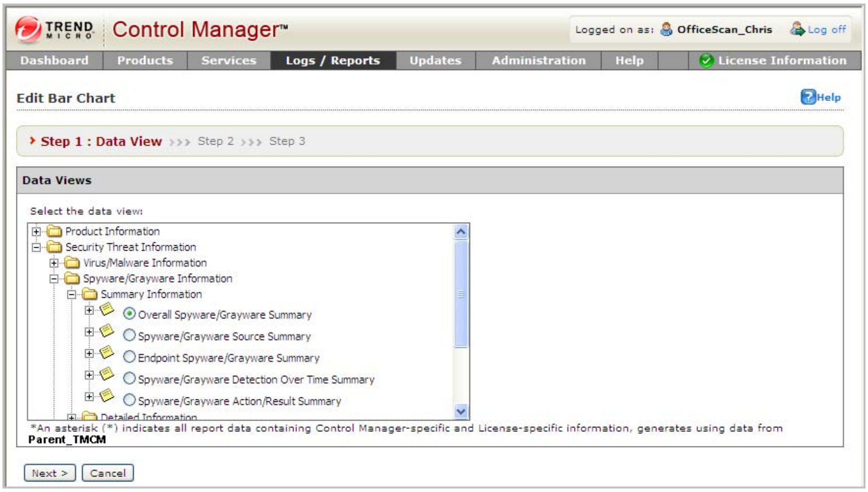
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Overall Spyware/Grayware Summary grid table:

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



Edit Bar Chart

› Step 1 : Data View >>> Step 2 >>> Step 3

Data Views

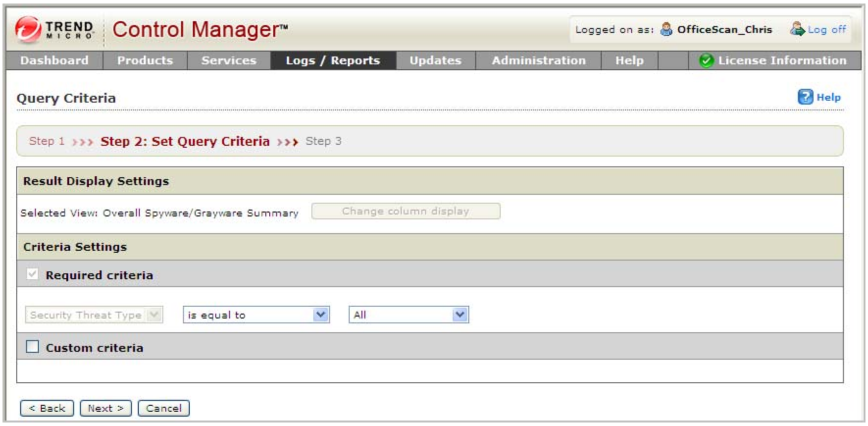
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ● Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Result Display Settings

Selected View: Overall Spyware/Grayware Summary

Criteria Settings

☑ **Required criteria**

Security Threat Type | is equal to | All

□ **Custom criteria**

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.

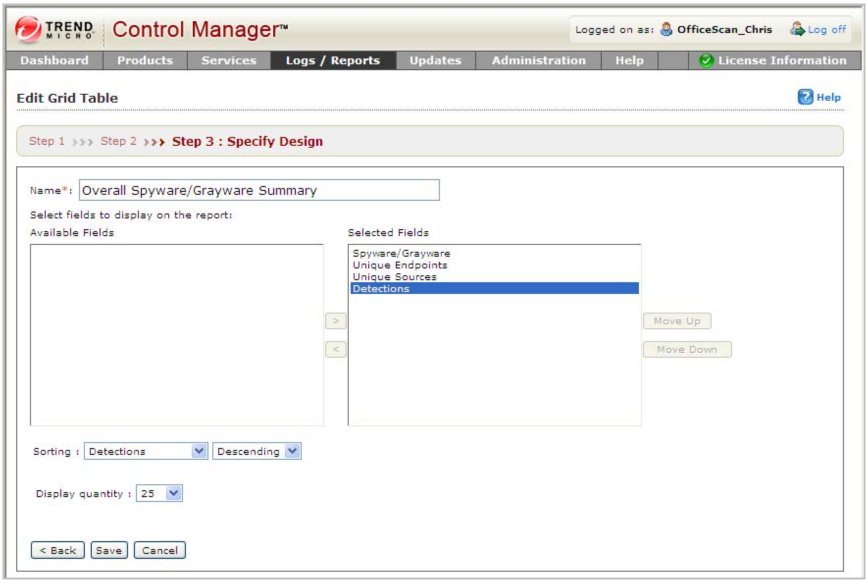
Chris does not want cookies to appear in his grid table for spyware/grayware.

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

   Security Threat 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.



Name*: Overall Spyware/Grayware Summary

Select fields to display on the report:

Available Fields

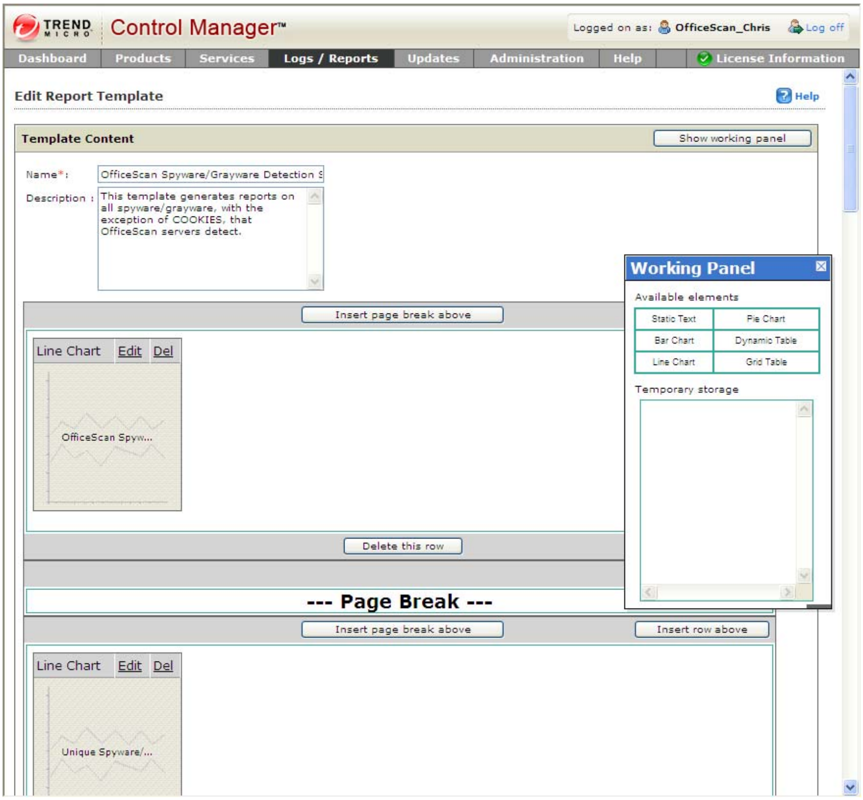
Selected Fields: Spyware/Grayware, Unique Endpoints, Unique Sources, Detections

Sorting : Detections, Descending

Display quantity : 25

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 Report Template

Template Content

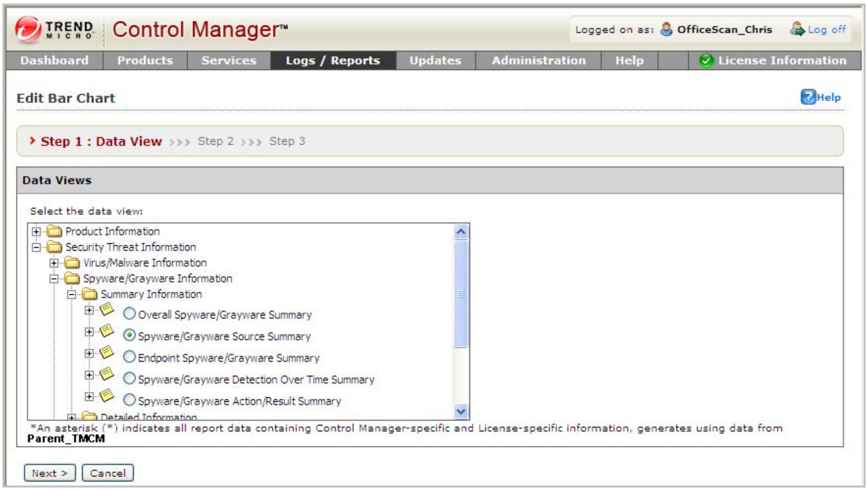
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Top 25 Spyware/Grayware Sources bar chart:

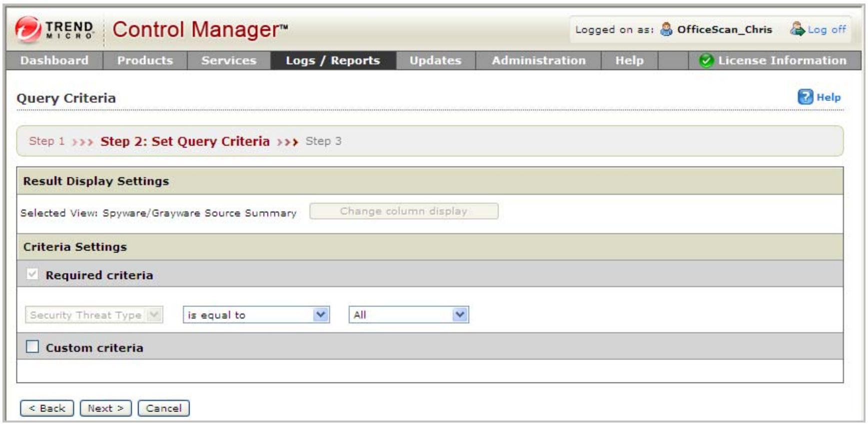
1. Click **Edit** on the Top 25 Spyware/Grayware Sources bar chart. The Edit Bar Chart screen appears.


TREND MICRO
Control Manager™
Logged on as: OfficeScan_Chris
Log off
Dashboard
Products
Services
Logs / Reports
Updates
Administration
Help
License Information
Edit Bar Chart
Help
› Step 1 : Data View ››› Step 2 ››› Step 3
Data Views
Select the data view:
Product Information
Security Threat Information
Virus/Malware Information
Spyware/Grayware Information
Summary Information
○ Overall Spyware/Grayware Summary
● Spyware/Grayware Source Summary
○ Endpoint Spyware/Grayware Summary
○ Spyware/Grayware Detection Over Time Summary
○ Spyware/Grayware Action/Result Summary
Detailed Information
Next >
Cancel

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 ››› Step 2: Set Query Criteria ››› Step 3

Result Display Settings

Selected View: Spyware/Grayware Source Summary

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | All

□ Custom criteria

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.

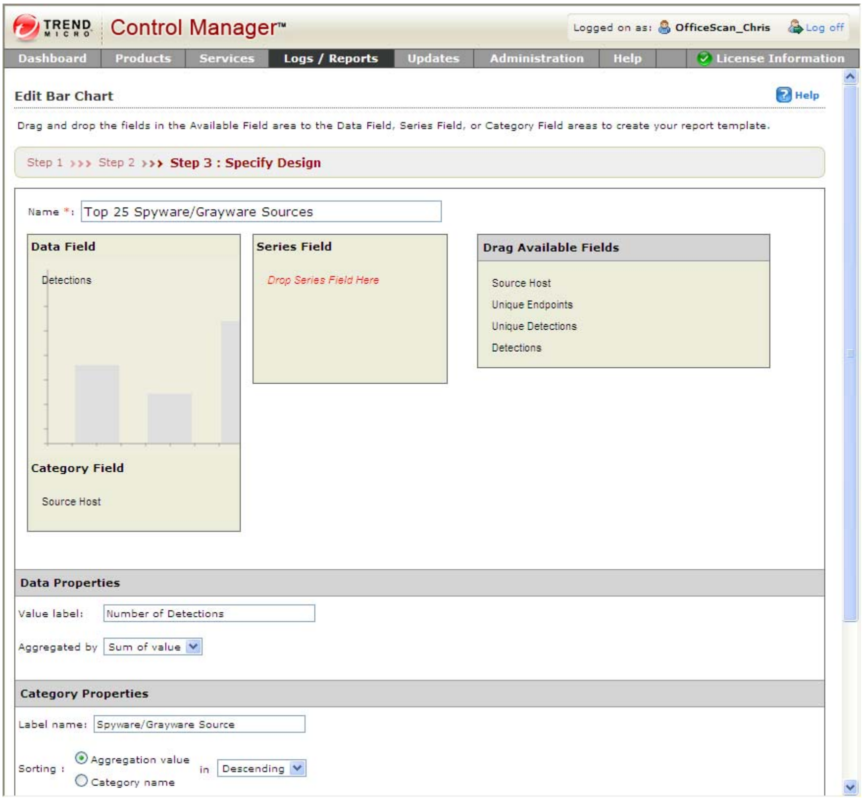
Chris does not want cookies to appear in his bar chart for spyware/grayware.

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

   Security Threat 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.



Edit Bar Chart

Help

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *: Top 25 Spyware/Grayware Sources

Data Field

Detections

Category Field

Source Host

Series Field

Drop Series Field Here

Drag Available Fields

Source Host
Unique Endpoints
Unique Detections
Detections

Data Properties

Value label: Number of Detections

Aggregated by Sum of value

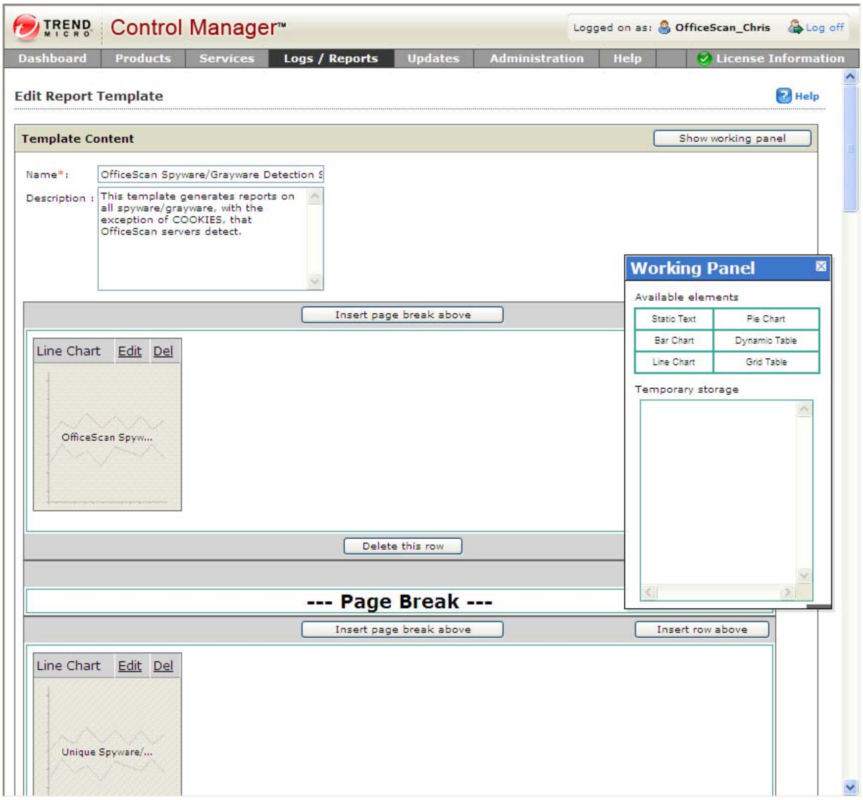
Category Properties

Label name: Spyware/Grayware Source

Sorting : ● Aggregation value ○ Category name in Descending

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

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



Edit Report Template

Template Content

Name*: OfficeScan Spyware/Grayware Detection S

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

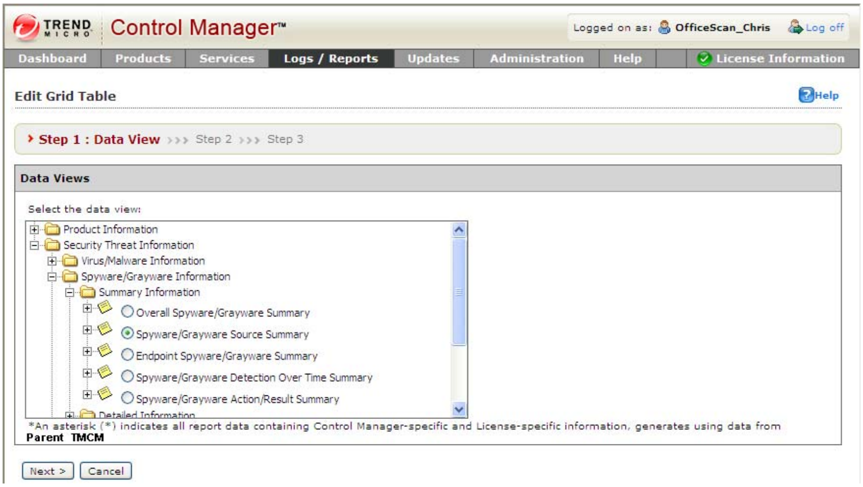
OfficeScan Spyw...

Unique Spyware/...

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.



Edit Grid Table

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

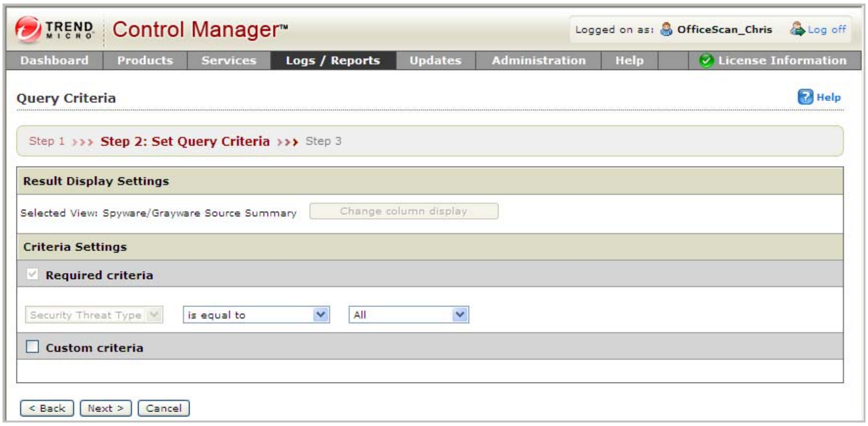
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ● Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 >>> Step 2: Set Query Criteria >>> Step 3

Result Display Settings

Selected View: Spyware/Grayware Source Summary

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | All

□ Custom criteria

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.

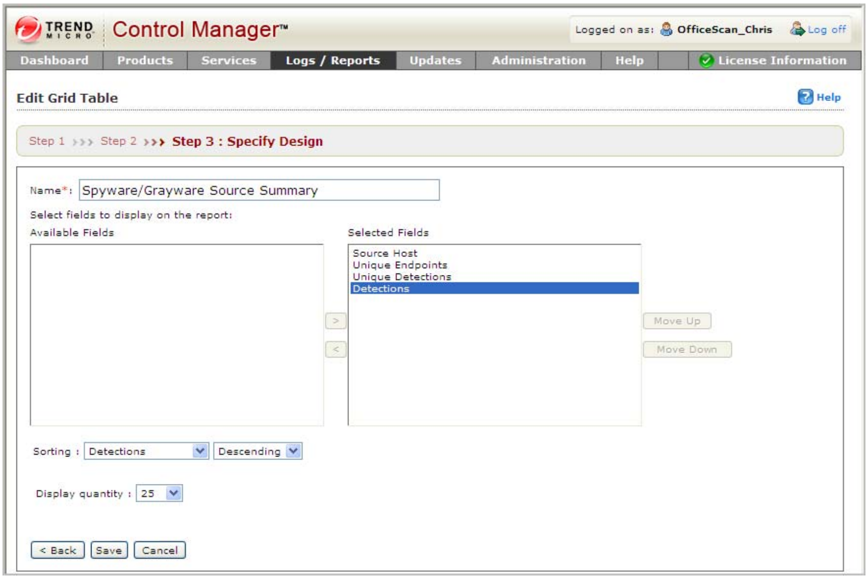
Chris does not want cookies to appear in his grid table for spyware/grayware.

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

Security Threat 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.



Edit Grid Table

Step 1 ››› Step 2 ››› Step 3 : Specify Design

Name*: Spyware/Grayware Source Summary

Select fields to display on the report:

Available Fields

Selected Fields

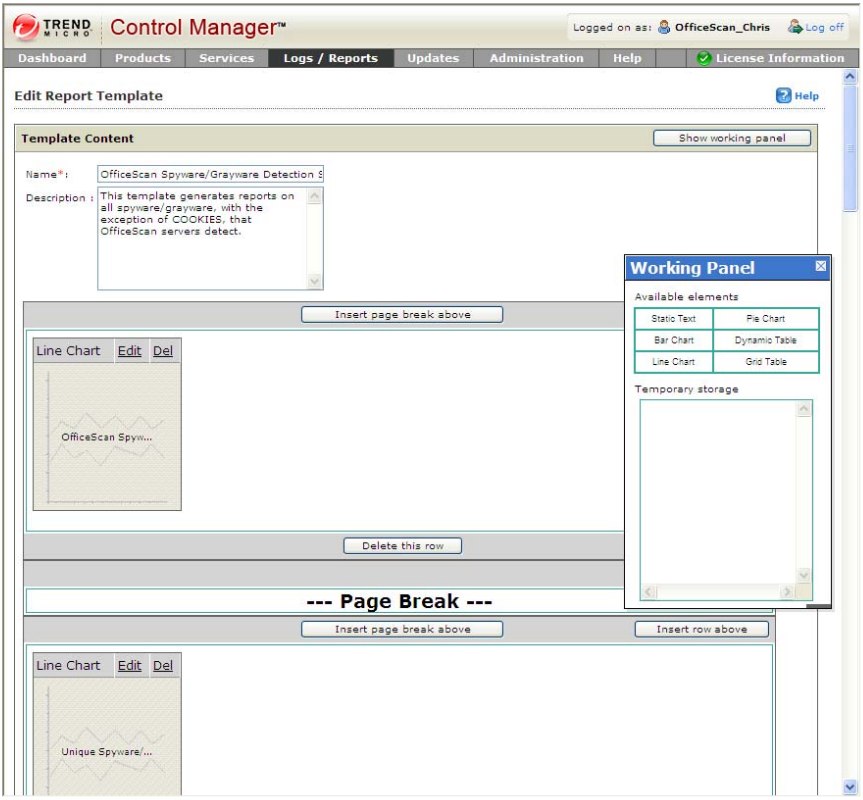
Source Host
Unique Endpoints
Unique Detections
Detections

Sorting : Detections | Descending

Display quantity : 25

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

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



Edit Report Template

Template Content

Name*: OfficeScan Spyware/Grayware Detection S

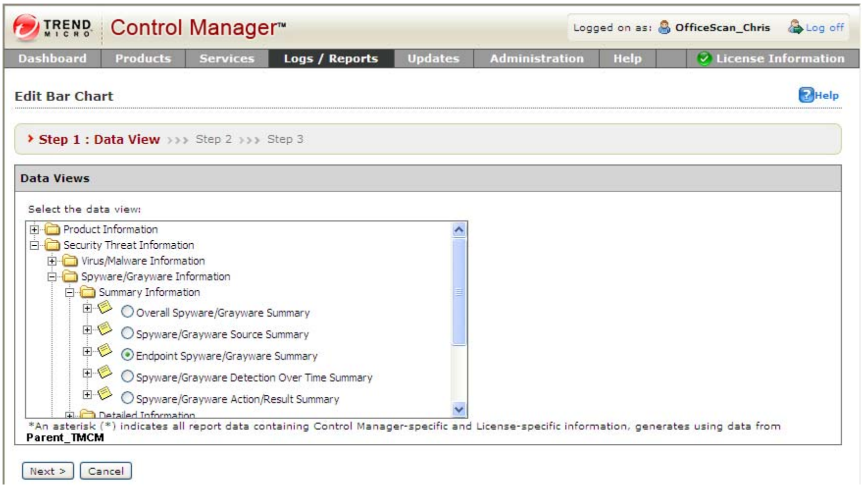
Description : This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.

--- Page Break ---

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.



Edit Bar Chart

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

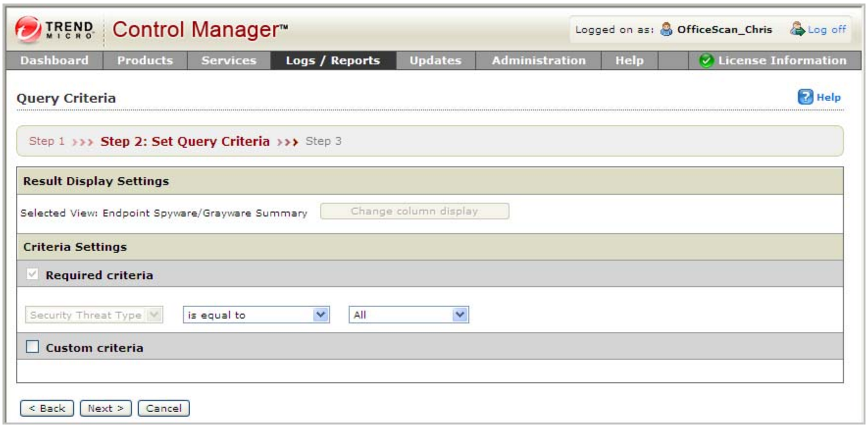
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ● Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Selected View: Endpoint Spyware/Grayware Summary

☑ Required criteria

Security Threat Type | is equal to | All

□ Custom criteria

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.

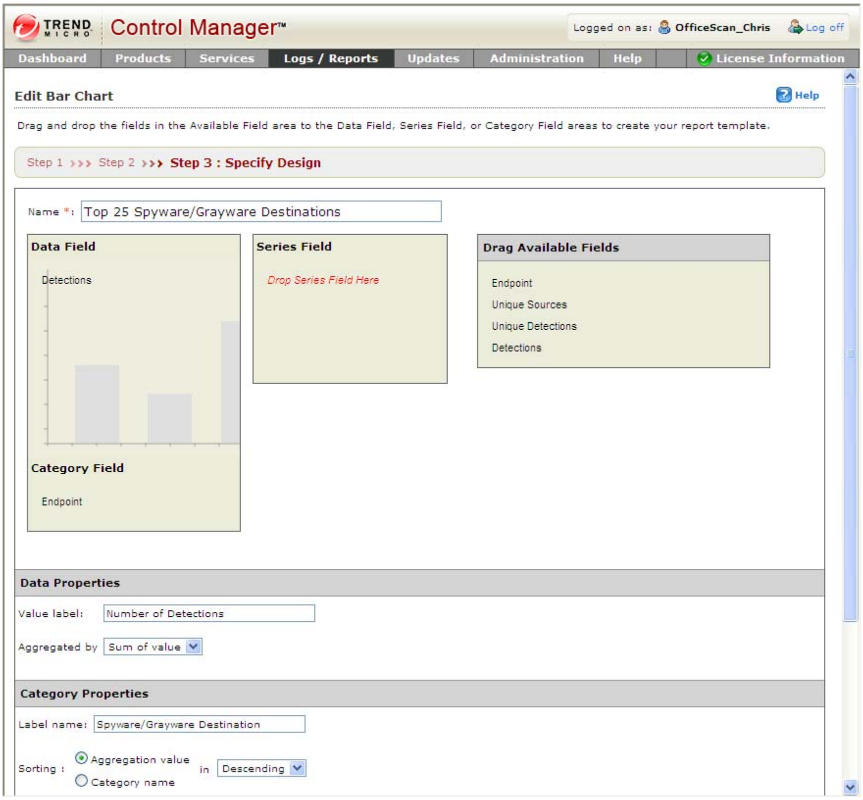
Chris does not want cookies to appear in his bar chart for spyware/grayware.

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

   Security Threat 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.



Edit Bar Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *: Top 25 Spyware/Grayware Destinations

Data Field: Detections

Series Field: Drop Series Field Here

Drag Available Fields: Endpoint, Unique Sources, Unique Detections, Detections

Category Field: Endpoint

Data Properties

Value label: Number of Detections

Aggregated by: Sum of value

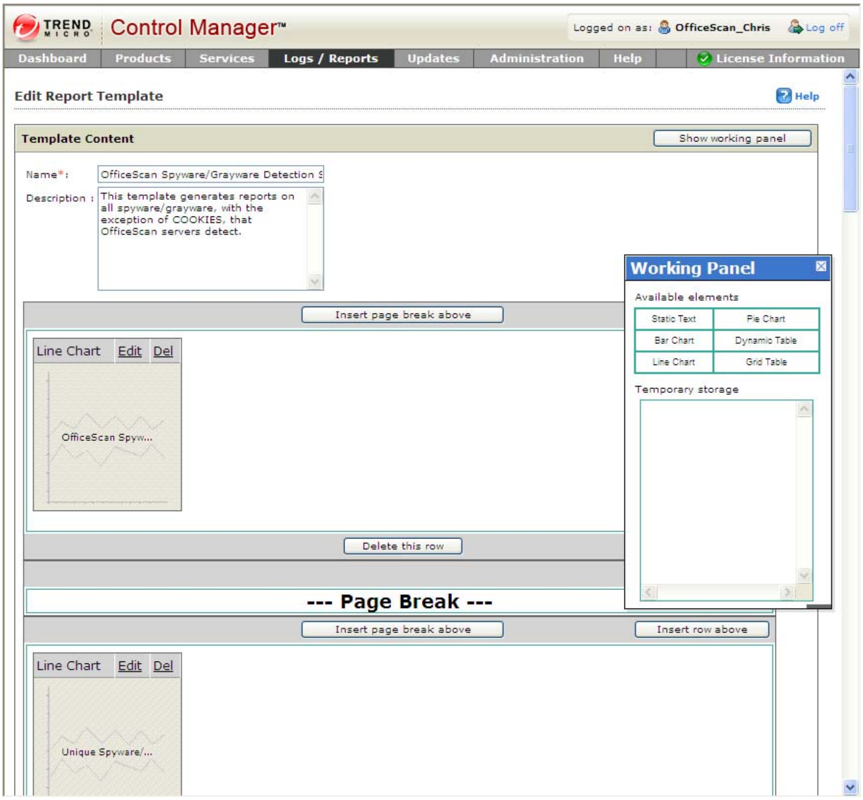
Category Properties

Label name: Spyware/Grayware Destination

Sorting: ● Aggregation value ○ Category name in Descending

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

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



Edit Report Template

Template Content

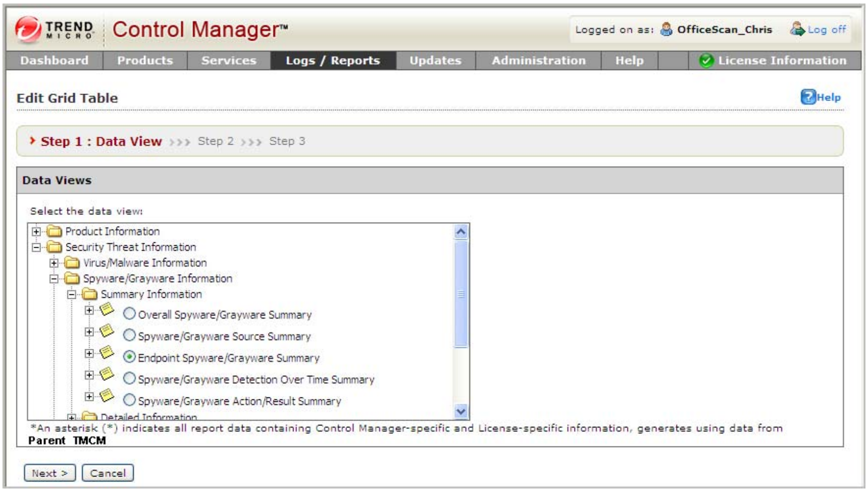
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Destination Summary grid table:

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



Edit Grid Table

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

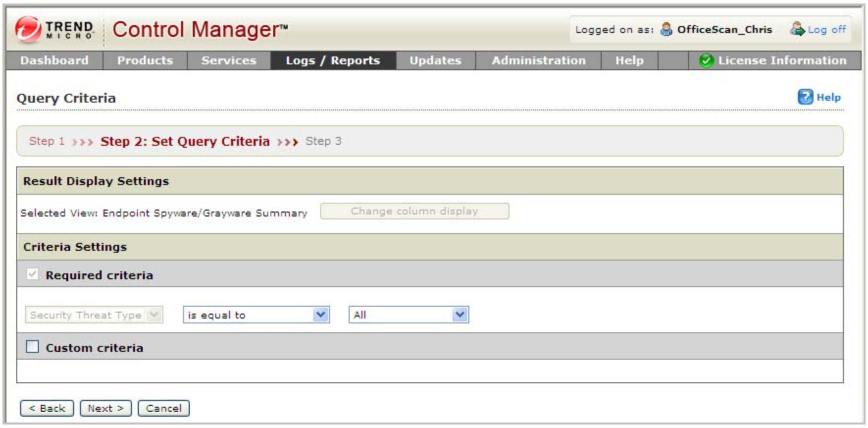
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ● Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ○ Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

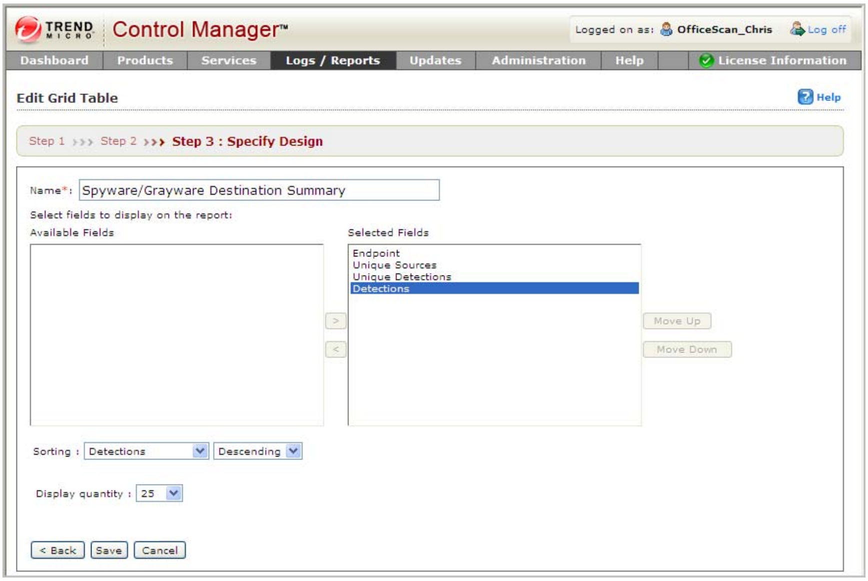
Chris does not want cookies to appear in his grid table for spyware/grayware.

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

   Security Threat 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.



Edit Grid Table

Name*: Spyware/Grayware Destination Summary

Select fields to display on the report:

Available Fields

Selected Fields

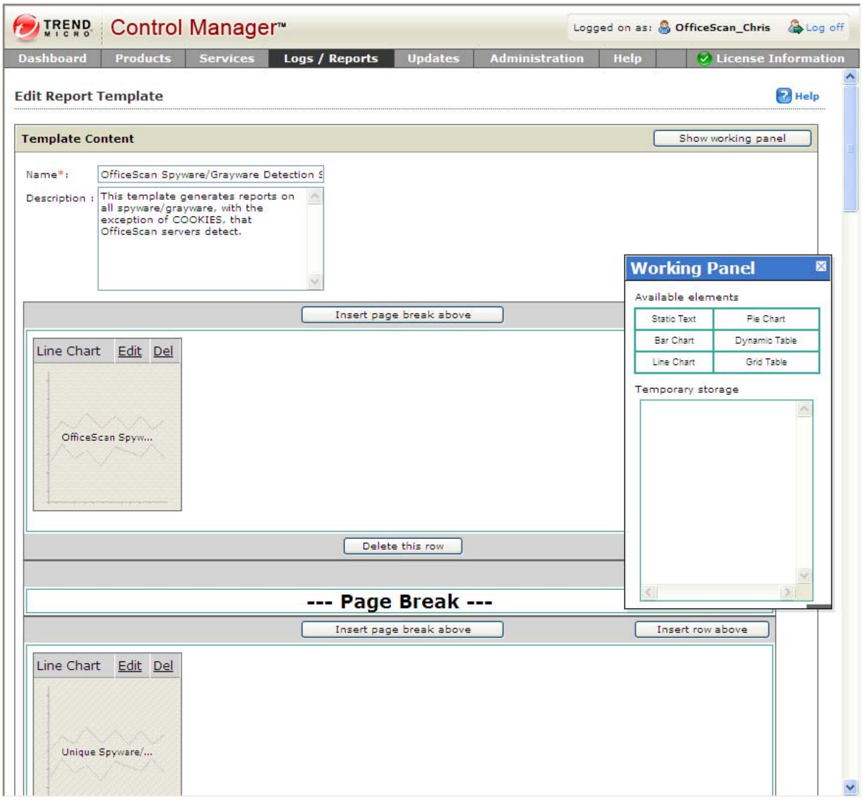
Endpoint
Unique Sources
Unique Detections
Detections

Sorting : Detections | Descending

Display quantity : 25

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

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



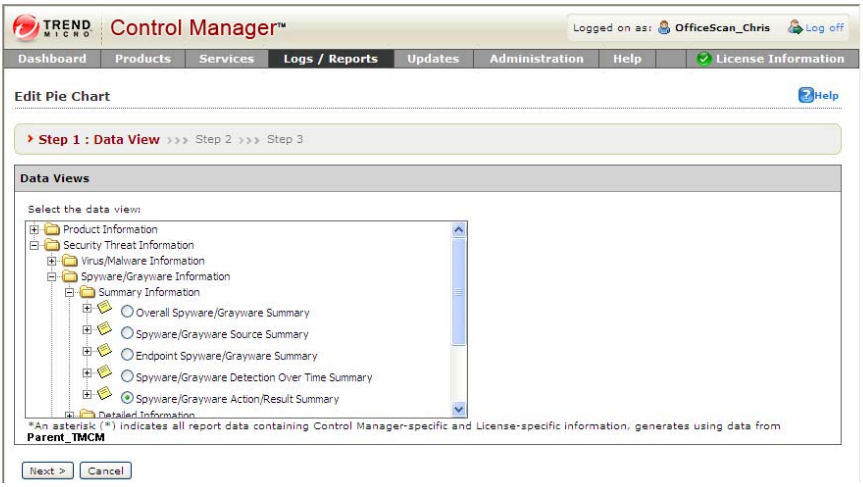
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Action Result Summary pie chart:

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



Edit Pie Chart

Step 1 : Data View >>> Step 2 >>> Step 3

Data Views

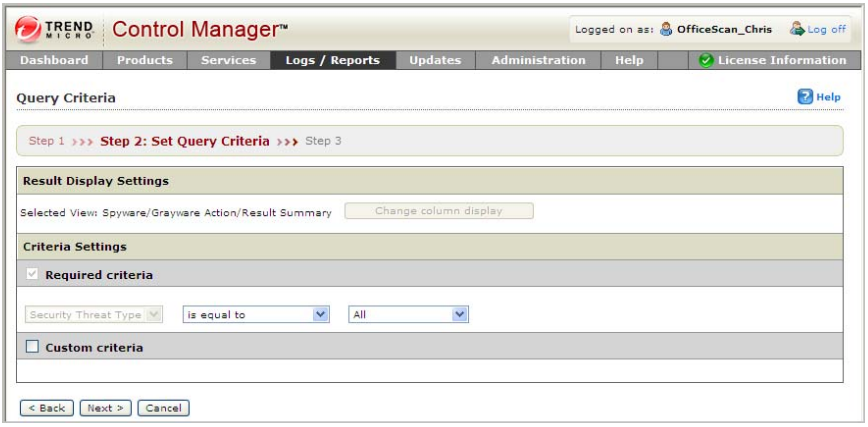
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ● Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

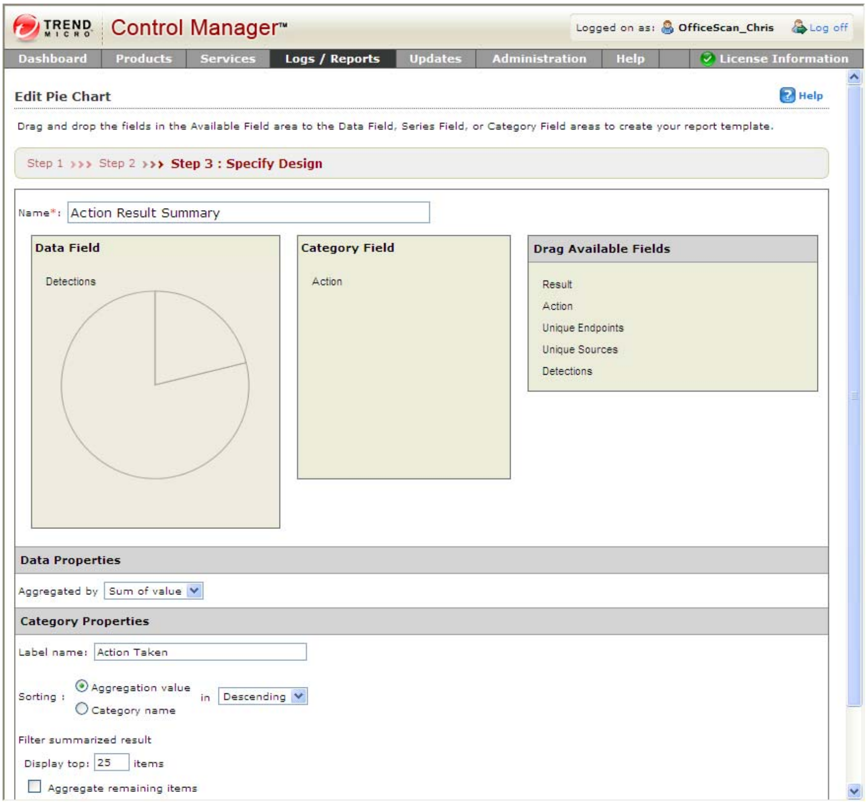
Chris does not want cookies to appear in his pie chart for spyware/grayware.

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

   Security Threat 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.



Edit Pie Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› **Step 3 : Specify Design**

Name*: Action Result Summary

Data Field: Detections

Category Field: Action

Data Properties

Aggregated by: Sum of value

Category Properties

Label name: Action Taken

Sorting : ● Aggregation value ○ Category name in Descending

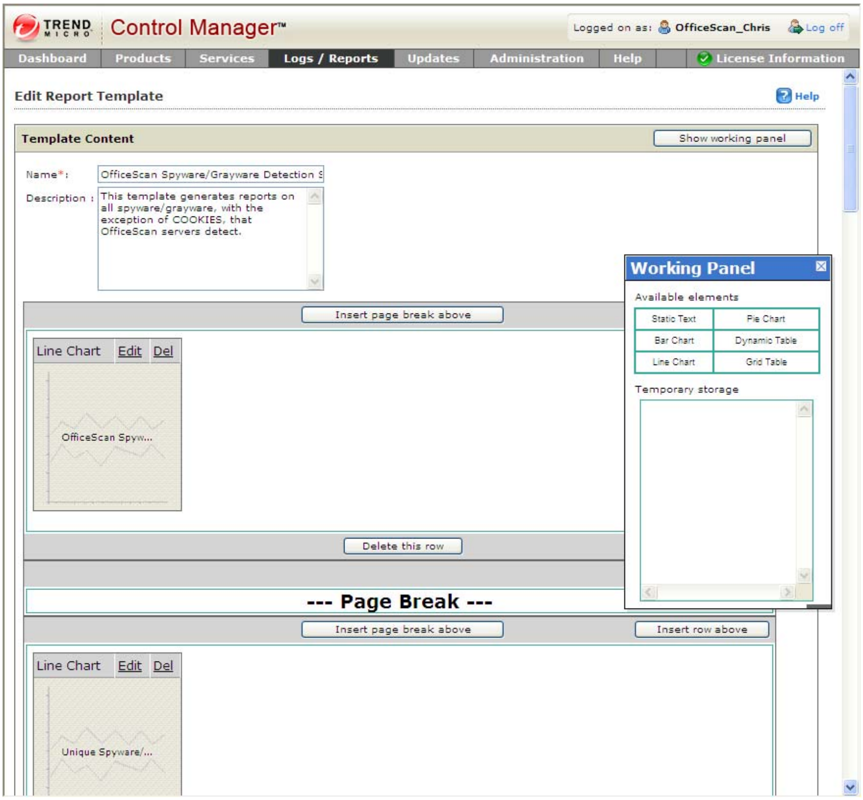
Filter summarized result

Display top: 25 items

□ Aggregate remaining items

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

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



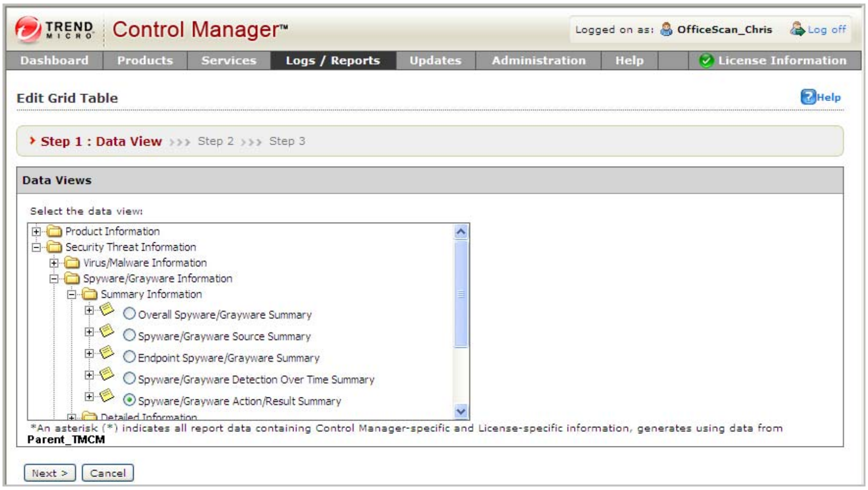
Name*: OfficeScan Spyware/Grayware Detection S

Description : 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 Action/Result Summary grid table:

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



Edit Grid Table

› Step 1 : Data View ››› Step 2 ››› Step 3

Data Views

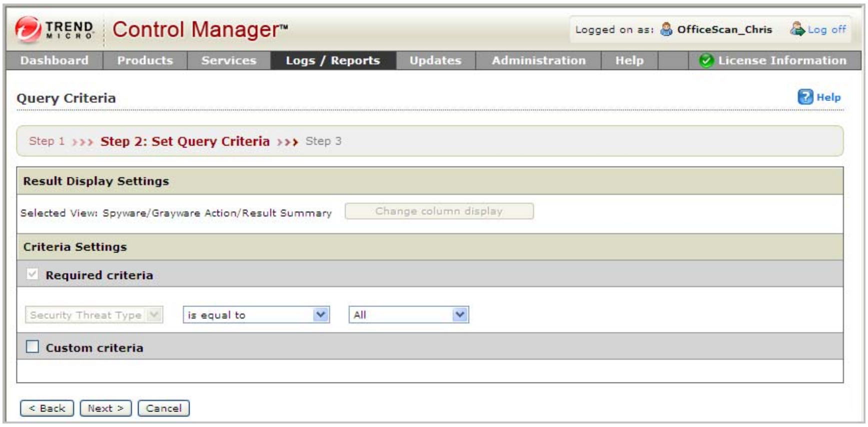
Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
      - ○ Overall Spyware/Grayware Summary
      - ○ Spyware/Grayware Source Summary
      - ○ Endpoint Spyware/Grayware Summary
      - ○ Spyware/Grayware Detection Over Time Summary
      - ● Spyware/Grayware Action/Result Summary
    - Detailed Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

2. Click **Next**. The Query Criteria > Step 2: Set 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.

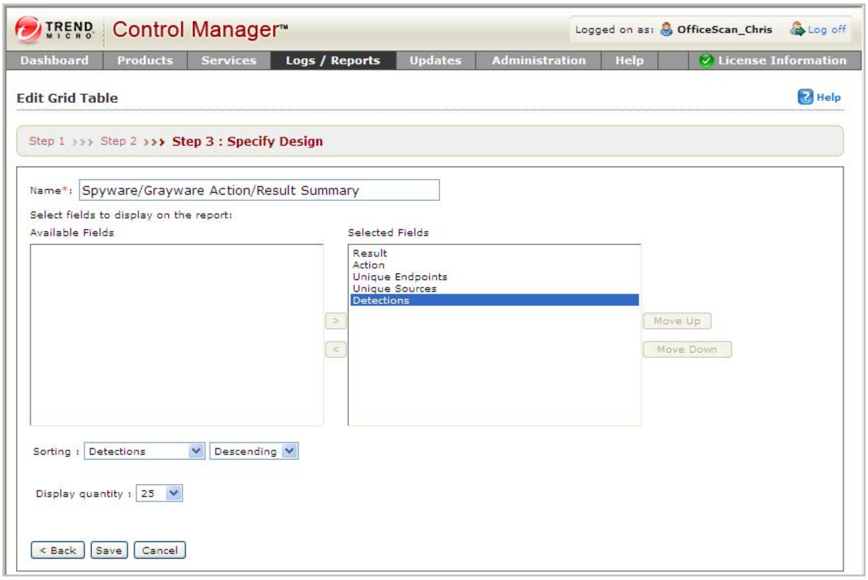
Chris does not want cookies to appear in his grid table for spyware/grayware.

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

   Security Threat 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.



Name*: Spyware/Grayware Action/Result Summary

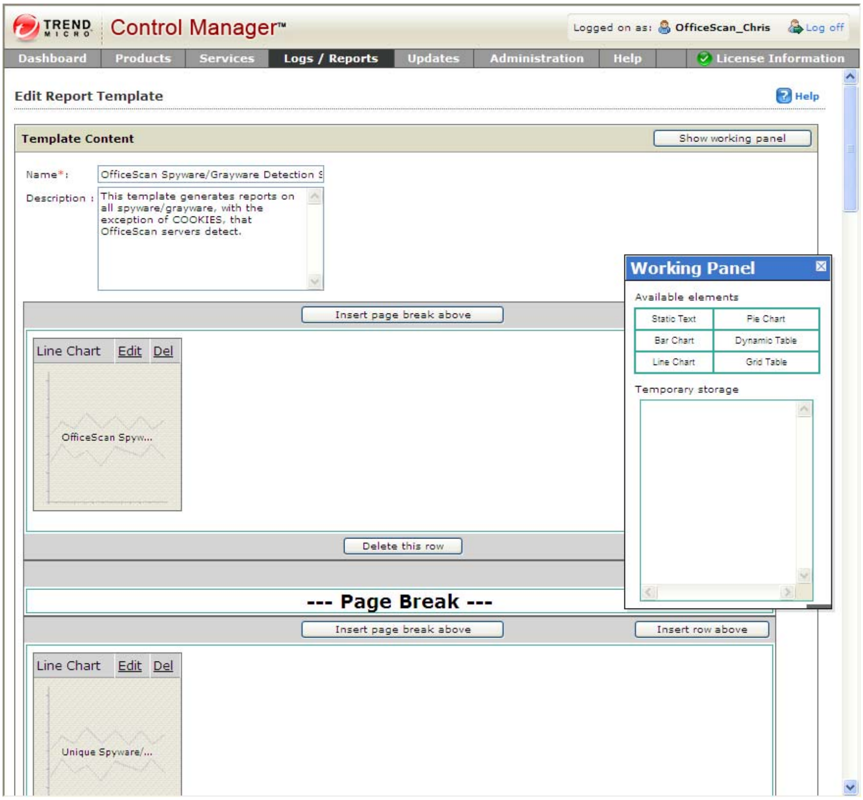
Selected Fields: Result, Action, Unique Endpoints, Unique Sources, Detections

Sorting : Detections Descending

Display quantity : 25

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

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



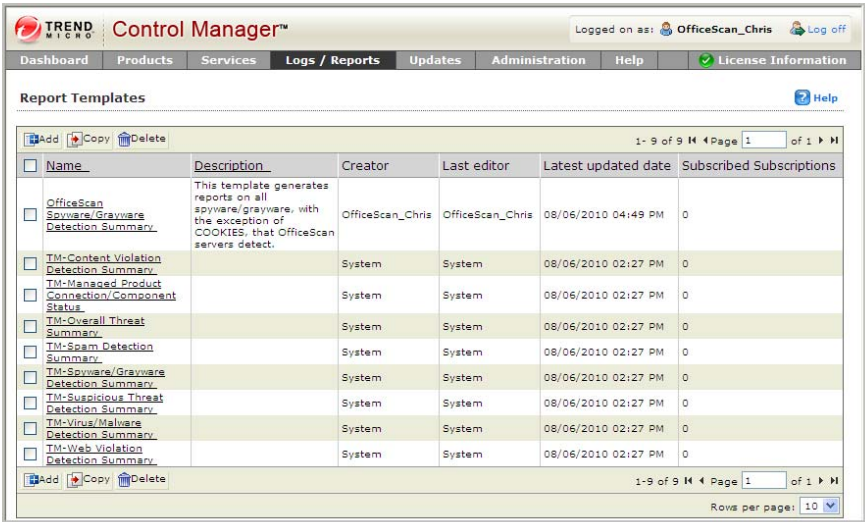
Edit Report Template

Template Content

Name*: OfficeScan Spyware/Grayware Detection S

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

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



Report Templates

☐	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
☐	OfficeScan Spyware/Grayware Detection Summary	This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.	OfficeScan_Chris	OfficeScan_Chris	08/06/2010 04:49 PM	0
☐	TM-Content Violation Detection Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Managed Product Connection/Component Status		System	System	08/06/2010 02:27 PM	0
☐	TM-Overall Threat Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Spam Detection Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Spyware/Grayware Detection Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Suspicious Threat Detection Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Virus/Malware Detection Summary		System	System	08/06/2010 02:27 PM	0
☐	TM-Web Violation Detection Summary		System	System	08/06/2010 02:27 PM	0

Rows per page: 10

Viewing a Generated Report Using the Template

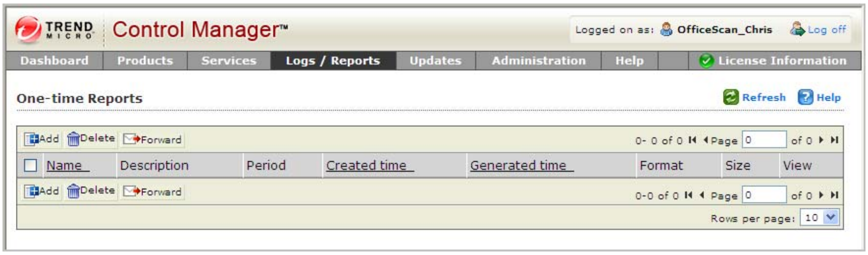
After modifying the template, Chris wants to see how the report would look. To quickly view a report using this template Chris needs to create a one-time report. Chris would also like to gather feedback from other OfficeScan administrators and his boss on the layout of the report. He will email the report,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

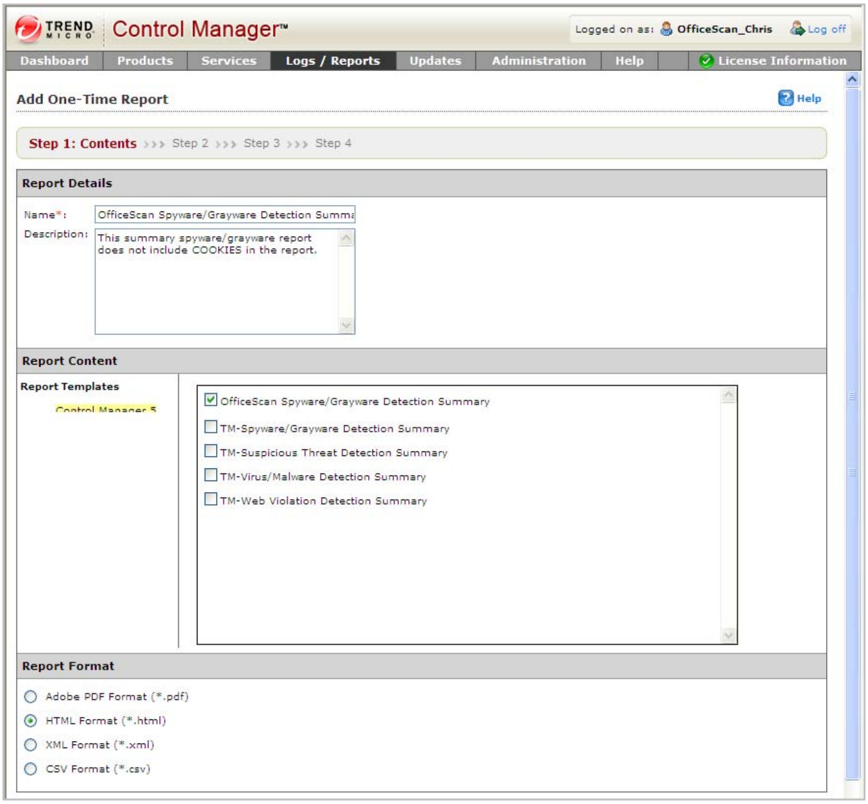
1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.

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



□	Name	Description	Period	Created time	Generated time	Format	Size	View

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



Add One-Time Report

Report Details

Name*: OfficeScan Spyware/Grayware Detection Summa

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

Report Content

Report Templates

Control Manager 5

☑ OfficeScan Spyware/Grayware Detection Summary

□ TM-Spyware/Grayware Detection Summary

□ TM-Suspicious Threat Detection Summary

□ TM-Virus/Malware Detection Summary

□ TM-Web Violation Detection Summary

Report Format

○ Adobe PDF Format (*.pdf)

● HTML Format (*.html)

○ XML Format (*.xml)

○ CSV Format (*.csv)

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

   OfficeScan Spyware-Grayware Detection Summary

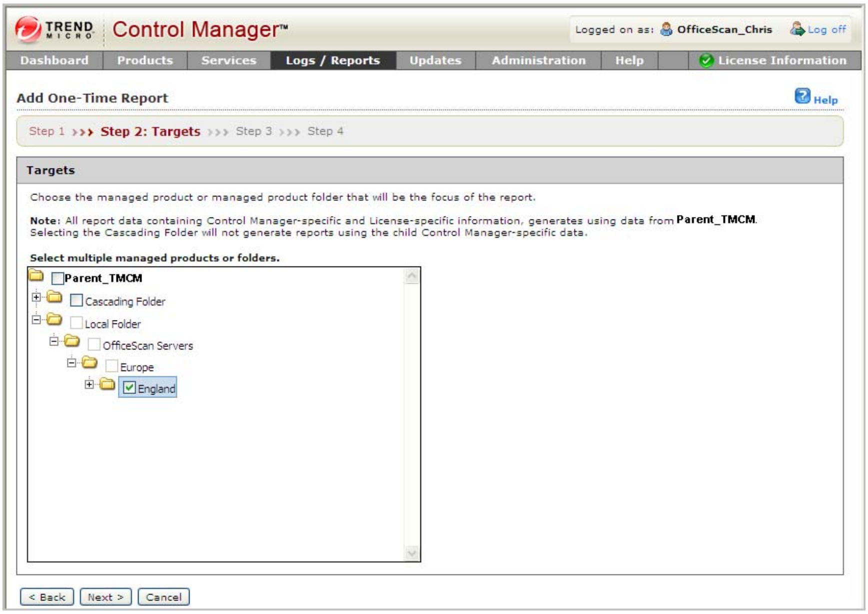
6. Type the following in the **Description** field, under Report Details:

   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.



Add One-Time Report

Step 1 >>> **Step 2: Targets** >>> Step 3 >>> Step 4

Targets

Choose the managed product or managed product folder that will be the focus of the report.

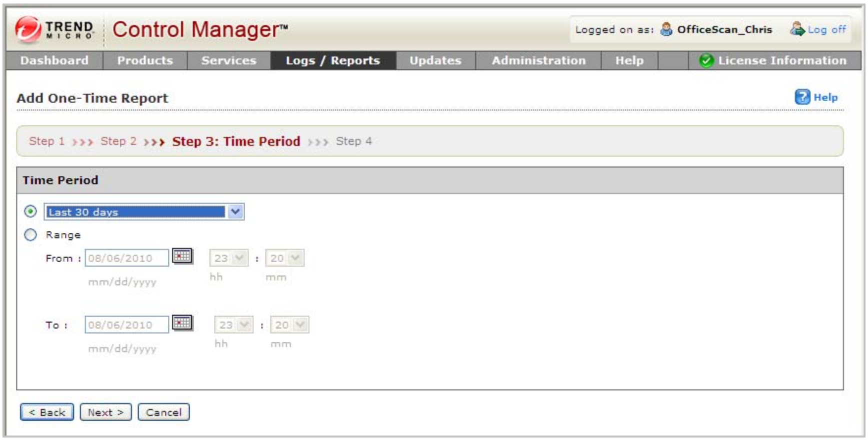
Note: All report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.

Select multiple managed products or folders.

- □ **Parent_TMCM**
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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.



Add One-Time Report

Time Period

● Last 30 days

○ Range

From : 08/06/2010 (mm/dd/yyyy) 23 : 20 (hh mm)

To : 08/06/2010 (mm/dd/yyyy) 23 : 20 (hh mm)

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.

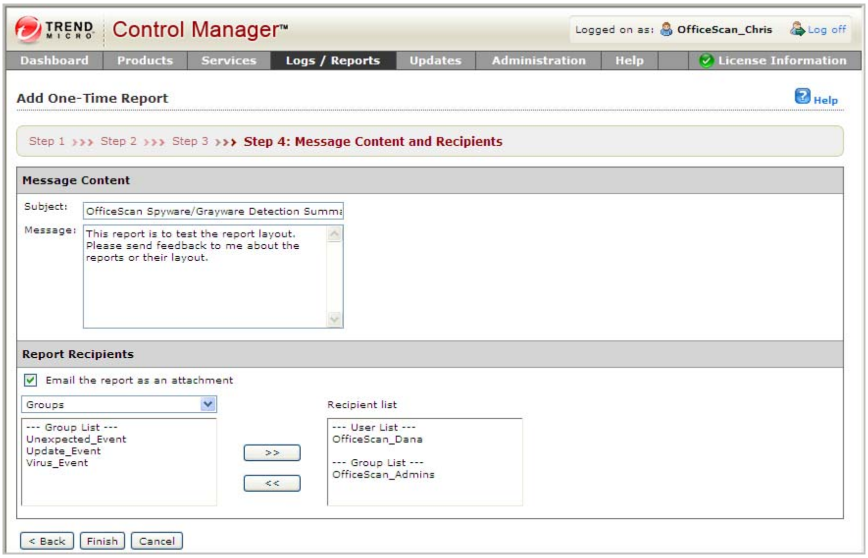
   b. Specify a time in the accompanying **hh** and **mm** fields.

   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.



Add One-Time Report

Step 1 >>> Step 2 >>> Step 3 >>> Step 4: Message Content and Recipients

Message Content

Subject: OfficeScan Spyware/Grayware Detection Summa

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

Report Recipients

☑ Email the report as an attachment

--- Group List ---
Unexpected_Event
Update_Event
Virus_Event

Recipient list

--- User List ---
OfficeScan_Dana

--- Group List ---
OfficeScan_Admins

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

1. Type the following in the **Subject** 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:

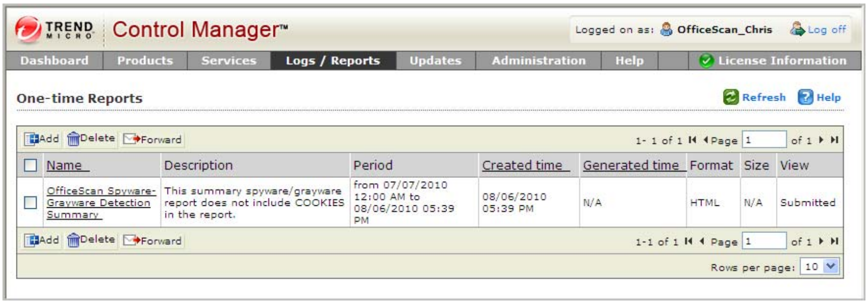
   Users:

   - **OfficeScan_Dana**

Groups:

- **OfficeScan_Admins**

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

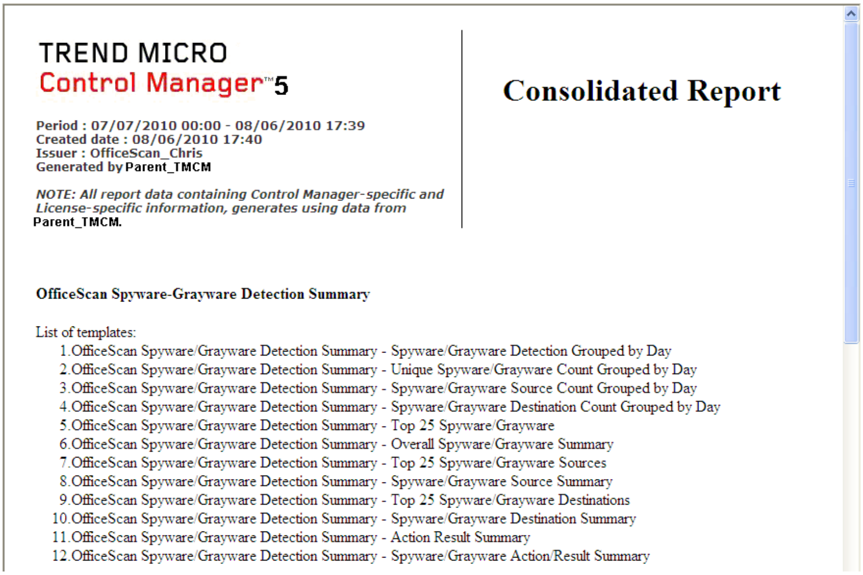


One-time Reports

□	Name	Description	Period	Created time	Generated time	Format	Size	View
□	OfficeScan Spyware-Grayware Detection Summary	This summary spyware/grayware report does not include COOKIES in the report.	from 07/07/2010 12:00 AM to 08/06/2010 05:39 PM	08/06/2010 05:39 PM	N/A	HTML	N/A	Submitted

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

Period : 07/07/2010 00:00 - 08/06/2010 17:39
Created date : 08/06/2010 17:40
Issuer : OfficeScan_Chris
Generated by Parent_TMCM

NOTE: All report data containing Control Manager-specific and License-specific information, generates using data from Parent_TMCM.

Consolidated Report

OfficeScan Spyware-Grayware Detection Summary

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

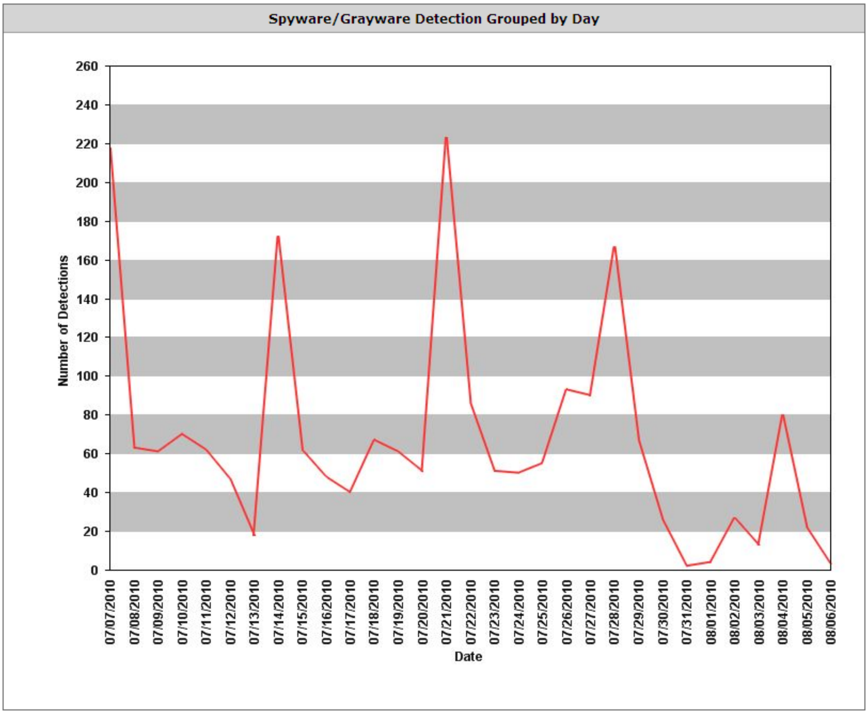
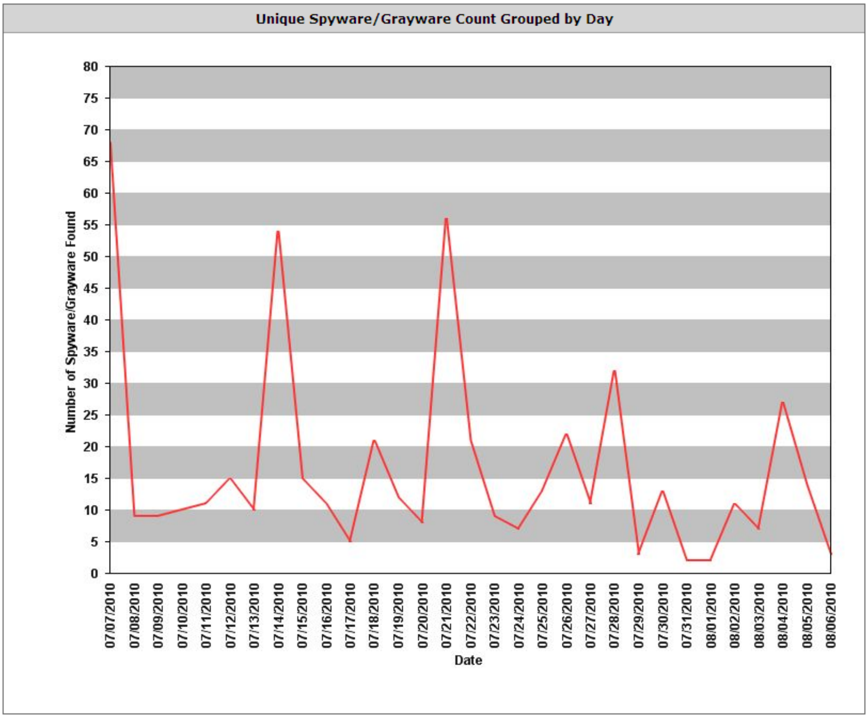
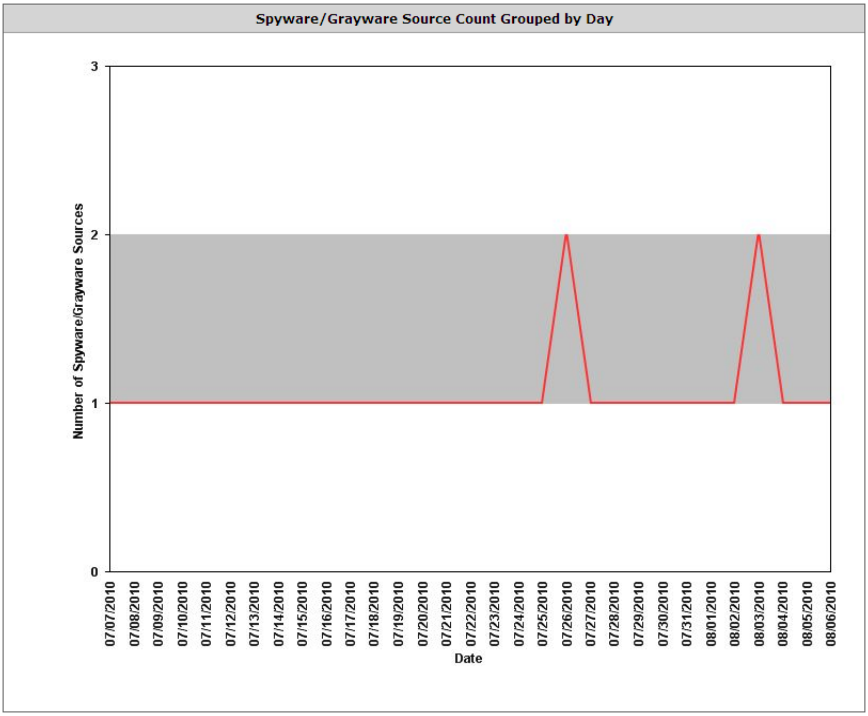
<table>
<tr><td colspan="2">
</td></tr>
<tr><td>Data view:
• Spyware/Grayware Detection Over Time Summary
Query Criteria:
• Security Threat Type > is equal to > Non-cookie types</td><td>Data Properties:
• Detections
• Value label: Number of Detections
• Aggregated by: Sum of Value
Category Properties:
• Summary Time
• Label name: Date
• Group by: Day</td></tr>
</table>

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



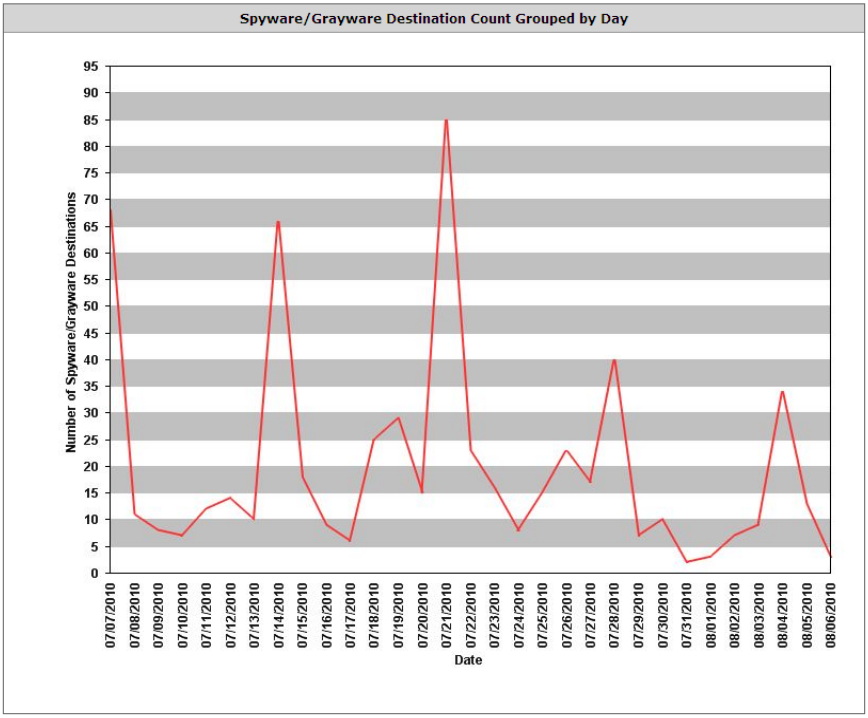
Data view: • **Spyware/Grayware Detection Over Time Summary** Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Data Properties: • Unique Detections • Value label: Number of Spyware/Grayware Found • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date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

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



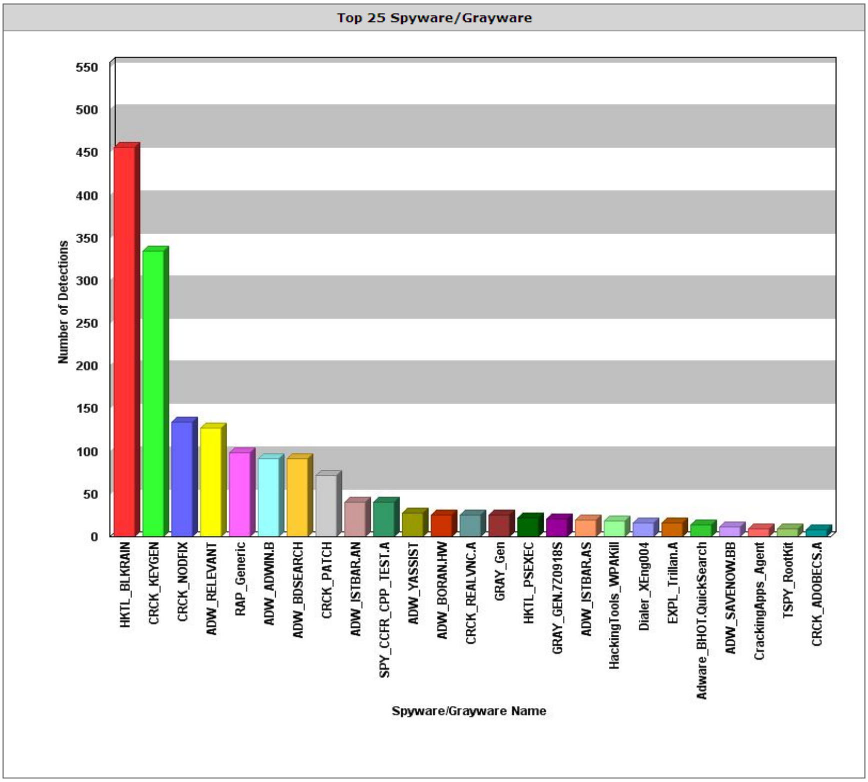
Data view: • Spyware/Grayware Detection Over Time Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Data Properties: • Unique Sources • Value label: Number of Spyware/Grayware Sources • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: Date •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

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



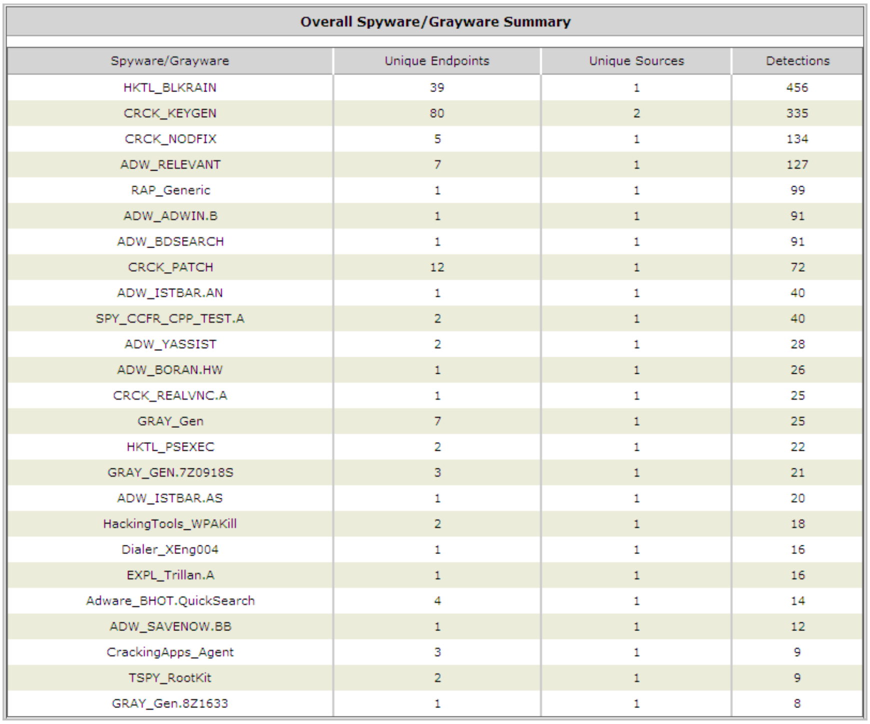
Data view:	Data Properties:
• Spyware/Grayware Detection Over Time Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	• Unique Endpoints • Value label: Number of Spyware/Grayware Destinations • Aggregated by: Sum of Value Category Properties: • Summary Time • Label name: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

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



Data view: • Overall Spyware/Grayware Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Data Properties: • Detections • Value label: Number of Detections • Aggregated by: Sum of Value Category Properties: • Spyware/Grayware • 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	Unique Endpoints	Unique Sources	Detections
HKTL_BLKRAIN	39	1	456
CRCK_KEYGEN	80	2	335
CRCK_NODFIX	5	1	134
ADW_RELEVANT	7	1	127
RAP_Generic	1	1	99
ADW_ADWIN.B	1	1	91
ADW_BDSEARCH	1	1	91
CRCK_PATCH	12	1	72
ADW_ISTBAR.AN	1	1	40
SPY_CCFR_CPP_TEST.A	2	1	40
ADW_YASSIST	2	1	28
ADW_BORAN.HW	1	1	26
CRCK_REALVNC.A	1	1	25
GRAY_Gen	7	1	25
HKTL_PSEXEC	2	1	22
GRAY_GEN.7Z0918S	3	1	21
ADW_ISTBAR.AS	1	1	20
HackingTools_WPAKill	2	1	18
Dialer_XEng004	1	1	16
EXPL_Trillan.A	1	1	16
Adware_BHOT.QuickSearch	4	1	14
ADW_SAVENOW.BB	1	1	12
CrackingApps_Agent	3	1	9
TSPY_RootKit	2	1	9
GRAY_Gen.8Z1633	1	1	8

Data view:

- Overall Spyware/Grayware Summary

Query Criteria:

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

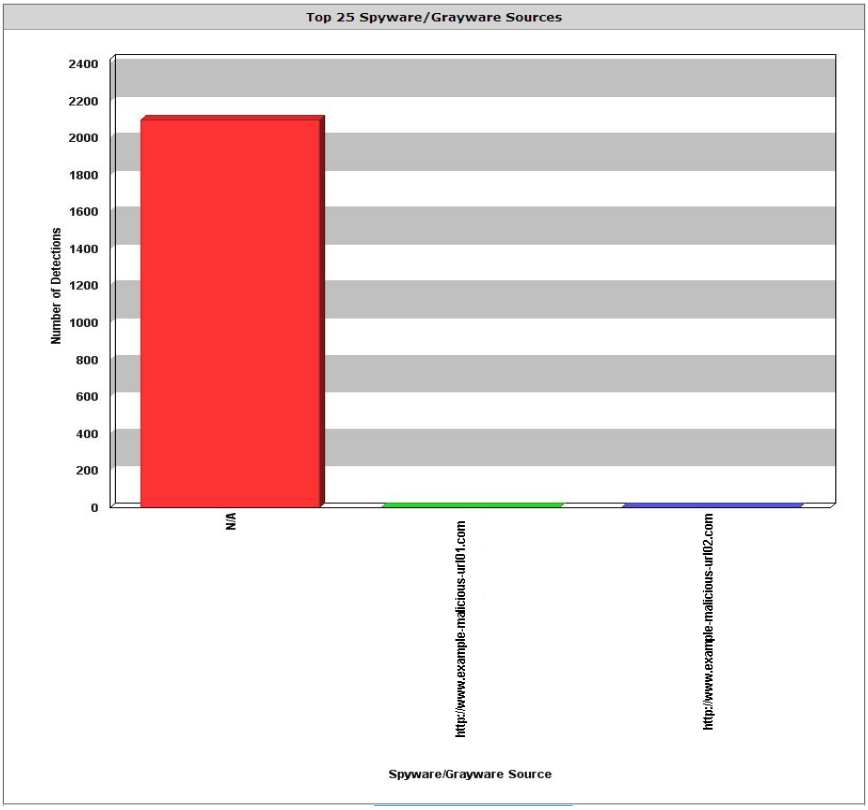
Table Columns:

- Spyware/Grayware
- Unique Endpoints
- Unique Sources
- Detections

Sorting: Detections > Descending

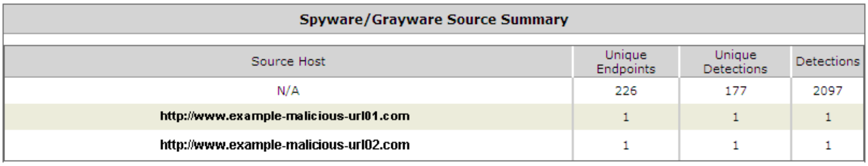
Display quantity: 25

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



Data view:	Data Properties:
- Spyware/Grayware Source Summary Query Criteria: - Security Threat Type > is equal to > Non-cookie types	- Detections - Value label: Number of Detections - Aggregated by: Sum of Value Category Properties: - Source Host - 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

Source Host	Unique Endpoints	Unique Detections	Detections
N/A	226	177	2097
http://www.example-malicious-url01.com	1	1	1
http://www.example-malicious-url02.com	1	1	1

Data view: • Spyware/Grayware Source Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Table Columns: • Source Host • Unique Endpoints • Unique Detections • Detections Sorting: Detections > Descending Display quantity: 25

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

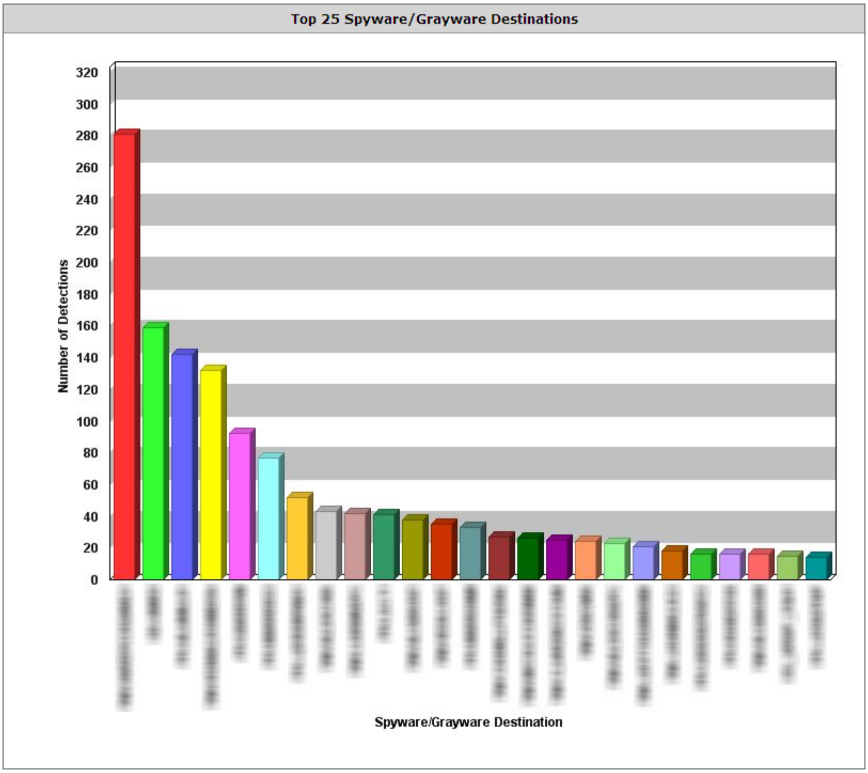
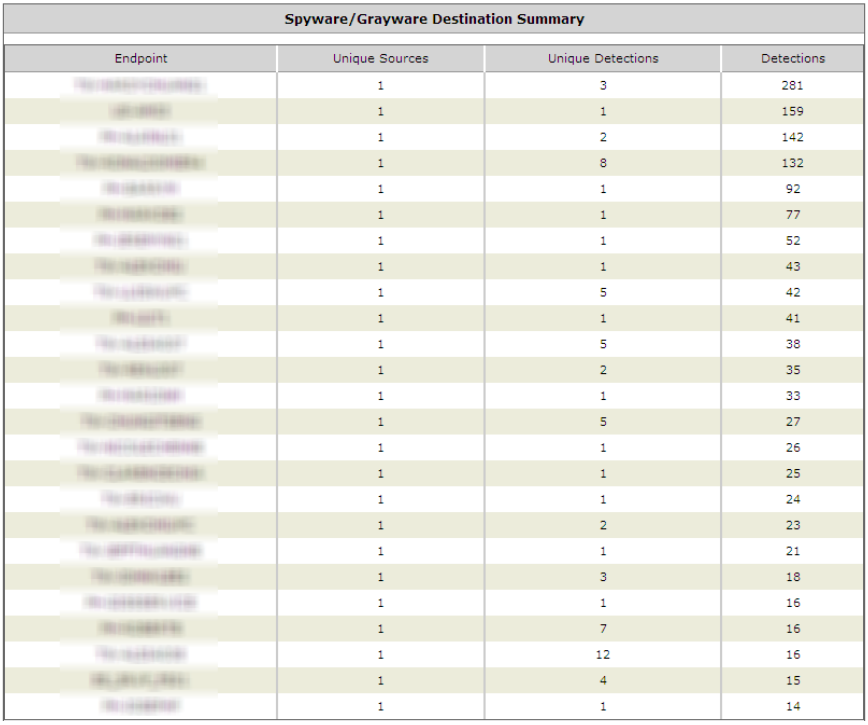
<table>
<tr><td colspan="2">
</td></tr>
<tr><td>Data view:
• Endpoint Spyware/Grayware Summary
Query Criteria:
• Security Threat Type > is equal to > Non-cookie types</td><td>Data Properties:
• Detections
• Value label: Number of Detections
• Aggregated by: Sum of Value
Category Properties:
• Endpoint
• Label name: Spyware/Grayware Destination
• Sorting: Aggregation value > Descending
• Filter summarized result: Display top 25</td></tr>
</table>

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



Spyware/Grayware Destination Summary

Endpoint	Unique Sources	Unique Detections	Detections
[redacted]	1	3	281
[redacted]	1	1	159
[redacted]	1	2	142
[redacted]	1	8	132
[redacted]	1	1	92
[redacted]	1	1	77
[redacted]	1	1	52
[redacted]	1	1	43
[redacted]	1	5	42
[redacted]	1	1	41
[redacted]	1	5	38
[redacted]	1	2	35
[redacted]	1	1	33
[redacted]	1	5	27
[redacted]	1	1	26
[redacted]	1	1	25
[redacted]	1	1	24
[redacted]	1	2	23
[redacted]	1	1	21
[redacted]	1	3	18
[redacted]	1	1	16
[redacted]	1	7	16
[redacted]	1	12	16
[redacted]	1	4	15
[redacted]	1	1	14

Data view:

- Endpoint Spyware/Grayware Summary

Query Criteria:

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

Table Columns:

- Endpoint
- Unique Sources
- Unique Detections
- Detections

Sorting: Detections > Descending

Display quantity: 25

TABLE 4-17. Action Result Summary Pie Chart

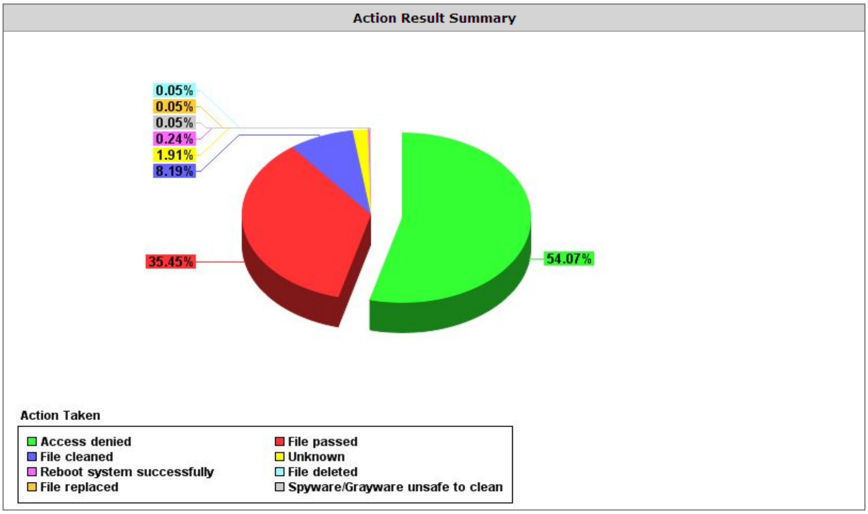
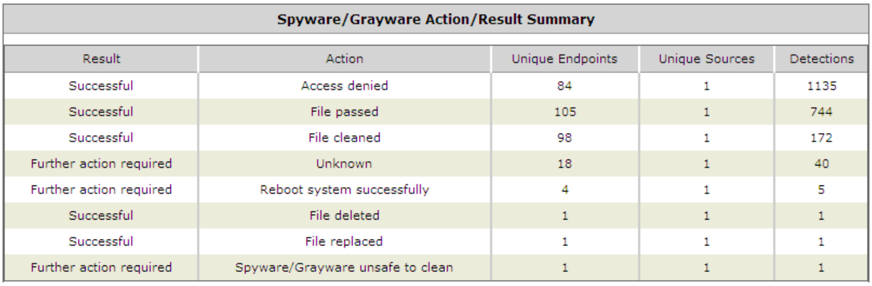
	
Data view: • Spyware/Grayware Action/Result Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Data Properties: • Detections • Aggregated by: Sum of Value Category Properties: • Action • Label name: Action Taken • Sorting: Aggregation value > Descending

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



Spyware/Grayware Action/Result Summary

Result	Action	Unique Endpoints	Unique Sources	Detections
Successful	Access denied	84	1	1135
Successful	File passed	105	1	744
Successful	File cleaned	98	1	172
Further action required	Unknown	18	1	40
Further action required	Reboot system successfully	4	1	5
Successful	File deleted	1	1	1
Successful	File replaced	1	1	1
Further action required	Spyware/Grayware unsafe to clean	1	1	1

Data View: • Spyware/Grayware Action/Result Summary Query Criteria: • Security Threat Type > is equal to > Non-cookie types	Table Columns: • Result • Action • Unique Endpoints • Unique Sources • Detections Sorting: Detections > Descending Display quantity: 25

After looking over the reports and gathering feedback from his manager and other OfficeScan administrator's, Chris decides he does not need to modify the report template.

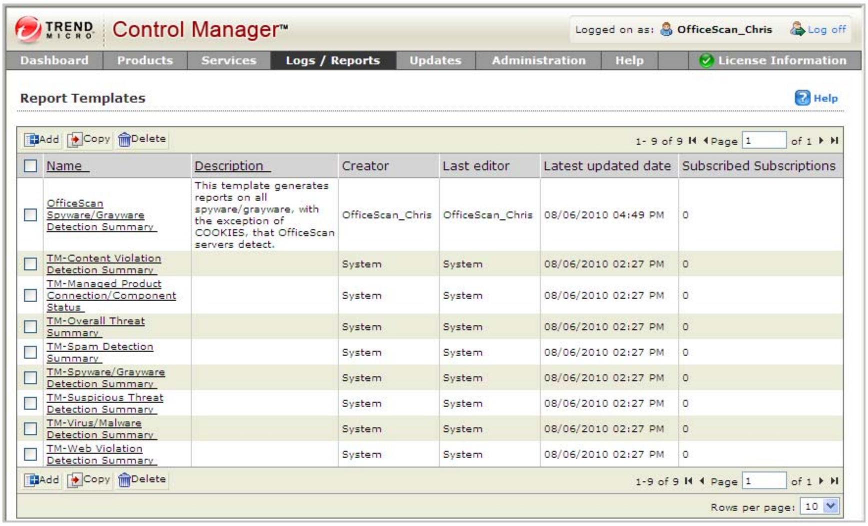
Creating a New Report Template

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.

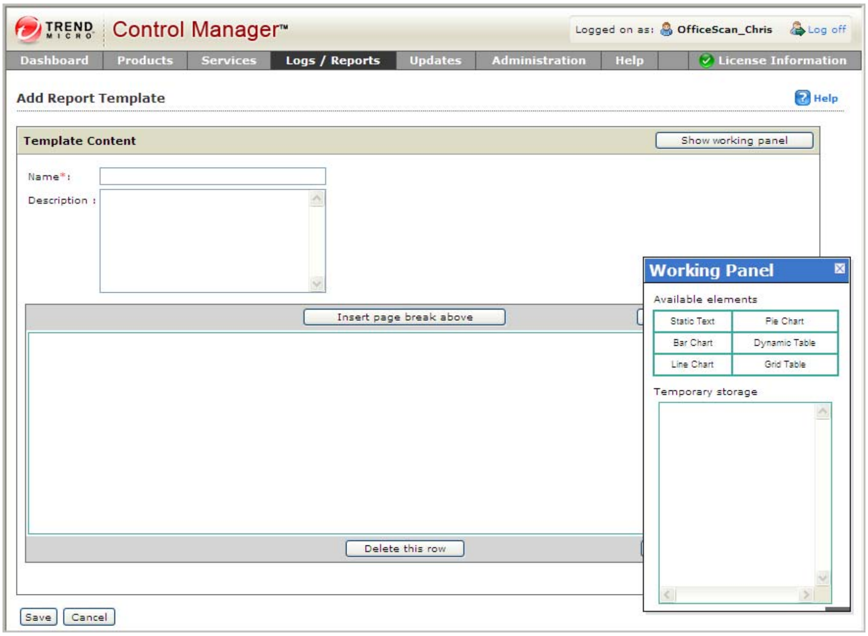
3. Click **Report Templates** from the menu. The Report Templates screen appears.



Report Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	OfficeScan Spyware/Grayware Detection Summary	This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.	OfficeScan_Chris	OfficeScan_Chris	08/06/2010 04:49 PM	0
□	TM-Content Violation Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Managed Product Connection/Component Status		System	System	08/06/2010 02:27 PM	0
□	TM-Overall Threat Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Spam Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Spyware/Grayware Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Suspicious Threat Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Virus/Malware Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Web Violation Detection Summary		System	System	08/06/2010 02:27 PM	0

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



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

   OfficeScan Endpoint Requires Further Action Report

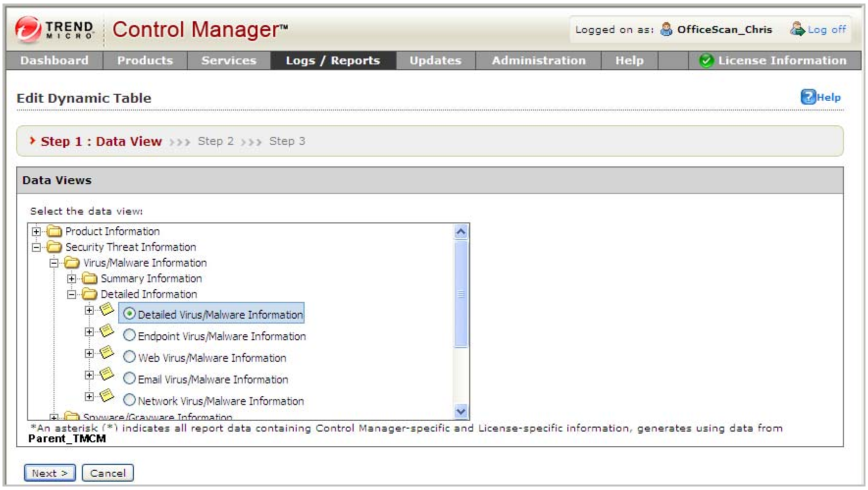
6. Type the following in the **Description** field:

   This report provides information on OfficeScan endpoints 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 > Step 1 Data View screen appears.



Edit Dynamic Table

Data Views

Select the data view:

- Product Information
- Security Threat Information
  - Virus/Malware Information
    - Summary Information
    - Detailed Information
      - ● Detailed Virus/Malware Information
      - ○ Endpoint Virus/Malware Information
      - ○ Web Virus/Malware Information
      - ○ Email Virus/Malware Information
      - ○ Network Virus/Malware Information
  - Spyware/Grayware Information

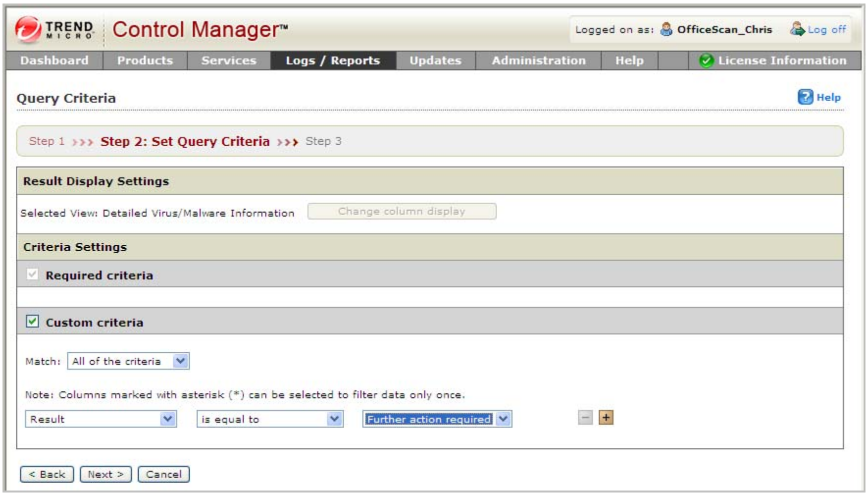
*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

3. Select **Detailed Virus/Malware Information**.

Step 2: Specify the query criteria for the template:

1. Click **Next**. The Query Criteria > Step 2 Set Query Criteria screen appears.



Selected View: Detailed Virus/Malware Information

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

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.

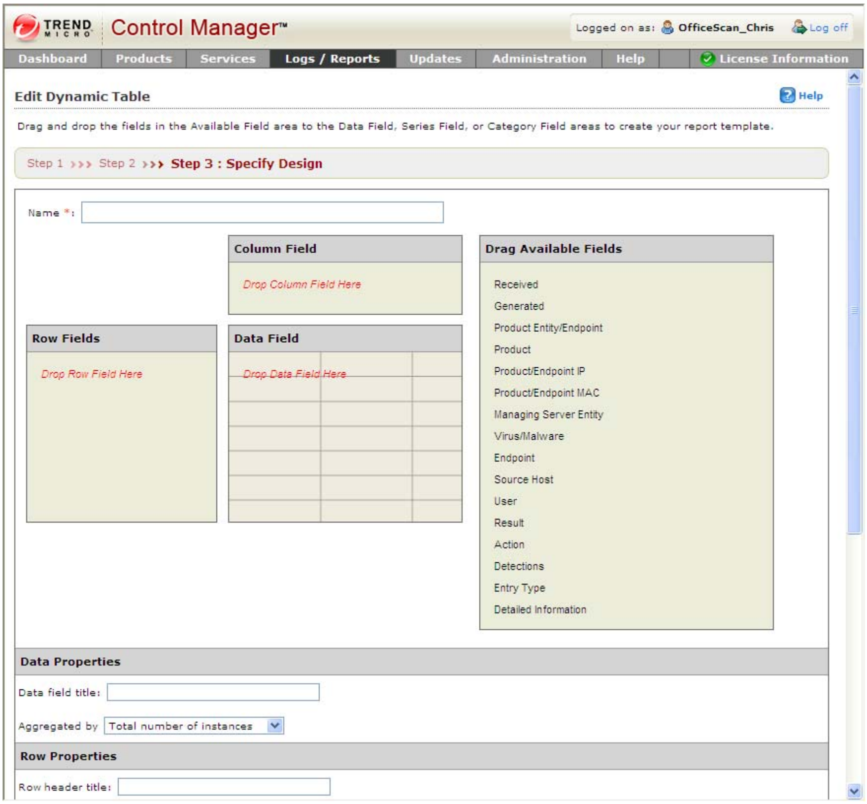
Chris only wants to see computers that require further action (OfficeScan was not able to clean, delete, or quarantine the virus).

2. Specify the following:

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

Step 3: Specify the design for the template:

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



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> **Step 3 : Specify Design**

Name *:

Column Field: Drop Column Field Here

Row Fields: Drop Row Field Here

Data Field: Drop Data Field Here

Drag Available Fields:
- Received
- Generated
- Product Entity/Endpoint
- Product
- Product/Endpoint IP
- Product/Endpoint MAC
- Managing Server Entity
- Virus/Malware
- Endpoint
- Source Host
- User
- Result
- Action
- Detections
- Entry Type
- Detailed Information

Data Properties

Data field title:

Aggregated by: Total number of instances

Row Properties

Row header title:

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.

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

   OfficeScan Endpoints Requiring Further Action: Virus/Malware

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

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

4. Drag-and-drop **Managing Server Entity** and then **Endpoint** 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.

5. Drag-and-drop **Detections** to **Drop Data Field Here.**

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

6. 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

7. Specify the display settings for the Row Properties.

   a. Type the following in the **Row header title** field:

      OfficeScan Server > Endpoint

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

      Aggregation value > Descending

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

8. Specify the display settings for the Column Properties.

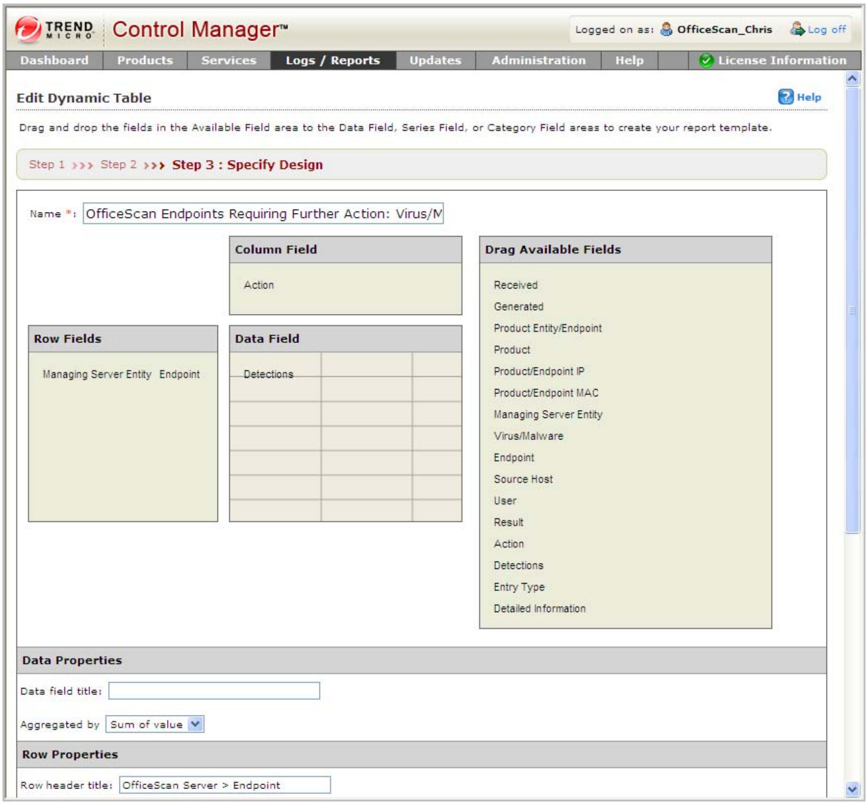
   a. Type the following in the **Column header title** field:

      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.



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› **Step 3 : Specify Design**

Name *: OfficeScan Endpoints Requiring Further Action: Virus/M

Column Field: Action

Row Fields: Managing Server Entity Endpoint

Data Field: Detections

Drag Available Fields:
- Received
- Generated
- Product Entity/Endpoint
- Product
- Product/Endpoint IP
- Product/Endpoint MAC
- Managing Server Entity
- Virus/Malware
- Endpoint
- Source Host
- User
- Result
- Action
- Detections
- Entry Type
- Detailed Information

Data Properties

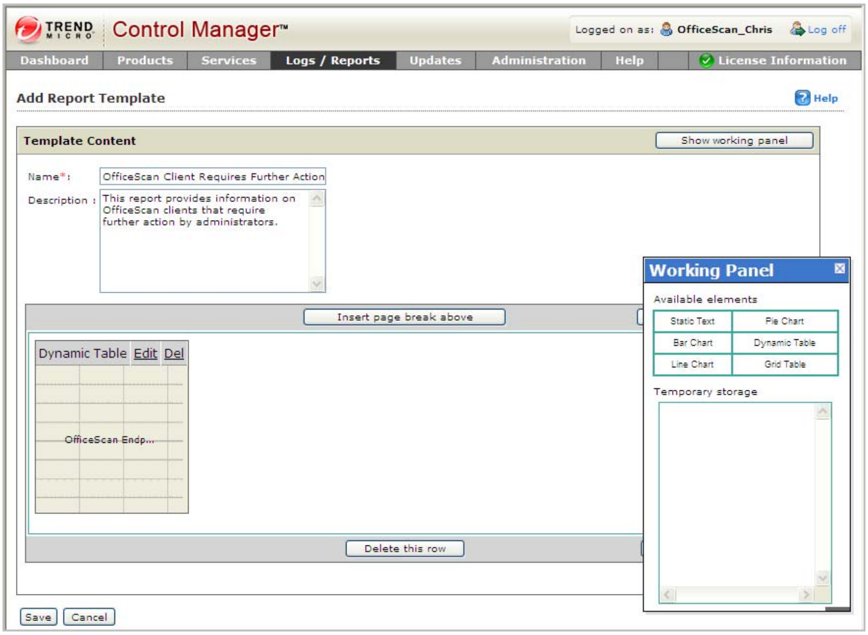
Data field title:

Aggregated by: Sum of value

Row Properties

Row header title: OfficeScan Server > Endpoint

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



Name*: OfficeScan Client Requires Further Action

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

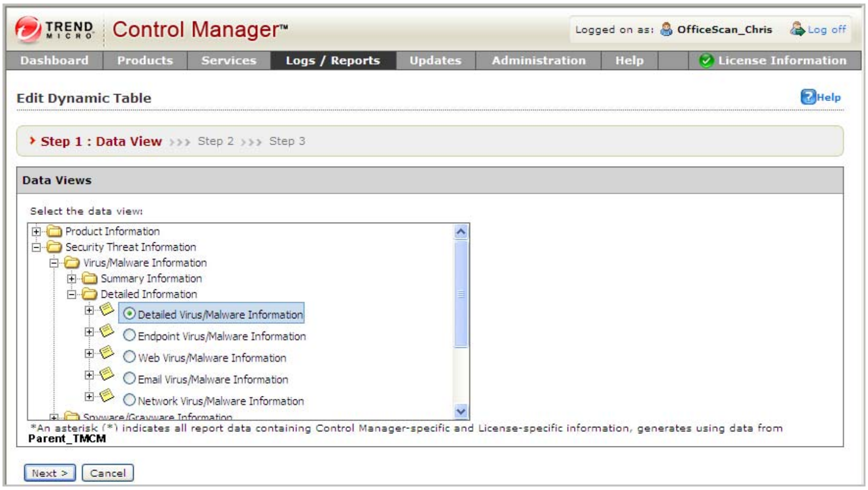
10. Click **Insert Row Below**. A row appears below the first row.

11. 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 > Step 1: Data View screen appears.

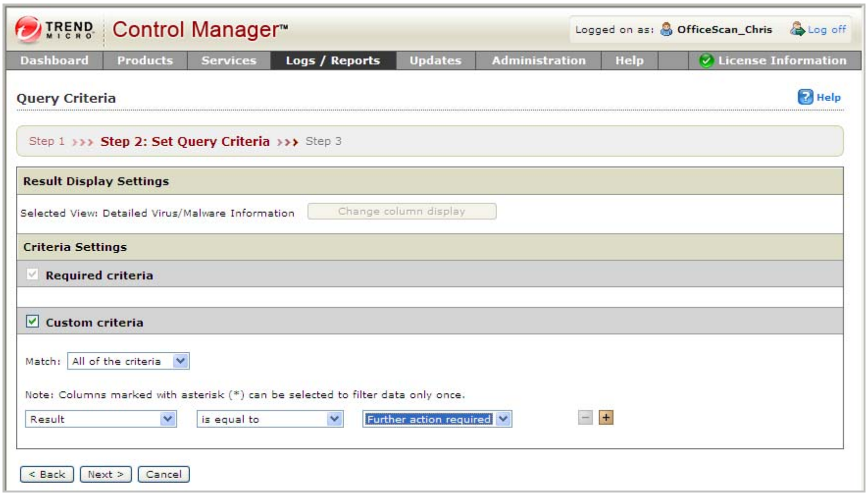

TREND MICRO
Control Manager™
Logged on as: OfficeScan_Chris
Log off
Dashboard
Products
Services
Logs / Reports
Updates
Administration
Help
License Information
Edit Dynamic Table
Help
› Step 1 : Data View ››› Step 2 ››› Step 3
Data Views
Select the data view:
Product Information
Security Threat Information
Virus/Malware Information
Summary Information
Detailed Information
● Detailed Virus/Malware Information
○ Endpoint Virus/Malware Information
○ Web Virus/Malware Information
○ Email Virus/Malware Information
○ Network Virus/Malware Information
Spyware/Grayware Information
Next >
Cancel

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

Step 2: Specify the query criteria for the template:

1. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Selected View: Detailed Virus/Malware Information

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

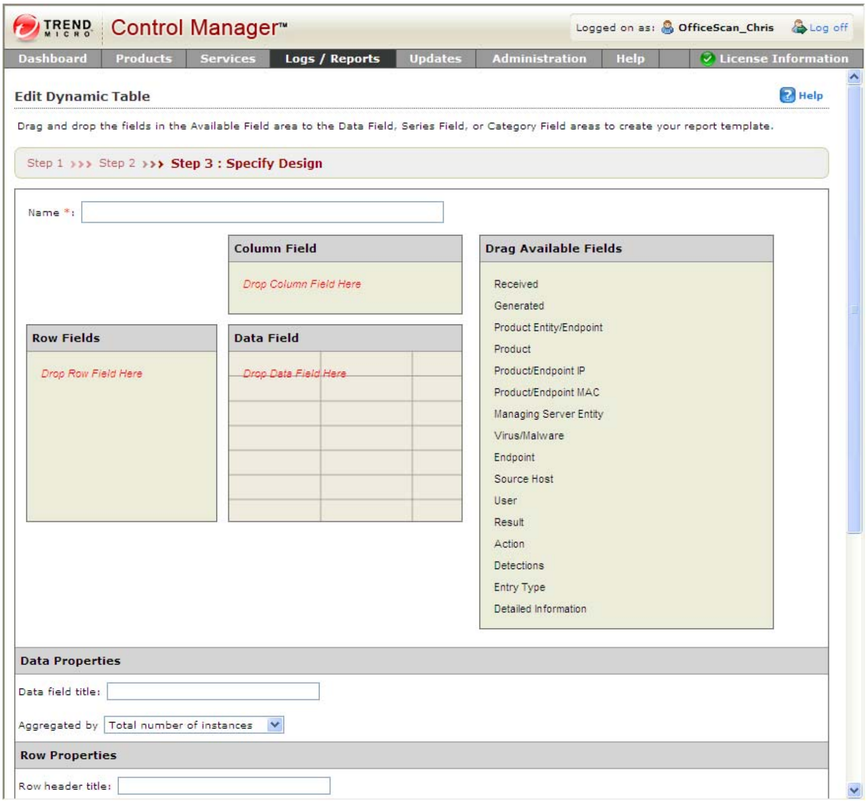
Result | is equal to | Further action required

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).

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

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



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Data field title:

Aggregated by: Total number of instances

Row header title:

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** to **Drop Column Field Here.**

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

3. Drag-and-drop **Managing Server Entity** and then **Endpoint** 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 **Detections** 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 **Row header title** field:

      OfficeScan Server > Endpoint

   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.

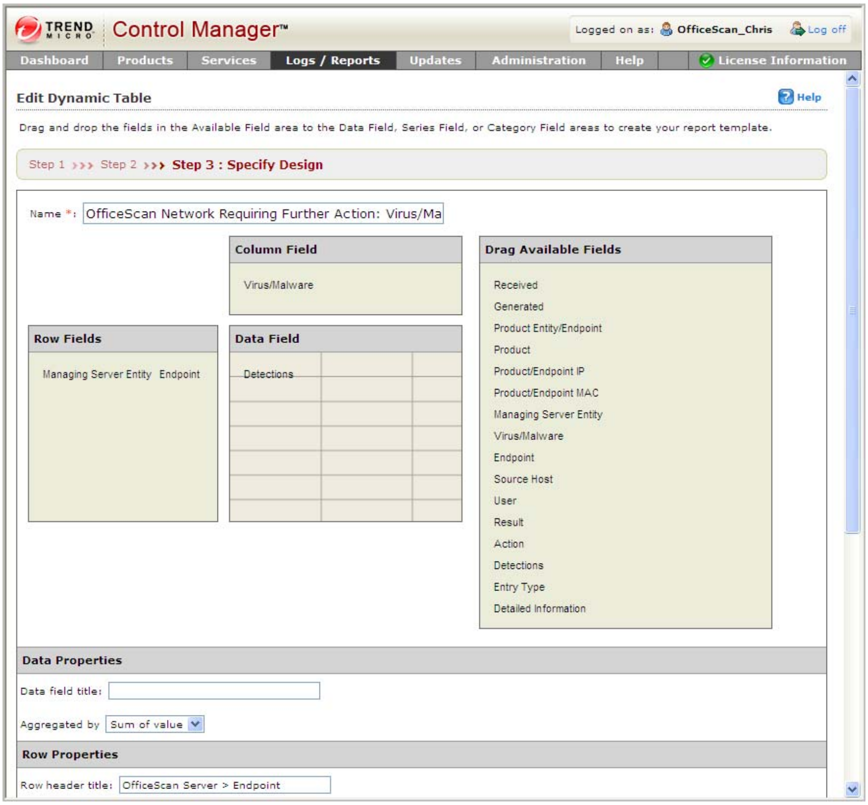
   a. Type the following in the **Column header title** field:

      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.



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› **Step 3 : Specify Design**

Name *: OfficeScan Network Requiring Further Action: Virus/Ma

Column Field

Virus/Malware

Drag Available Fields

Received
Generated
Product Entity/Endpoint
Product
Product/Endpoint IP
Product/Endpoint MAC
Managing Server Entity
Virus/Malware
Endpoint
Source Host
User
Result
Action
Detections
Entry Type
Detailed Information

Row Fields

Managing Server Entity Endpoint

Data Field

Detections

Data Properties

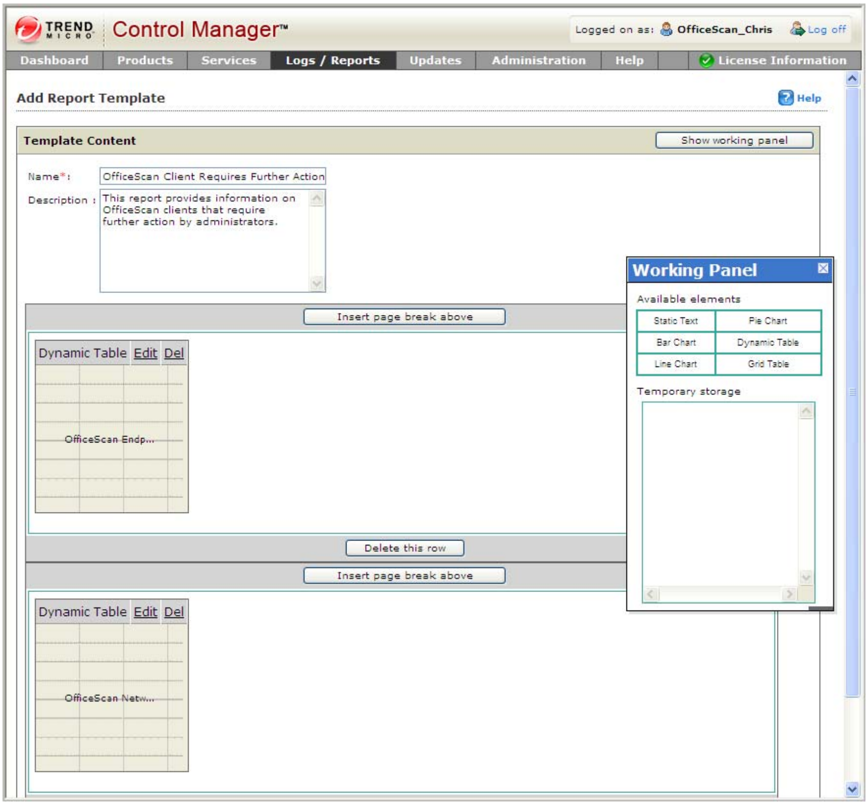
Data field title:

Aggregated by: Sum of value

Row Properties

Row header title: OfficeScan Server > Endpoint

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



Name*: OfficeScan Client Requires Further Action

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

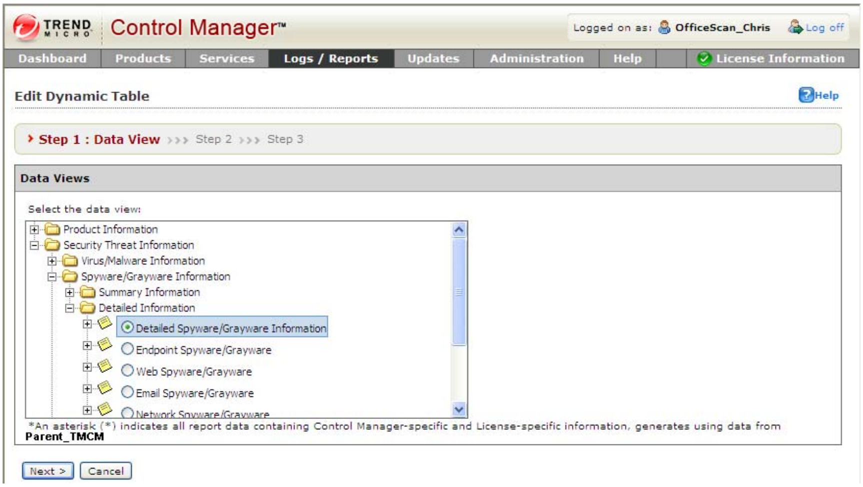
9. Click **Insert Row Below** under the second row. A row appears below the second row.

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 > Step 1: Data View screen appears.



Edit Dynamic Table

Data Views

Select the data view:

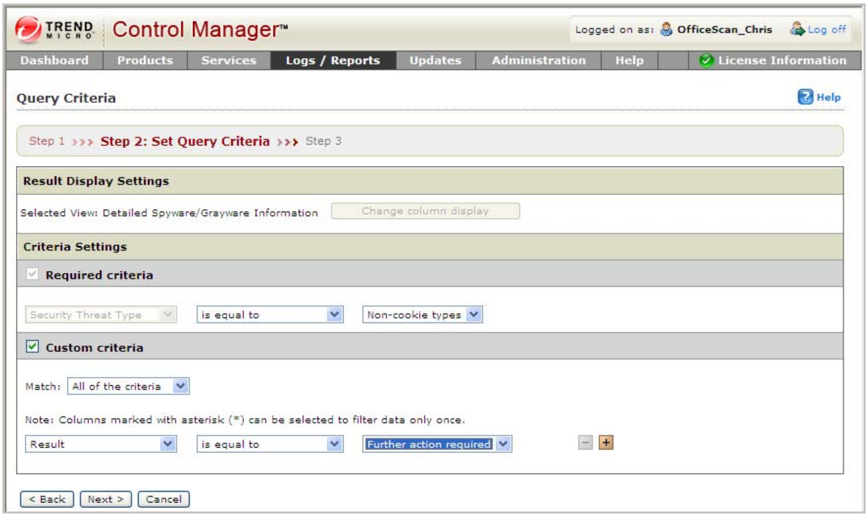
- Product Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
    - Summary Information
    - Detailed Information
      - ● Detailed Spyware/Grayware Information
      - ○ Endpoint Spyware/Grayware
      - ○ Web Spyware/Grayware
      - ○ Email Spyware/Grayware
      - ○ Network Spyware/Grayware

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

Step 2: Specify the query criteria for the template:

1. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 >>> **Step 2: Set Query Criteria** >>> Step 3

Result Display Settings

Selected View: Detailed Spyware/Grayware Information

Criteria Settings

☑ **Required criteria**

Security Threat Type | is equal to | Non-cookie types

☑ **Custom criteria**

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

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.

2. Specify the following:

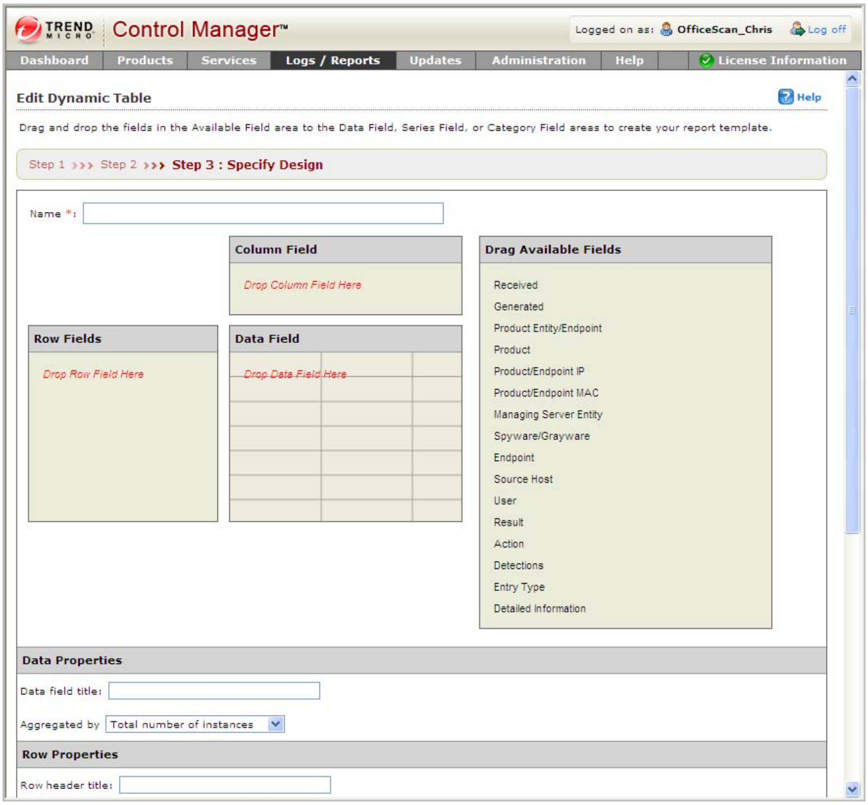
Required criteria:

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

Custom criteria:

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

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



Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Aggregated by: Total number of instances

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 Endpoints Requiring Further Action: Spyware/Grayware

2. Drag-and-drop **Action** 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 **Managing Server Entity** and then **Endpoint** 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 **Detections** 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 **Row header title** field:

      OfficeScan Server > Endpoint

   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.

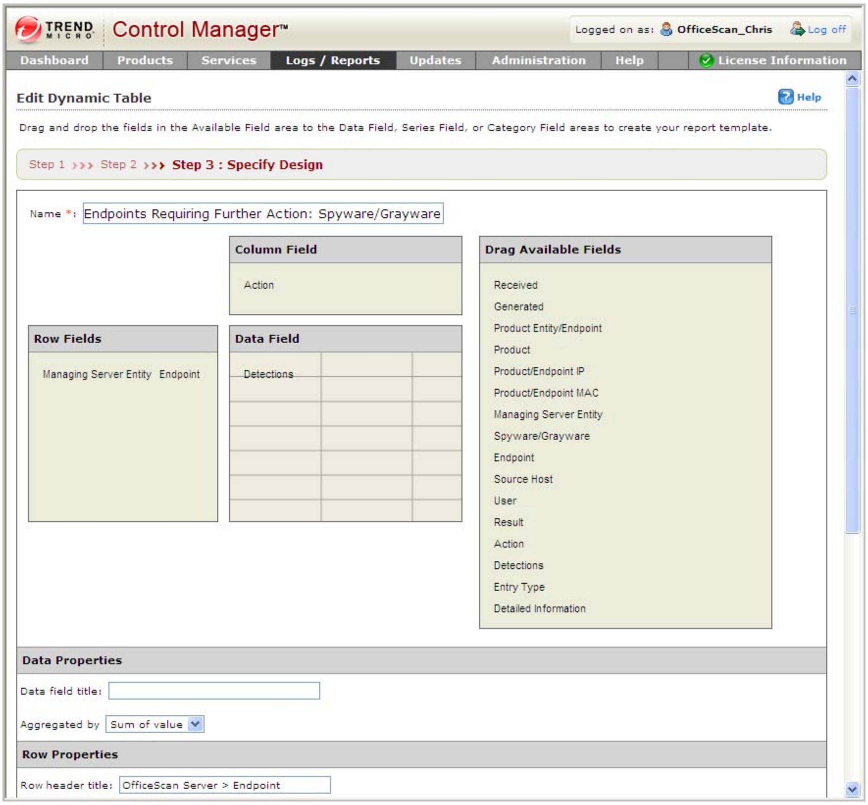
   a. Type the following in the **Column header title** field:

      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.



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› Step 3 : Specify Design

Name *: Endpoints Requiring Further Action: Spyware/Grayware

Column Field: Action

Row Fields: Managing Server Entity Endpoint

Data Field: Detections

Drag Available Fields:
Received
Generated
Product Entity/Endpoint
Product
Product/Endpoint IP
Product/Endpoint MAC
Managing Server Entity
Spyware/Grayware
Endpoint
Source Host
User
Result
Action
Detections
Entry Type
Detailed Information

Data Properties

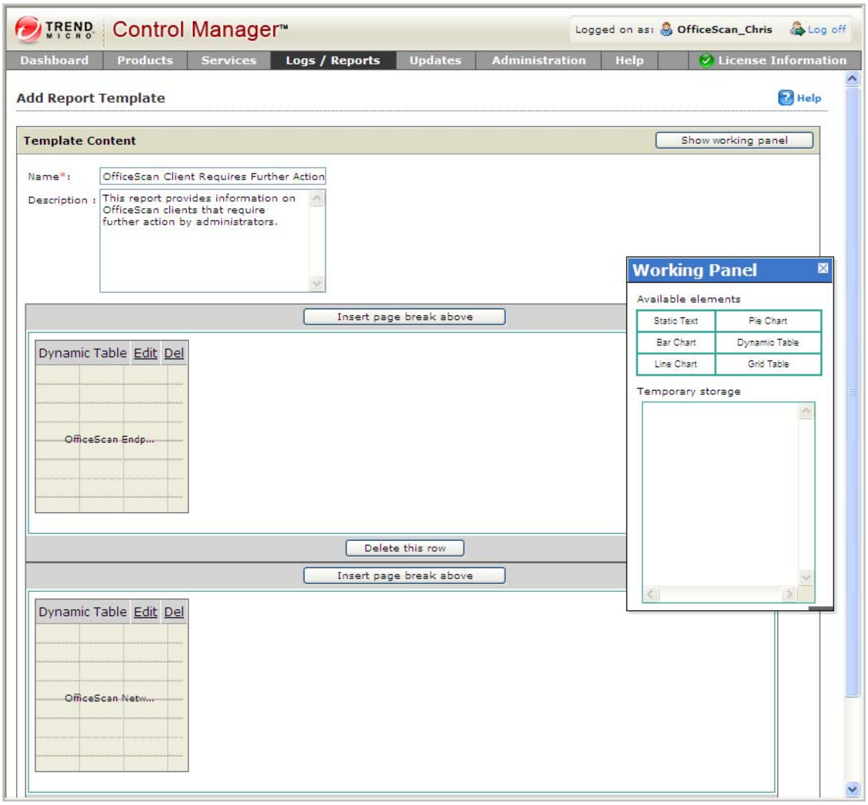
Data field title:

Aggregated by: Sum of value

Row Properties

Row header title: OfficeScan Server > Endpoint

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



Add Report Template

Template Content

Name*: OfficeScan Client Requires Further Action

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

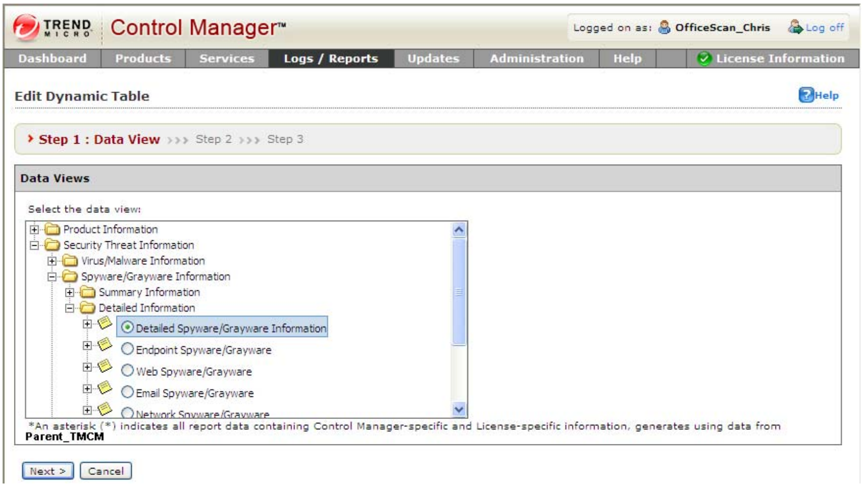
9. Click **Insert Row Below** under the third row. A row appears below the third row.

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 > Step 1: Data View screen appears.



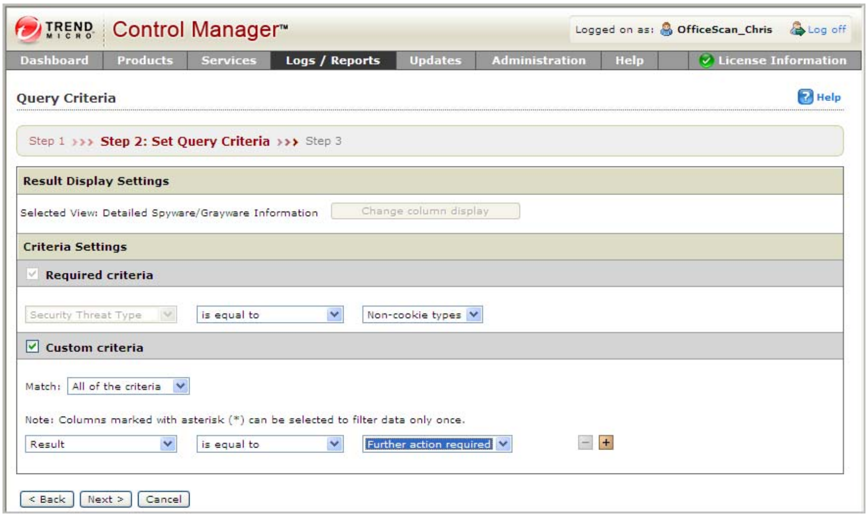
● Detailed Spyware/Grayware Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**

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

Step 2: Specify the filtering criteria for the template:

1. Click **Next**. The Query Criteria > Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 >>> Step 2: Set Query Criteria >>> Step 3

Result Display Settings

Selected View: Detailed Spyware/Grayware Information

Criteria Settings

☑ Required criteria

Security Threat Type | is equal to | Non-cookie types

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

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.

2. Specify the following:

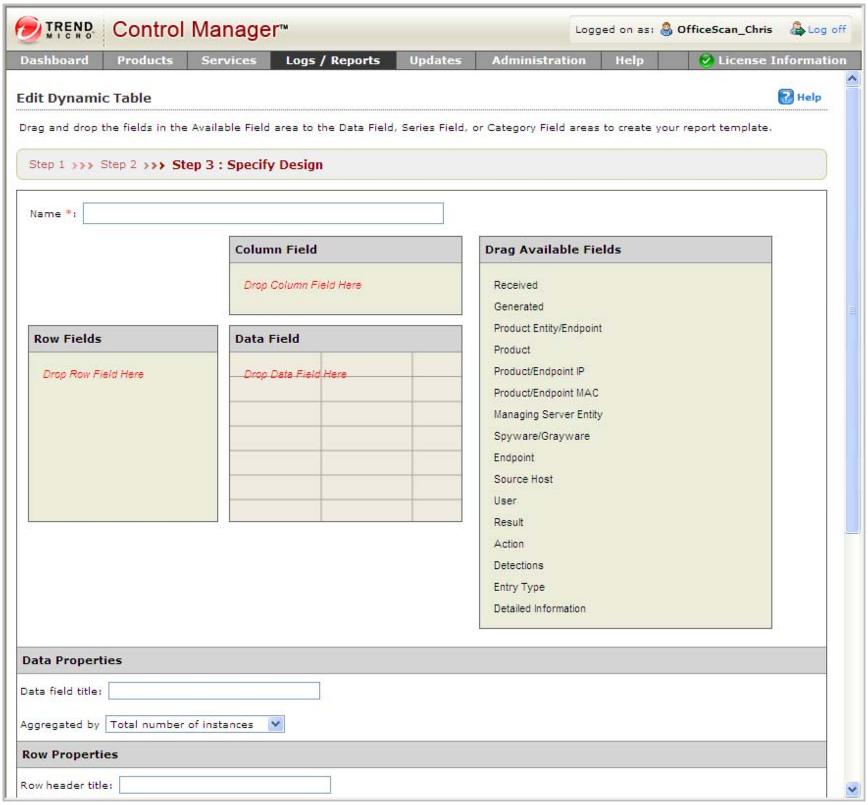
   Required criteria:

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

   Custom criteria:

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

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



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *:

Column Field: Drop Column Field Here

Row Fields: Drop Row Field Here

Data Field: Drop Data Field Here

Drag Available Fields:
- Received
- Generated
- Product Entity/Endpoint
- Product
- Product/Endpoint IP
- Product/Endpoint MAC
- Managing Server Entity
- Spyware/Grayware
- Endpoint
- Source Host
- User
- Result
- Action
- Detections
- Entry Type
- Detailed Information

Data Properties

Data field title:

Aggregated by: Total number of instances

Row Properties

Row header title:

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** to **Drop Column Field Here.**

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

3. Drag-and-drop **Managing Server Entity** and then **Endpoint** 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 **Detections** 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 **Row header title** field:

      OfficeScan Server > Endpoint

   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.

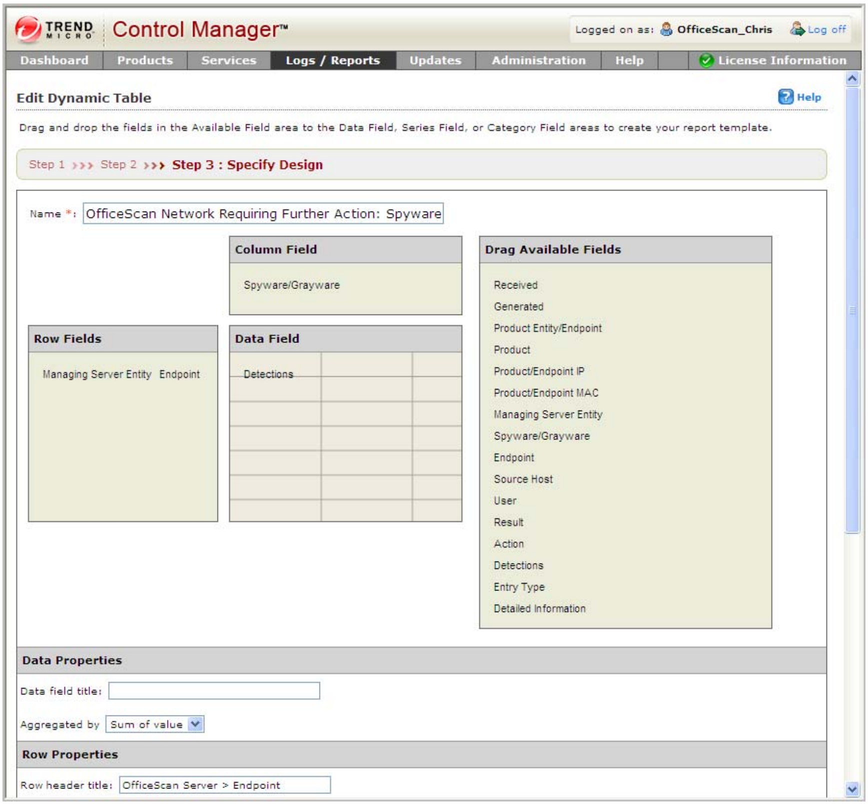
   a. Type the following in the **Column header title** field:

      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.



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 ››› Step 2 ››› **Step 3 : Specify Design**

Name *: OfficeScan Network Requiring Further Action: Spyware

Column Field

Spyware/Grayware

Row Fields

Managing Server Entity Endpoint

Data Field

Detections

Drag Available Fields

Received
Generated
Product Entity/Endpoint
Product
Product/Endpoint IP
Product/Endpoint MAC
Managing Server Entity
Spyware/Grayware
Endpoint
Source Host
User
Result
Action
Detections
Entry Type
Detailed Information

Data Properties

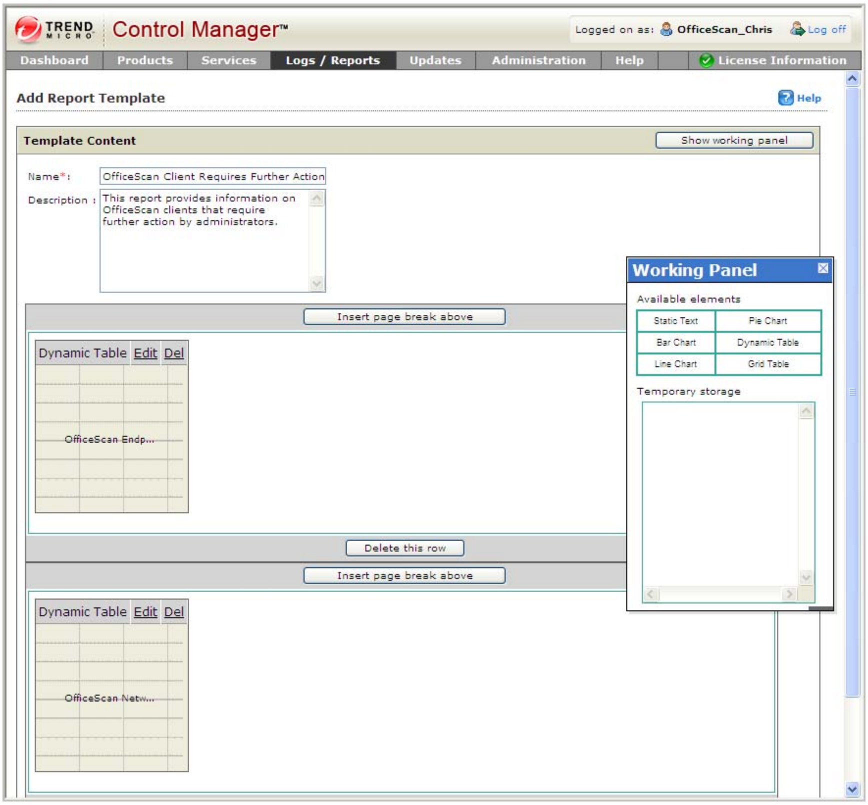
Data field title:

Aggregated by: Sum of value

Row Properties

Row header title: OfficeScan Server > Endpoint

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



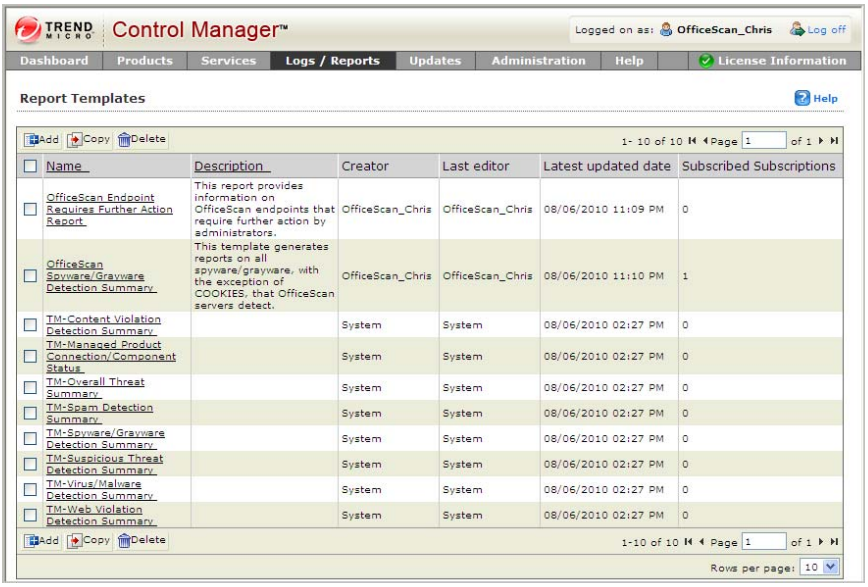
Add Report Template

Template Content

Name*: OfficeScan Client Requires Further Action

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

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



Report Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	OfficeScan Endpoint Requires Further Action Report	This report provides information on OfficeScan endpoints that require further action by administrators.	OfficeScan_Chris	OfficeScan_Chris	08/06/2010 11:09 PM	0
□	OfficeScan Spyware/Grayware Detection Summary	This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.	OfficeScan_Chris	OfficeScan_Chris	08/06/2010 11:10 PM	1
□	TM-Content Violation Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Managed Product Connection/Component Status		System	System	08/06/2010 02:27 PM	0
□	TM-Overall Threat Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Spam Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Spyware/Grayware Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Suspicious Threat Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Virus/Malware Detection Summary		System	System	08/06/2010 02:27 PM	0
□	TM-Web Violation Detection Summary		System	System	08/06/2010 02:27 PM	0

Viewing the Generated Report

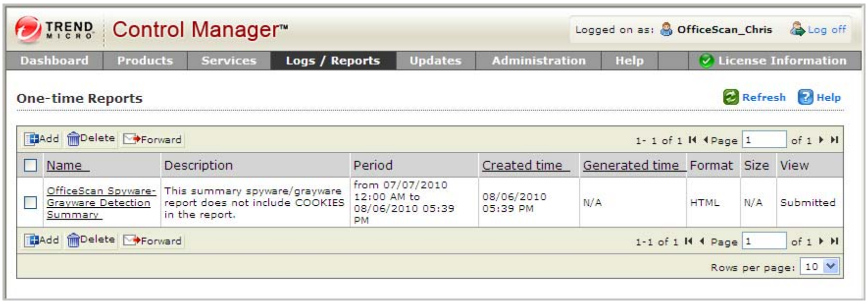
After modifying the template, Chris wants to see how the report would look. Again, to quickly view a report using this template, Chris needs to create a one-time report. Chris would also like to gather feedback from other OfficeScan administrators and his boss on the layout of the report. He will email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

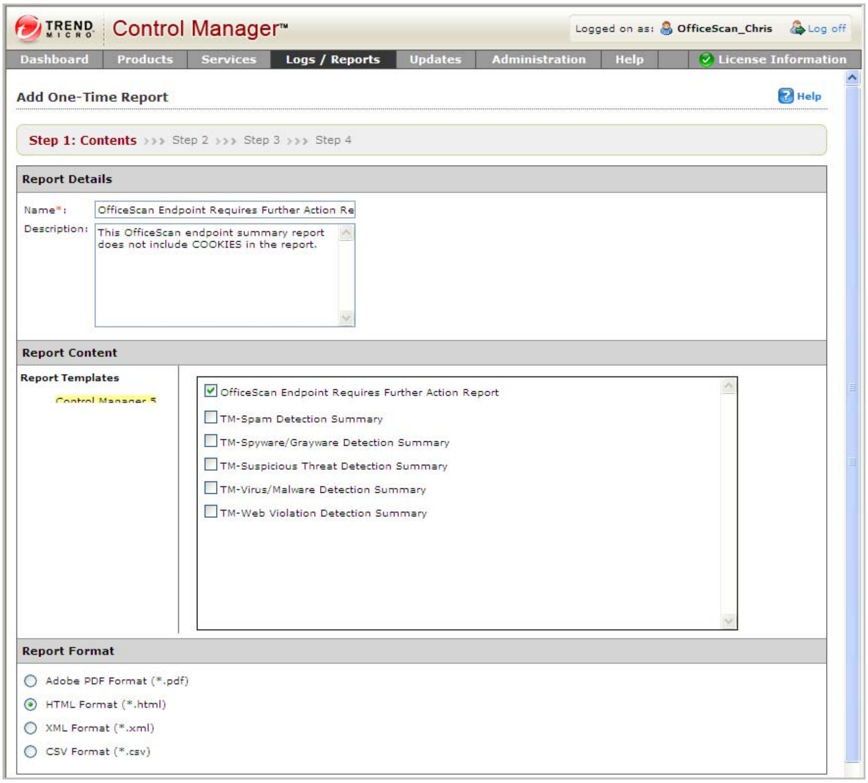
3. Click **One-time Reports** from the menu. The One-time Reports screen appears.



One-time Reports

☐	Name	Description	Period	Created time	Generated time	Format	Size	View
☐	OfficeScan Spyware-Grayware Detection Summary	This summary spyware/grayware report does not include COOKIES in the report.	from 07/07/2010 12:00 AM to 08/06/2010 05:39 PM	08/06/2010 05:39 PM	N/A	HTML	N/A	Submitted

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



Add One-Time Report

Report Details

Name*: OfficeScan Endpoint Requires Further Action Re

Description: This OfficeScan endpoint summary report does not include COOKIES in the report.

Report Content

Report Templates

Control Manager 5

☑ OfficeScan Endpoint Requires Further Action Report

□ TM-Spam Detection Summary

□ TM-Spyware/Grayware Detection Summary

□ TM-Suspicious Threat Detection Summary

□ TM-Virus/Malware Detection Summary

□ TM-Web Violation Detection Summary

Report Format

○ Adobe PDF Format (*.pdf)

● HTML Format (*.html)

○ XML Format (*.xml)

○ CSV Format (*.csv)

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

   OfficeScan Endpoint Requires Further Action Report

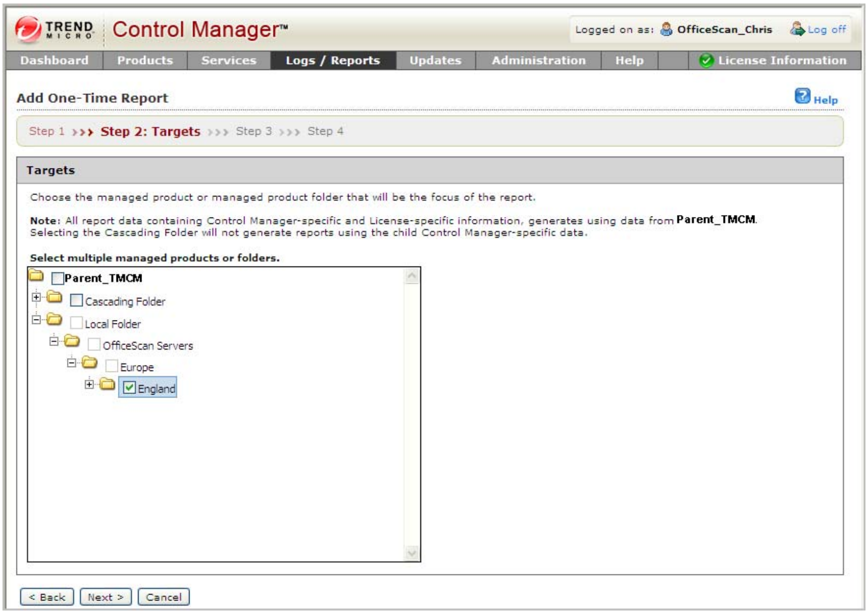
6. Type the following in the **Description** field, under Report Details:

   This OfficeScan endpoint summary report does not include COOKIES in the report.

7. Select the **OfficeScan Endpoint 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.



Add One-Time Report

Step 1 >>> **Step 2: Targets** >>> Step 3 >>> Step 4

Targets

Choose the managed product or managed product folder that will be the focus of the report.

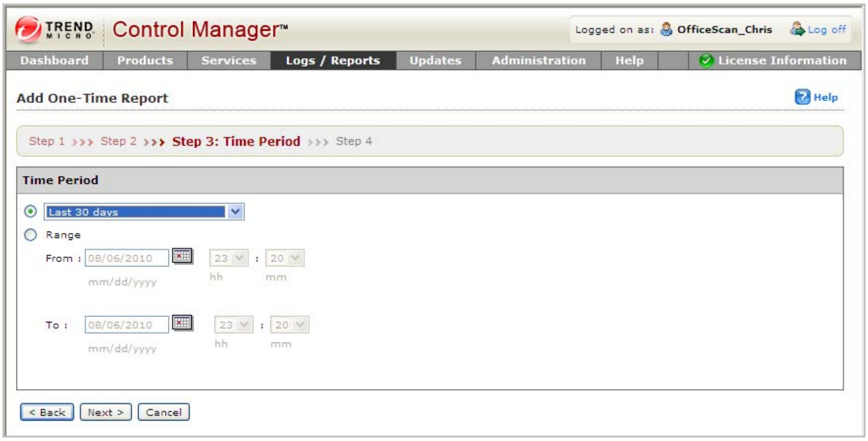
Note: All report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.

Select multiple managed products or folders.

- □ **Parent_TMCM**
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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.



Add One-Time Report

Time Period

● Last 30 days

○ Range

From : 08/06/2010 mm/dd/yyyy 23 hh : 20 mm

To : 08/06/2010 mm/dd/yyyy 23 hh : 20 mm

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.

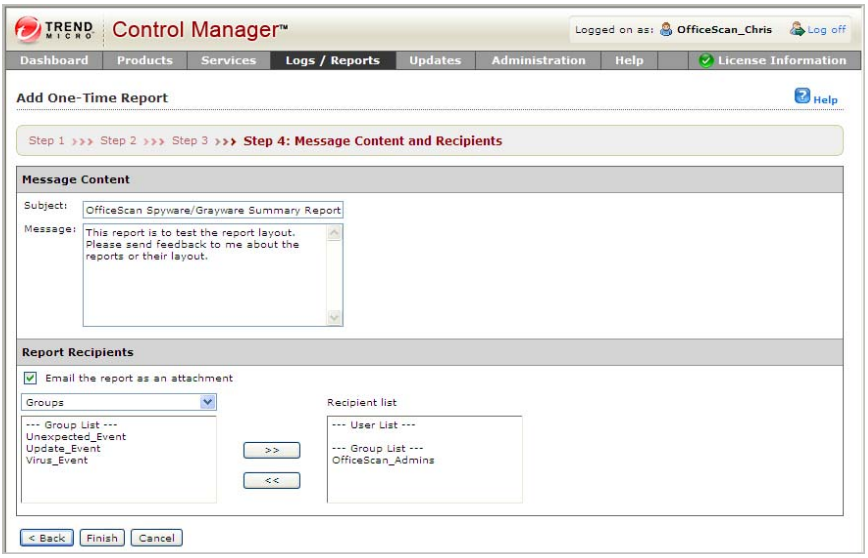
b. Specify a time in the accompanying **hh** and **mm** fields.

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.



Subject: OfficeScan Spyware/Grayware Summary Report

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

☑ Email the report as an attachment

--- Group List ---
Unexpected_Event
Update_Event
Virus_Event

--- User List ---

--- Group List ---
OfficeScan_Admins

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

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

   OfficeScan Spyware/Grayware Summary Report

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**.

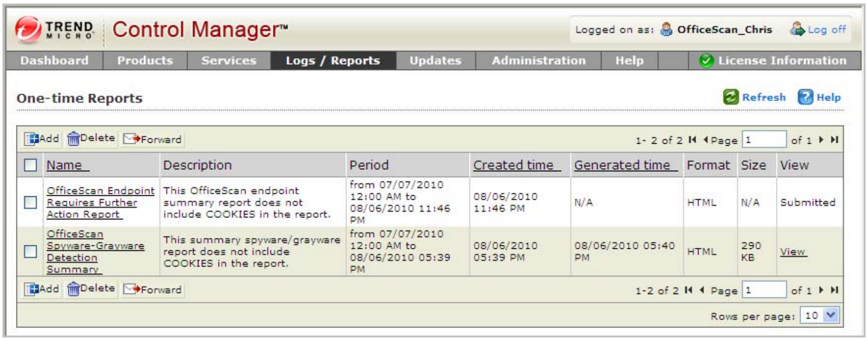
4. Add the following users to the **Report Recipients** list:

   Groups:

   - **OfficeScan_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.



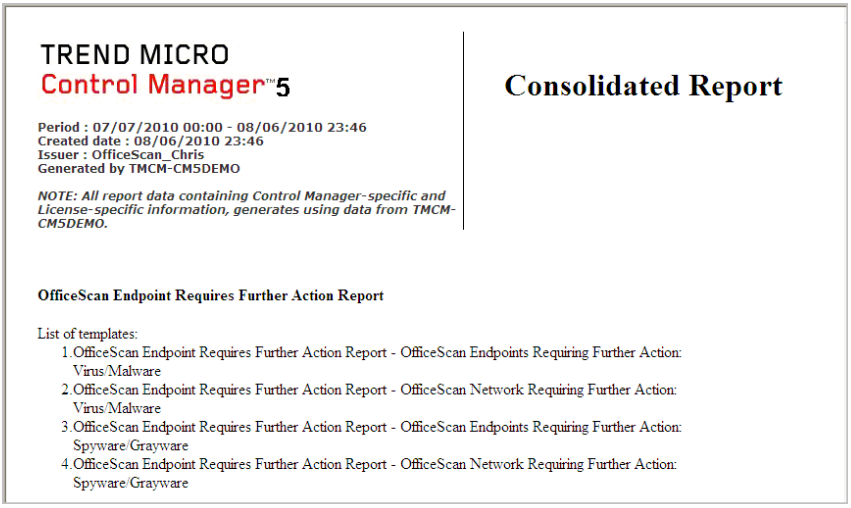
One-time Reports

□	Name	Description	Period	Created time	Generated time	Format	Size	View
□	OfficeScan Endpoint Requires Further Action Report	This OfficeScan endpoint summary report does not include COOKIES in the report.	from 07/07/2010 12:00 AM to 08/06/2010 11:46 PM	08/06/2010 11:46 PM	N/A	HTML	N/A	Submitted
□	OfficeScan Spyware-Grayware Detection Summary	This summary spyware/grayware report does not include COOKIES in the report.	from 07/07/2010 12:00 AM to 08/06/2010 05:39 PM	08/06/2010 05:39 PM	08/06/2010 05:40 PM	HTML	290 KB	View

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.



TREND MICRO
Control Manager™5

Period : 07/07/2010 00:00 - 08/06/2010 23:46
Created date : 08/06/2010 23:46
Issuer : OfficeScan_Chris
Generated by TMCM-CM5DEMO

NOTE: All report data containing Control Manager-specific and License-specific information, generates using data from TMCM-CM5DEMO.

Consolidated Report

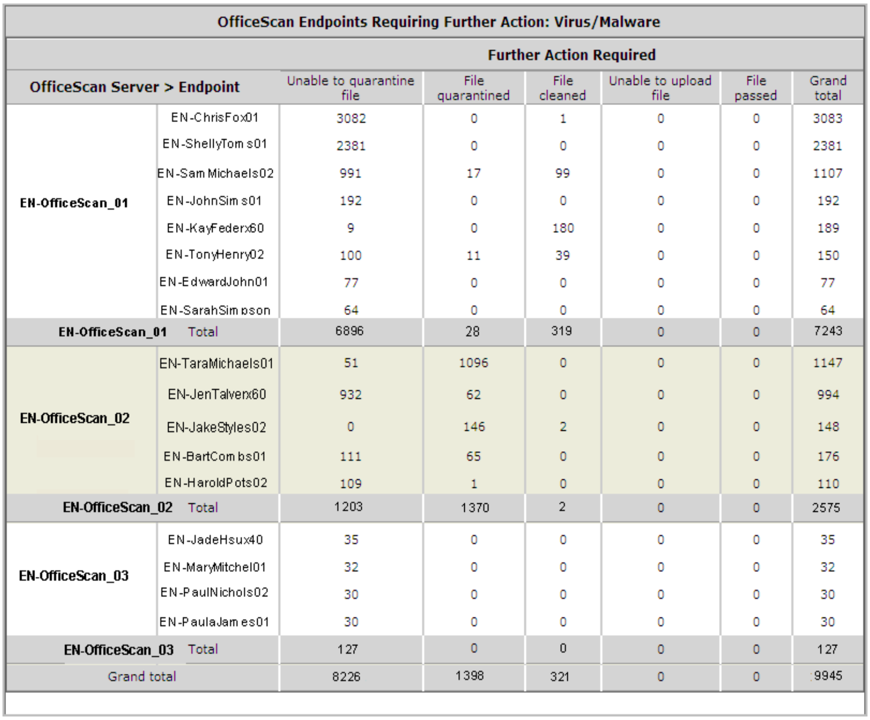
OfficeScan Endpoint Requires Further Action Report

List of templates:

1. OfficeScan Endpoint Requires Further Action Report - OfficeScan Endpoints Requiring Further Action: Virus/Malware
2. OfficeScan Endpoint Requires Further Action Report - OfficeScan Network Requiring Further Action: Virus/Malware
3. OfficeScan Endpoint Requires Further Action Report - OfficeScan Endpoints Requiring Further Action: Spyware/Grayware
4. OfficeScan Endpoint Requires Further Action Report - OfficeScan Network Requiring Further Action: Spyware/Grayware

.

TABLE 4-19. OfficeScan Endpoints Requiring Further Action: Virus/Malware Dynamic Table



OfficeScan Endpoints Requiring Further Action: Virus/Malware

OfficeScan Server > Endpoint		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-ShellyToms01	2381	0	0	0	0	2381
	EN-SamMichaels02	991	17	99	0	0	1107
	EN-JohnSims01	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-SarahSimpson	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-BartCombs01	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-PaulaJames01	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 Virus/Malware Information

Query Criteria:

- Result > is equal to > Further action required

Data Properties:

- Detections
- Aggregated by: Sum of value

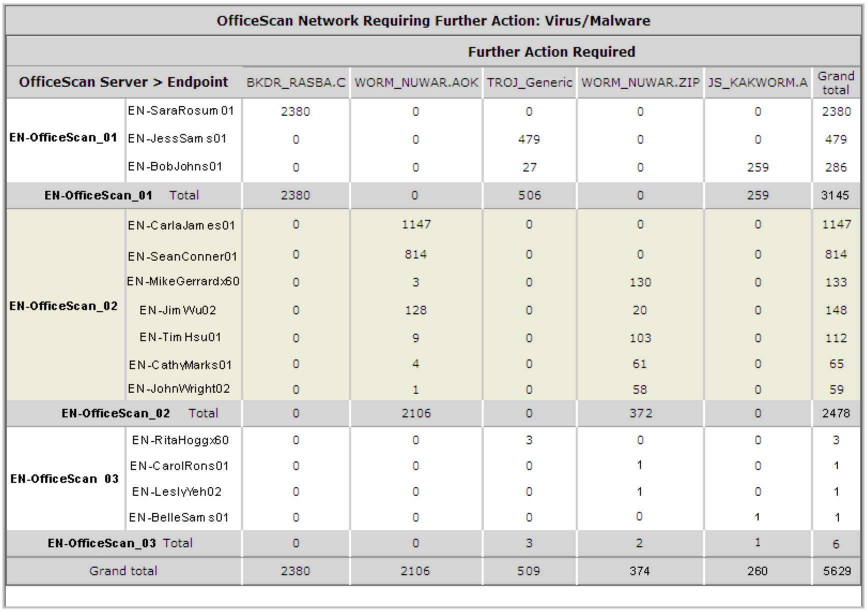
Row Properties:

- Managing Server Entity + Endpoint
- Row header title: OfficeScan Server > Endpoint
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Action
- Column header title: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-20. OfficeScan Network Requiring Further Action: Virus/Malware Dynamic Table



OfficeScan Network Requiring Further Action: Virus/Malware

OfficeScan Server > Endpoint		Further Action Required 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 Virus/Malware Information

Query Criteria:

- Result > is equal to > Further action required

Data Properties:

- Detections
- Aggregated by: Sum of value

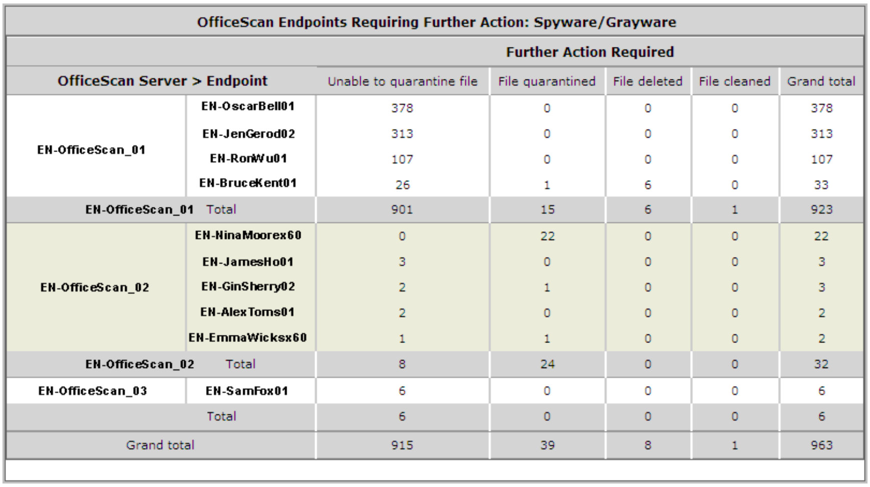
Row Properties:

- Managing Server Entity + Endpoint
- Row header title: OfficeScan Server > Endpoint
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Virus/Malware
- Column header title: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-21. OfficeScan Endpoints Requiring Further Action: Spyware/Grayware Dynamic Table



OfficeScan Endpoints Requiring Further Action: Spyware/Grayware

OfficeScan Server > Endpoint		Further Action Required				
		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 Spyware/Grayware Information

Query Criteria:

- Security Threat Type > is equal to > Non-cookie types
- Result > is equal to > Further action required

Data Properties:

- Detections
- Aggregated by: Sum of value

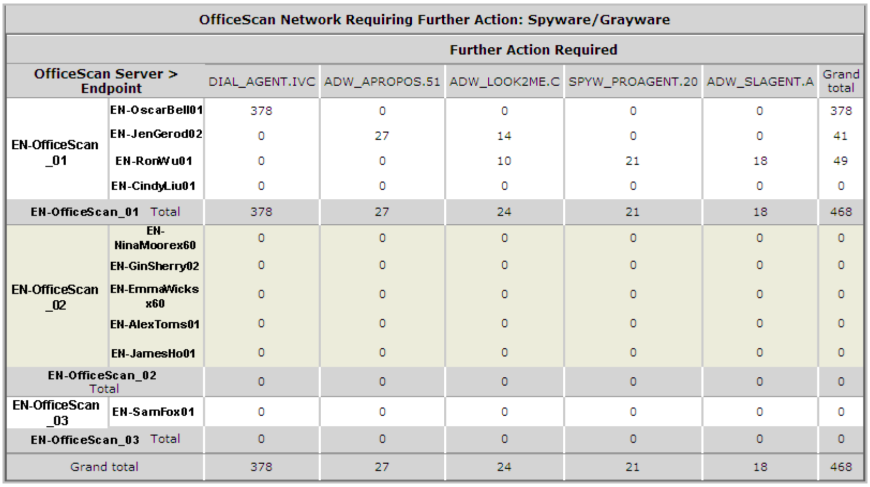
Row Properties:

- Managing Server Entity + Endpoint
- Row header title: OfficeScan Server > Endpoint
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Action
- Column header title: Further Action Required
- Sorting: Aggregation value > Descending

TABLE 4-22. OfficeScan Network Requiring Further Action: Spyware/Grayware Dynamic Table



OfficeScan Network Requiring Further Action: Spyware/Grayware

OfficeScan Server > Endpoint		Further Action Required					
		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 Spyware/Grayware Information

Query Criteria:

- Security Threat Type > is equal to > Non-cookie types
- Result > is equal to > Further action required

Data Properties:

- Detections
- Aggregated by: Sum of value

Row Properties:

- Managing Server Entity + Endpoint
- Row header title: OfficeScan Server > Endpoint
- Sorting: Aggregation value > Descending
- Do not filter summarized result

Category Properties:

- Spyware/Grayware
- Column header title: Further Action Required
- Sorting: Aggregation value > Descending

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a scheduled report is similar for all report types:

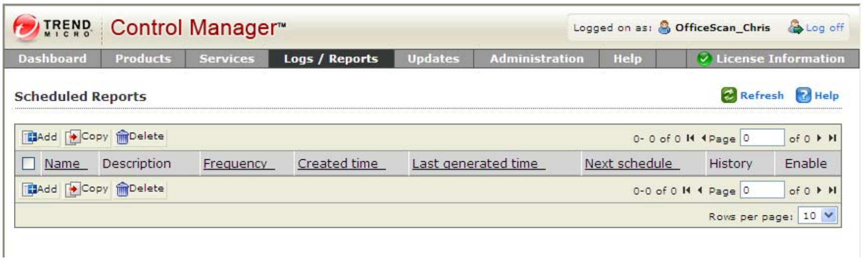
1. Access the Add Scheduled Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

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:

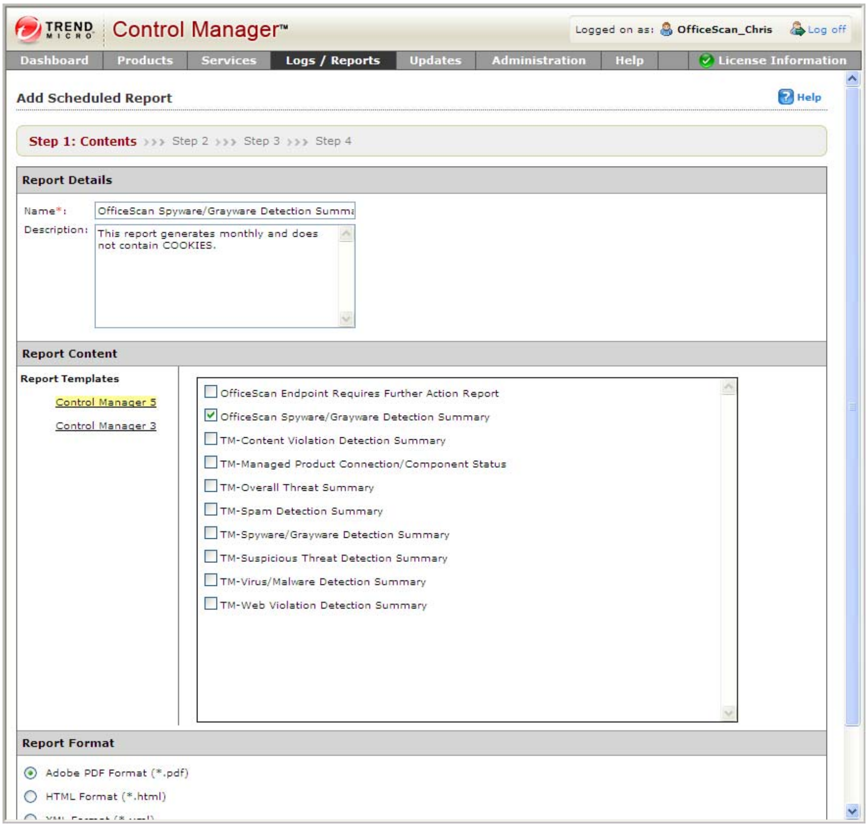
1. Log on to the Control Manager Web console as **Chris**.
2. Mouseover **Logs/Reports**. A drop-down menu appears.
3. Click **Scheduled Reports** from the menu. The Scheduled Reports screen appears.



Scheduled Reports

□	Name	Description	Frequency	Created time	Last generated time	Next schedule	History	Enable

4. Click **Add**. The Add Scheduled Report > Step 1: Contents screen appears.



Add Scheduled Report

Step 1: Contents >>> Step 2 >>> Step 3 >>> Step 4

Report Details

Name*: OfficeScan Spyware/Grayware Detection Summa

Description: This report generates monthly and does not contain COOKIES.

Report Content

Report Templates

Control Manager 5

Control Manager 3

- □ OfficeScan Endpoint Requires Further Action Report
- ☑ OfficeScan Spyware/Grayware Detection Summary
- □ TM-Content Violation Detection Summary
- □ TM-Managed Product Connection/Component Status
- □ TM-Overall Threat Summary
- □ TM-Spam Detection Summary
- □ TM-Spyware/Grayware Detection Summary
- □ TM-Suspicious Threat Detection Summary
- □ TM-Virus/Malware Detection Summary
- □ TM-Web Violation Detection Summary

Report Format

- ● Adobe PDF Format (*.pdf)
- ○ HTML Format (*.html)
- ○ XML Format (*.xml)

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

   OfficeScan Spyware/Grayware Detection Summary

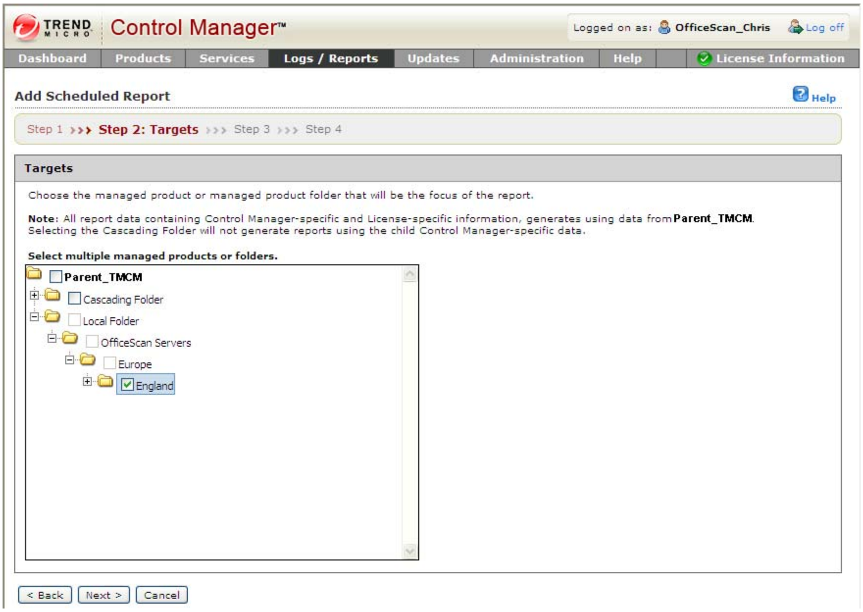
6. Type the following in the **Description** field:

   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.



Add Scheduled Report

Targets

Choose the managed product or managed product folder that will be the focus of the report.

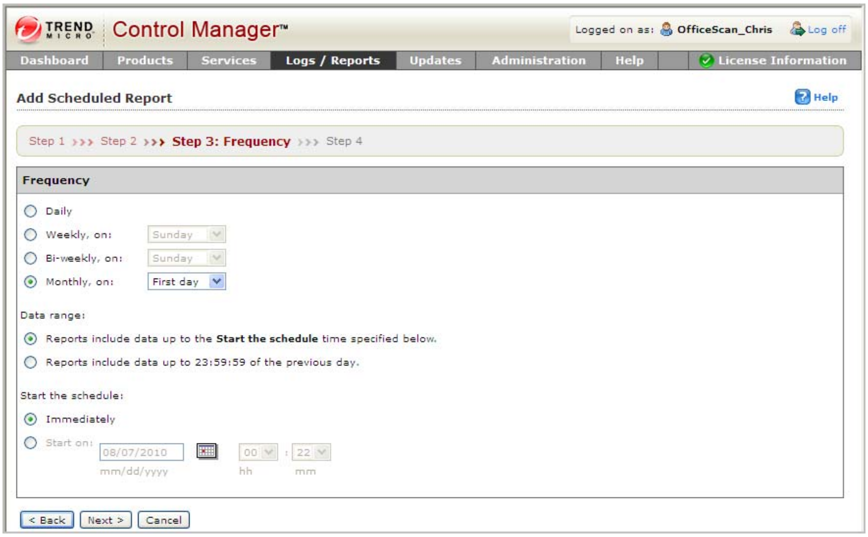
Note: All report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.

Select multiple managed products or folders.

- □ **Parent_TMCM**
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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.



Add Scheduled Report

Frequency

○ Daily
○ Weekly, on: Sunday
○ Bi-weekly, on: Sunday
● Monthly, on: First day

Data range:

● Reports include data up to the **Start the schedule** time specified below.
○ Reports include data up to 23:59:59 of the previous day.

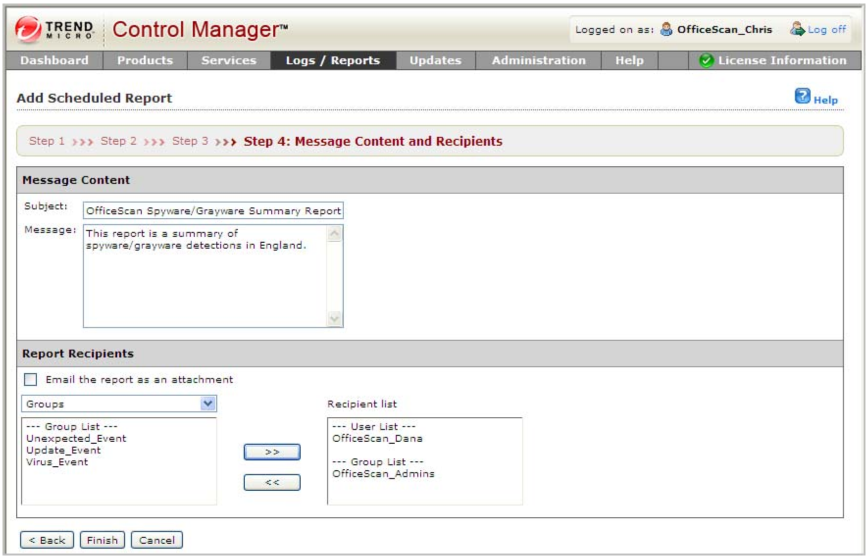
Start the schedule:

● Immediately
○ Start on: 08/07/2010 (mm/dd/yyyy) 00 (hh) : 22 (mm)

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.



Add Scheduled Report

Message Content

Subject: OfficeScan Spyware/Grayware Summary Report

Message: This report is a summary of spyware/grayware detections in England.

Report Recipients

□ Email the report as an attachment

Groups

--- Group List ---
Unexpected_Event
Update_Event
Virus_Event

Recipient list

--- User List ---
OfficeScan_Dana

--- Group List ---
OfficeScan_Admins

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:

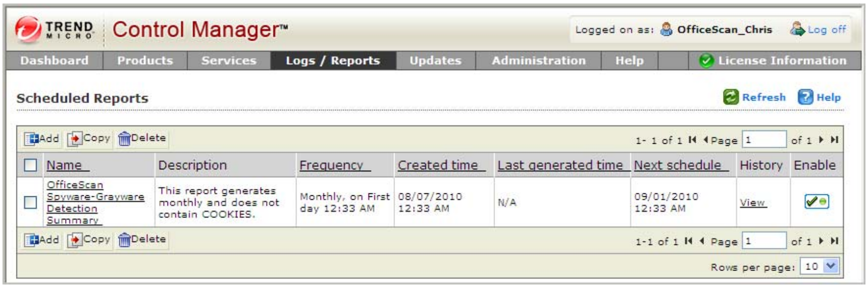
   Users:

   - **OfficeScan_Dana**

   Groups:

   - **OfficeScan_Admins**

5. Click **Finish**. The Scheduled Reports screen appears with the report in the Scheduled Reports list.

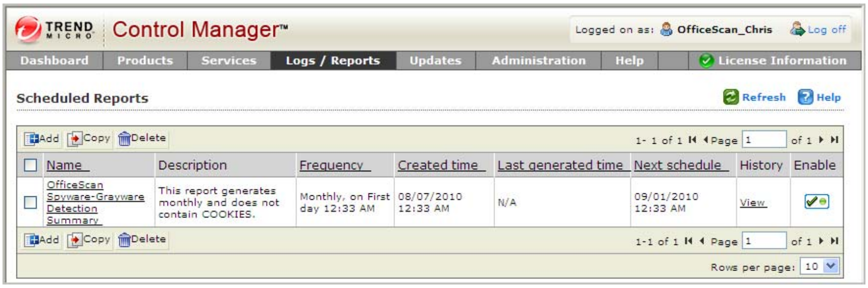


☐	Name	Description	Frequency	Created time	Last generated time	Next schedule	History	Enable
☐	OfficeScan Spyware-Grayware Detection Summary	This report generates monthly and does not contain COOKIES.	Monthly, on First day 12:33 AM	08/07/2010 12:33 AM	N/A	09/01/2010 12:33 AM	View	✓

To add OfficeScan Requires Further Action Report as a scheduled report:

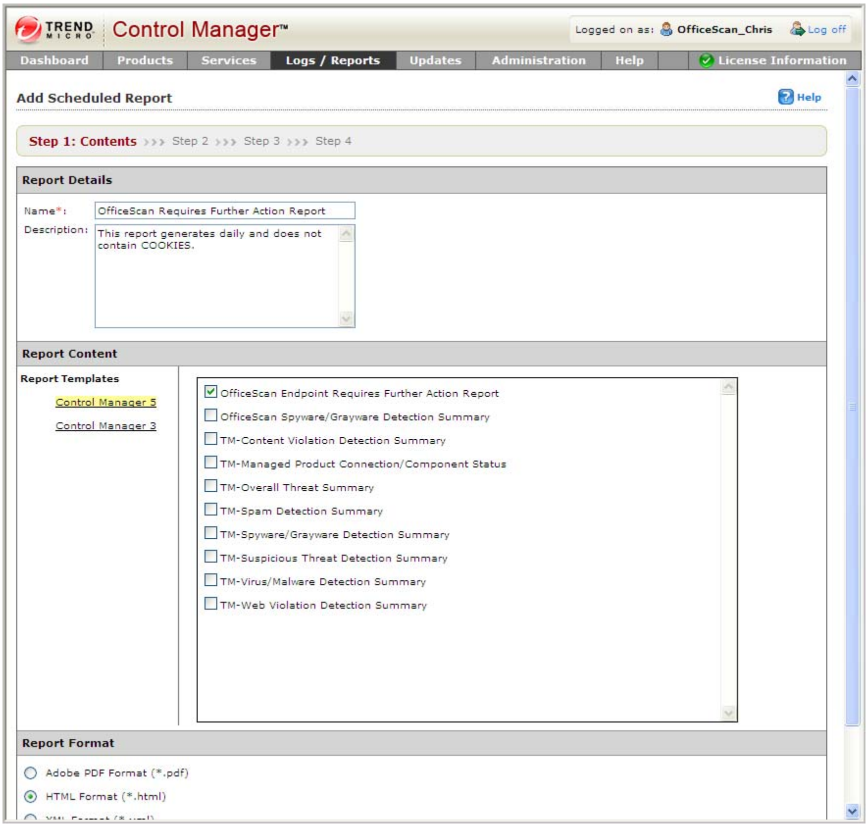
Step 1: Access the Add Scheduled Report screen and select the report type:

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.



☐	Name	Description	Frequency	Created time	Last generated time	Next schedule	History	Enable
☐	OfficeScan Spyware-Grayware Detection Summary	This report generates monthly and does not contain COOKIES.	Monthly, on First day 12:33 AM	08/07/2010 12:33 AM	N/A	09/01/2010 12:33 AM	View	✓

4. Click **Add**. The Add Scheduled Report > Step 1: Contents screen appears.



Add Scheduled Report

Step 1: Contents >>> Step 2 >>> Step 3 >>> Step 4

Report Details

Name*: OfficeScan Requires Further Action Report

Description: This report generates daily and does not contain COOKIES.

Report Content

Report Templates

Control Manager 5

Control Manager 3

☑ OfficeScan Endpoint Requires Further Action Report
☐ OfficeScan Spyware/Grayware Detection Summary
☐ TM-Content Violation Detection Summary
☐ TM-Managed Product Connection/Component Status
☐ TM-Overall Threat Summary
☐ TM-Spam Detection Summary
☐ TM-Spyware/Grayware Detection Summary
☐ TM-Suspicious Threat Detection Summary
☐ TM-Virus/Malware Detection Summary
☐ TM-Web Violation Detection Summary

Report Format

○ Adobe PDF Format (*.pdf)
● HTML Format (*.html)
○ XML Format (*.xml)

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

   OfficeScan Requires Further Action Report

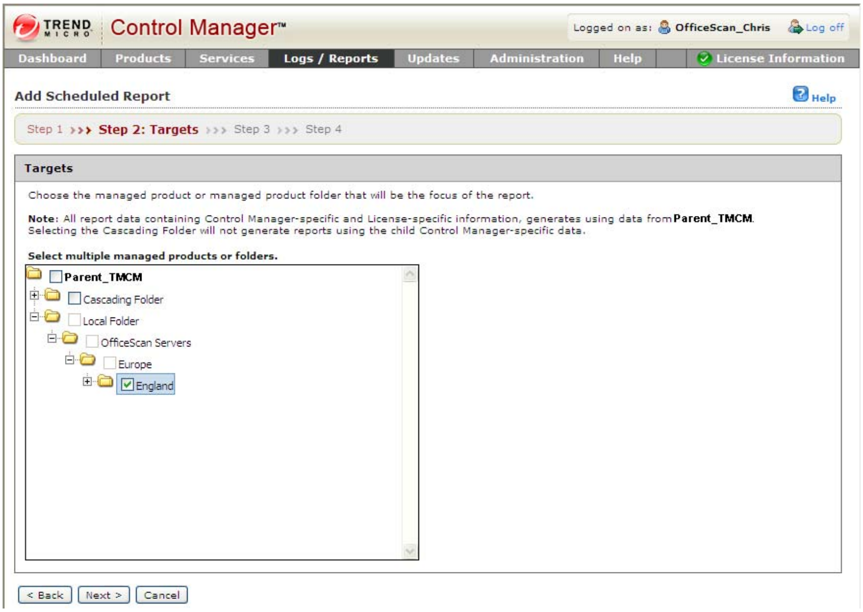
6. Type the following in the **Description** field:

   This report generates daily and does not contain COOKIES.

7. Select the **OfficeScan Endpoint Requires Further Action Report**.

8. Select **HTML Format (*.html)**.

9. Click **Next**. The Add Scheduled Report > Step 2: Targets screen appears.



Add Scheduled Report

Targets

Choose the managed product or managed product folder that will be the focus of the report.

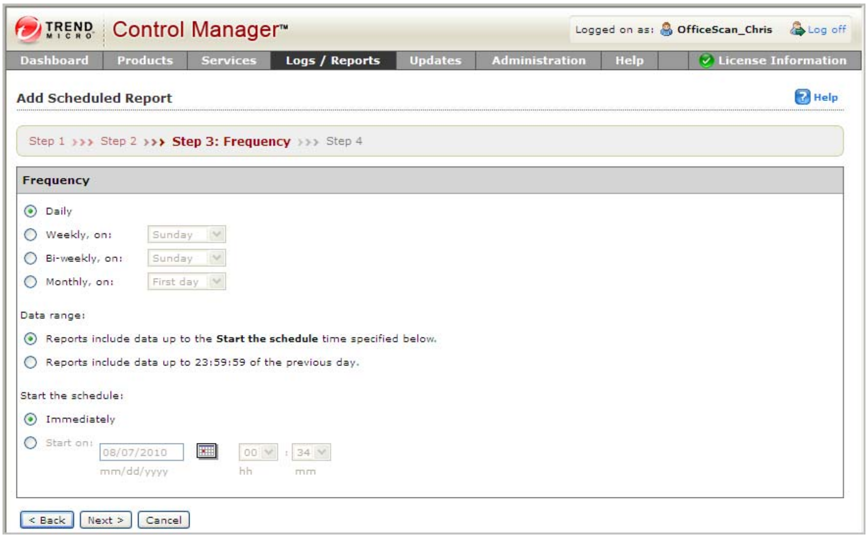
Note: All report data containing Control Manager-specific and License-specific information, generates using data from **Parent_TMCM**. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.

Select multiple managed products or folders.

- □ **Parent_TMCM**
  - □ Cascading Folder
  - □ Local Folder
    - □ OfficeScan Servers
      - □ Europe
        - ☑ England

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.



Add Scheduled Report

Step 1 >>> Step 2 >>> Step 3: Frequency >>> Step 4

Frequency

● Daily
○ Weekly, on: Sunday
○ Bi-weekly, on: Sunday
○ Monthly, on: First day

Data range:

● Reports include data up to the **Start the schedule** time specified below.
○ Reports include data up to 23:59:59 of the previous day.

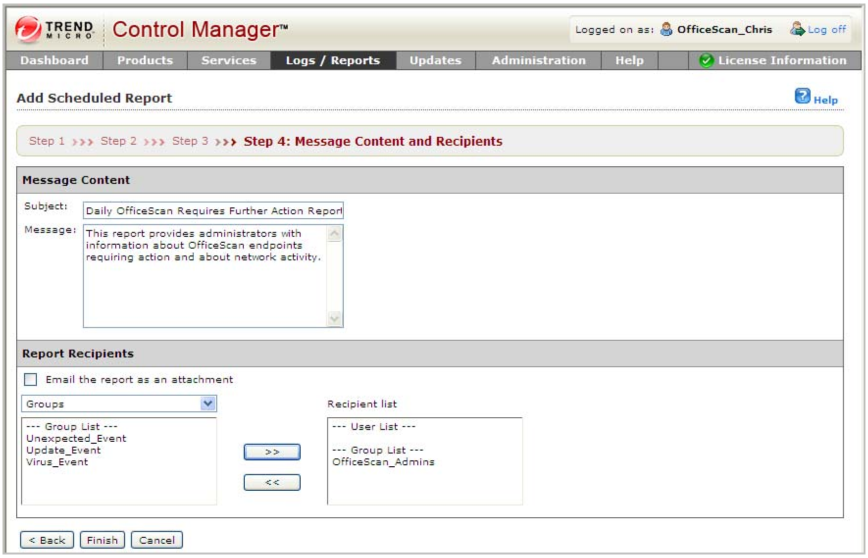
Start the schedule:

● Immediately
○ Start on: 08/07/2010 mm/dd/yyyy 00 hh : 34 mm

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.



Subject: Daily OfficeScan Requires Further Action Report

Message: This report provides administrators with information about OfficeScan endpoints requiring action and about network activity.

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 endpoints requiring action and about network activity.

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

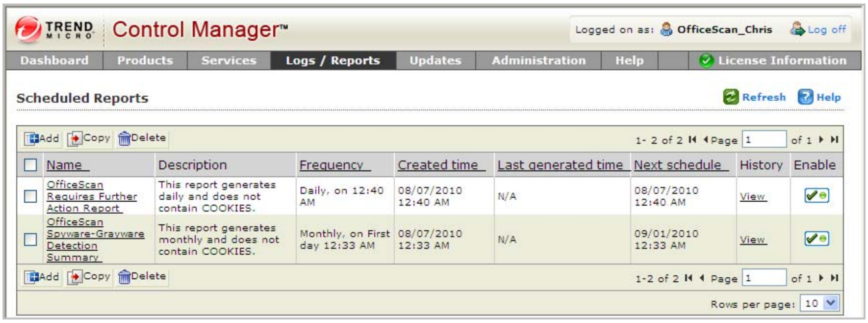
4. Add the following users to the **Report Recipients** list:

   Chris does not send this report to Dana because she is not an administrator.

   Groups:

   - **OfficeScan_Admins**

5. Click **Finish**. The Scheduled Reports screen appears with the report in the Scheduled Reports list.



Scheduled Reports

□	Name	Description	Frequency	Created time	Last generated time	Next schedule	History	Enable
□	OfficeScan Requires Further Action Report	This report generates daily and does not contain COOKIES.	Daily, on 12:40 AM	08/07/2010 12:40 AM	N/A	08/07/2010 12:40 AM	View	✓
□	OfficeScan Spyware-Grayware Detection Summary	This report generates monthly and does not contain COOKIES.	Monthly, on First day 12:33 AM	08/07/2010 12:33 AM	N/A	09/01/2010 12:33 AM	View	✓

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.

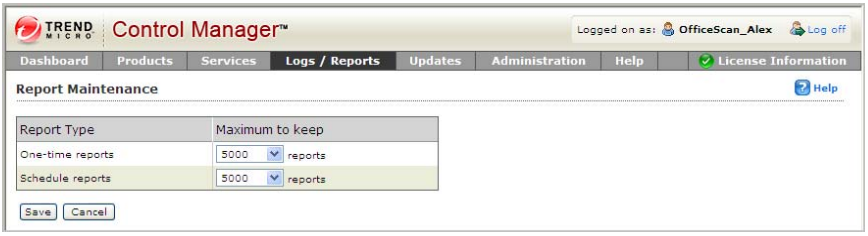
   c. Select the report to view from the History screen.

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.



Report Maintenance

Report Type	Maximum to keep
One-time reports	5000 reports
Schedule reports	5000 reports

5. Specify the following for **One-time reports** and **Scheduled reports**: **100000**
6. Click **Save**.

Chapter 5

Activating Managed Products

This chapter presents material administrators will need to activate or renew product licenses for Control Manager or managed products.

This chapter contains the following topics:

Activating and Registering Managed Products

To use the functionality of Control Manager 5.5, managed products (OfficeScan, ScanMail for Microsoft Exchange), 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. Use that key to register your software online to the Trend Micro Online Registration website 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 all the features of the software.

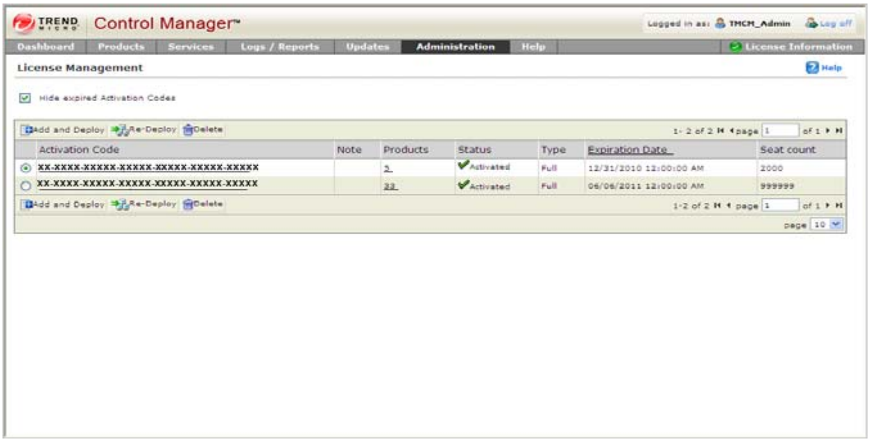
Activating Managed Products

Activating managed products allows you to use all the features for the product, 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:

Path: Administration > License Management > Managed Products

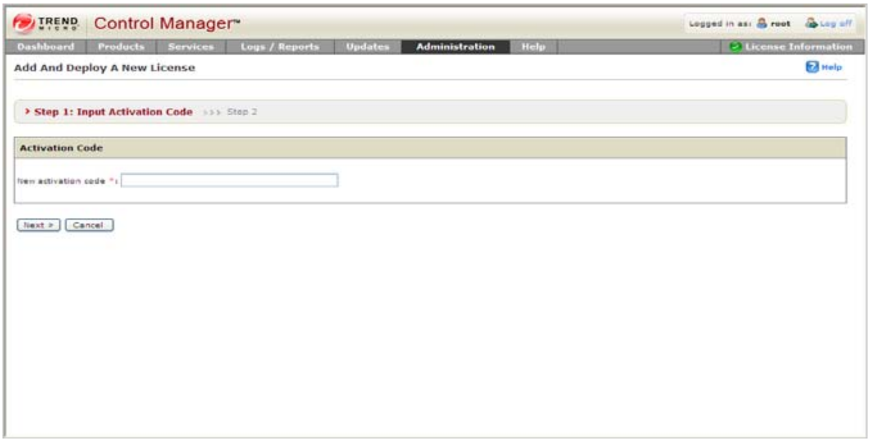
1. Navigate to the **License Management** screen.



☑ Hide expired Activation Codes

	Activation Code	Note	Products	Status	Type	Expiration Date	Seat count
●	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX		5	✓Activated	Full	12/31/2010 12:00:00 AM	2000
○	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX		33	✓Activated	Full	06/06/2011 12:00:00 AM	999999

2. Click **Add and Deploy**. The Step 1: Input Activation Code screen appears.



New activation code *:

3. Type an Activation Code for the product you want to activate in the New activation code field.

4. Click **Next**. The Step 2: Select Targets screen appears.

Note: If no products appear in the list, the selected Activation Code does not support any products currently registered to Control Manager. This could mean that the managed product does not support receiving Activation Codes from Control Manager servers.

5. Select the managed product to which to deploy the Activation Code.
6. Click **Finish**. The Managed Products License Management screen appears, with the new Activation Code listed in the table.

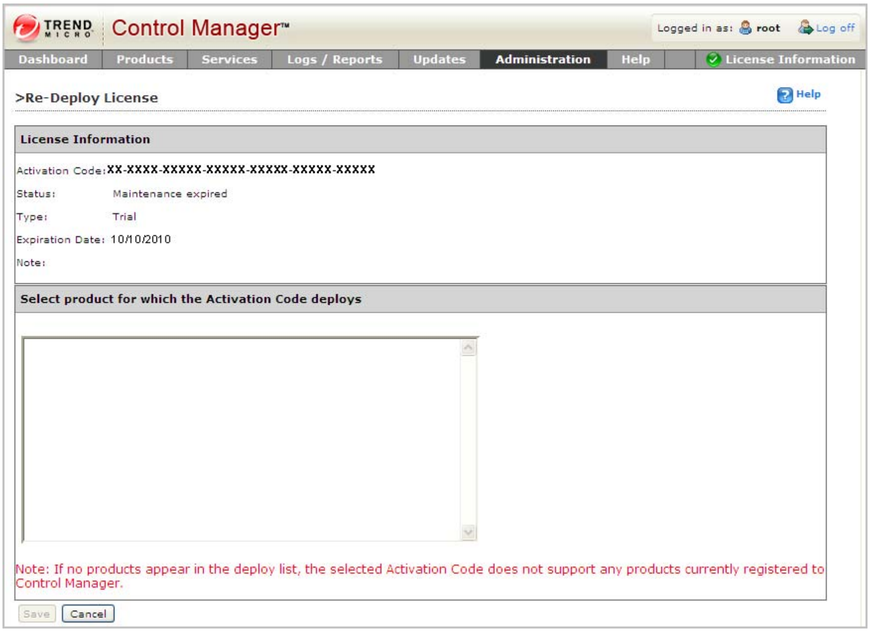
Renewing Managed Product Licenses

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:

Path: Administration > License Management > Managed Products

1. Navigate to the **License Management** screen.
2. Select an Activation Code from the list.
3. Click **Re-Deploy**. The Re-Deploy License screen appears.



>Re-Deploy License

License Information

Activation Code: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Status: Maintenance expired

Type: Trial

Expiration Date: 10/10/2010

Note:

Select product for which the Activation Code deploys

Note: If no products appear in the deploy list, the selected Activation Code does not support any products currently registered to Control Manager.

4. 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.
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

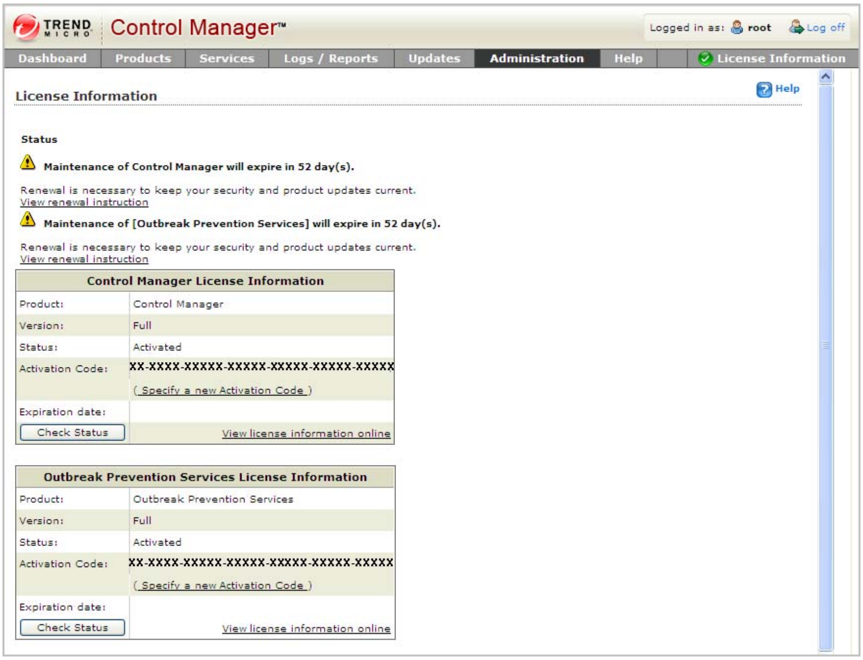
Activating Control Manager allows you to use all of the product's features, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Tip: After activating Control Manager, log off and then log on to the Control Manager web console for changes to take effect.

To register and activate Control Manager:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.



License Information

Status

Maintenance of Control Manager will expire in 52 day(s).

Renewal is necessary to keep your security and product updates current.
View renewal instruction

Maintenance of [Outbreak Prevention Services] will expire in 52 day(s).

Renewal is necessary to keep your security and product updates current.
View renewal instruction

Control Manager License Information	
Product:	Control Manager
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (Specify a new Activation Code)
Expiration date:	
Check Status	View license information online

Outbreak Prevention Services License Information	
Product:	Outbreak Prevention Services
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (Specify a new Activation Code)
Expiration date:	
Check Status	View license information online

2. On the working area under **Control Manager License Information**, click the **Activate the product** link.
3. Click the **Register online** link and follow the instructions on the Online Registration website.
4. In the **New box**, type your Activation Code.
5. Click **Activate**.
6. Click **OK**.

Renewing Maintenance for Control Manager or Managed Service

Renew maintenance for Control Manager or its integrated related products and services (Outbreak Prevention 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:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.
2. On the working area under the product or service to renew, click **Check Status**.
3. Click **OK**.

Note: Log off and then log on to the web console for changes to take effect.

To renew maintenance by manually entering an updated Activation Code:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.
2. 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 website).
3. In the **New box**, type your Activation Code.
4. Click **Activate**.
5. Click **OK**.

Note: Log off and then log on to the web console for changes to take effect.

Chapter 6

Managing Managed Products

This chapter presents material administrators need when managing the Control Manager network.

This chapter contains the following topics:

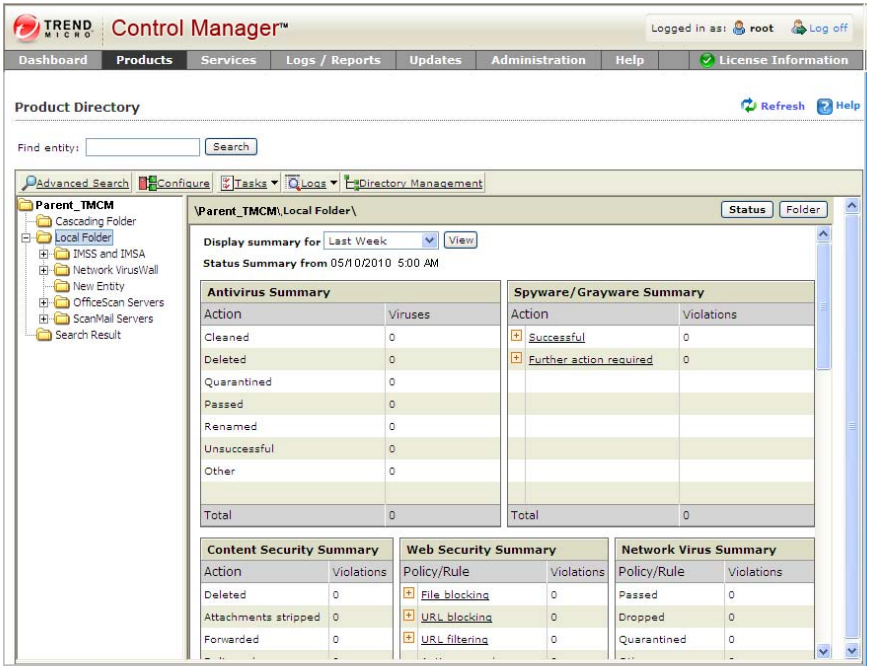
Manually Deploying Components Using the Product Directory

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 a specific managed product 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.



Display summary for Last Week

Status Summary from 05/10/2010 5:00 AM

Antivirus Summary

Action	Viruses
Cleaned	0
Deleted	0
Quarantined	0
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	0

Spyware/Grayware Summary

Action	Violations
Successful	0
Further action required	0
Total	0

Content Security Summary

Action	Violations
Deleted	0
Attachments stripped	0
Forwarded	0

Web Security Summary

Policy/Rule	Violations
File blocking	0
URL blocking	0
URL filtering	0

Network Virus Summary

Policy/Rule	Violations
Passed	0
Dropped	0
Quarantined	0

2. Select a managed product or directory from the Product Directory. The managed product or directory highlights.
3. Move the cursor over **Tasks** from the Product Directory menu.

4. Select **Deploy <component>** from the drop-down menu.
5. Click **Deploy Now** to start the manual deployment of new components.
6. Monitor the progress through the Command Tracking screen.
7. Click the **Command Details** link in the Command Tracking screen to view details for the Deploy Now task.

Viewing Managed Product's 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 the dashboard using the **Threat Detection Results** widget (found on the **Summary** tab)
- Through the Product Directory

To access through the dashboard

- Upon opening the Control Manager web console, the **Dashboard > Summary** tab displays the summary of the entire Control Manager network. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through the Product Directory:

1. Click **Products** on the main menu. The Product Directory screen appears.
2. From the Product Directory tree, 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 in the Display summary for list.

Configuring Managed Products

Depending on the product and agent version you can configure the managed product from the managed product's web console or through a Control Manager-generated console.

To configure a product:

1. Click **Products** on the main menu. The Product Directory screen appears.
2. Select the desired managed product from the Product Directory tree. The product status appears in the right-hand area of the screen.
3. Move the cursor over **Configure** in the Product Directory menu.
4. Select one of the following:

   Configuration Replication: The Configuration Settings screen appears.

   a. Select the folder to which the selected managed product’s settings replicate from the Product Directory tree.

   b. Click **Replicate**. The selected managed product’s settings replicate to the target managed products.

   <Managed Product Name> Single Sign On: The managed product’s web console or Control Manager-generated console appears.

   a. Configure the managed product from the web console.

Note: For additional information about configuring managed products, refer to the managed product's documentation.

Issuing Tasks to Managed Products

Use the Tasks menu item to invoke available actions to a 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 or 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. Click **Products** on the main menu. The Product Directory screen appears.
2. Select the managed product or directory to issue a task.
3. Mover the cursor over **Tasks**.
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.

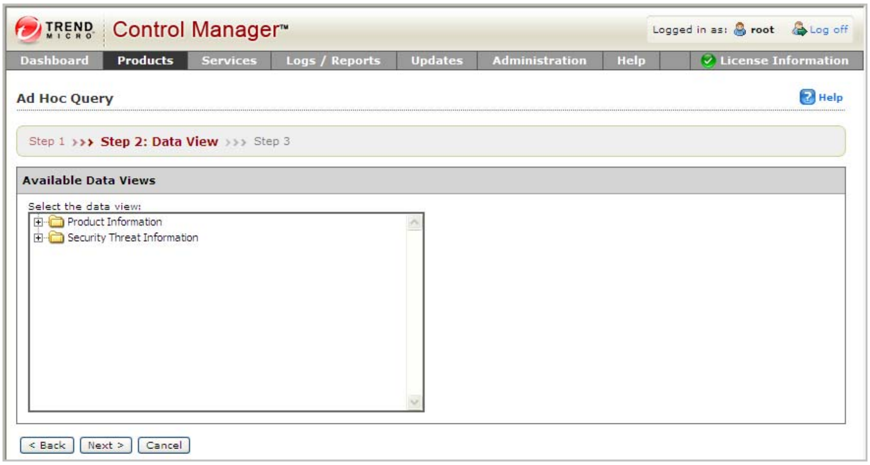
Querying and Viewing Managed Product Logs

Use the Logs tab to query and view logs for a group or a specific managed product.

To query and view managed product logs:

1. Click **Products** on the main menu. The Product Directory screen appears.
2. Select the desired managed product or folder from the Product Directory.
3. Move the cursor over **Logs** in the Product Directory menu.

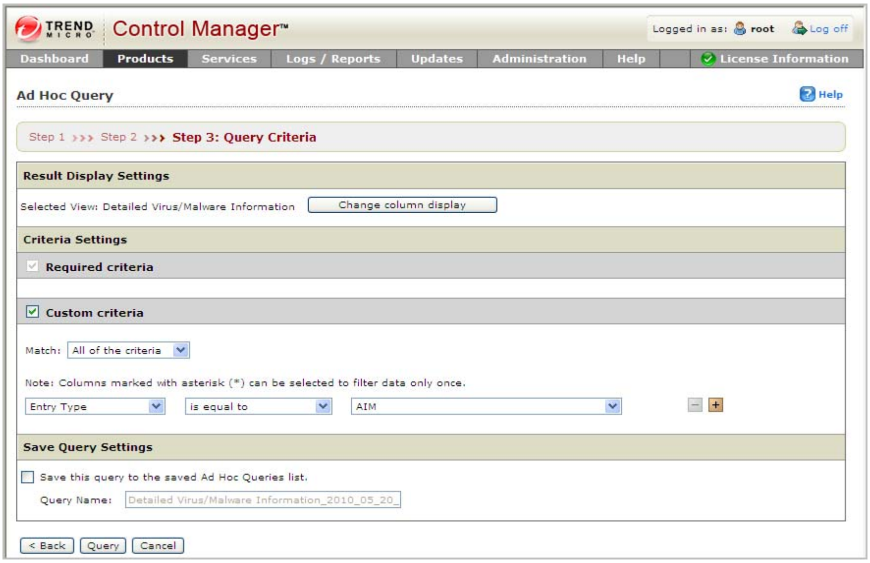
4. Click **Logs** from the drop-down menu. The Ad Hoc Query Step 2: Select Data View screen appears.



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 3: Query Criteria screen appears.



Ad Hoc Query

Step 1 >>> Step 2 >>> Step 3: Query Criteria

Result Display Settings

Selected View: Detailed Virus/Malware Information

Criteria Settings

☑ Required criteria

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Entry Type | is equal to | AIM

Save Query Settings

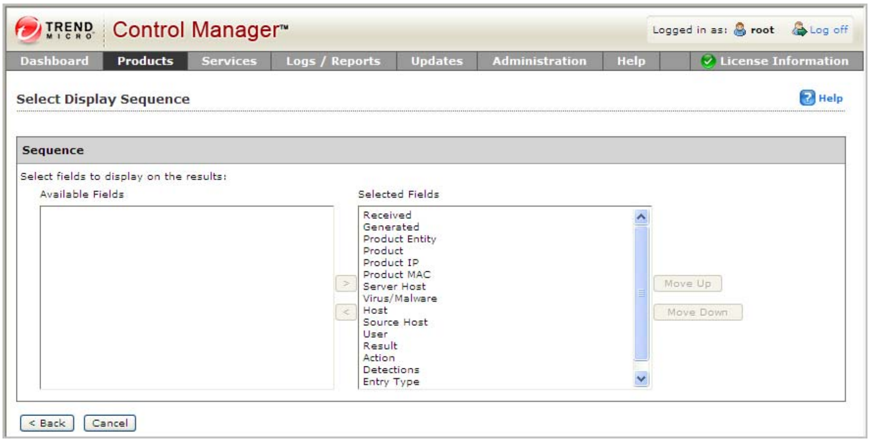
□ Save this query to the saved Ad Hoc Queries list.

Query Name: Detailed Virus/Malware Information_2010_05_20_

6. Specify the data to appear in the log and the order in which the data appears:

   Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.

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



Selected Fields:

Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type

b. Select a query column from the Available Fields list.

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.

7. Specify the filtering criteria for the data:

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

Required criteria:

- Specify a Summary Time for the data or whether you want COOKIES to appear in your reports.

Custom criteria:

a. Specify the criteria filtering rules for the data categories:

- **All of the criteria:** This selection acts as a logical AND function. Data appearing in the report must meet all the filtering criteria.
- **Any of the criteria:** This selection acts as a logical OR function. Data appearing in the report must meet any of the filtering criteria.

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

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

---

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.

10. To save the report as a CSV file:

a. Click **Export to CSV**.

b. Click **Save**.

c. Specify the location to save the file.

d. Click **Save**.

11. To save the report as an XML file:

a. Click **Export to XML**.

b. Click **Save**.

c. Specify the location to save the file.

d. Click **Save**.

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

---

12. To save the settings for the query:
    a. Click **Save query settings**.
    b. Type a name for the saved query in the **Query Name** field.
    c. Click **OK**. The saved query appears on the Saved Ad Hoc Queries screen.

Searching for Managed Products, Product Directory Folders, or Computers

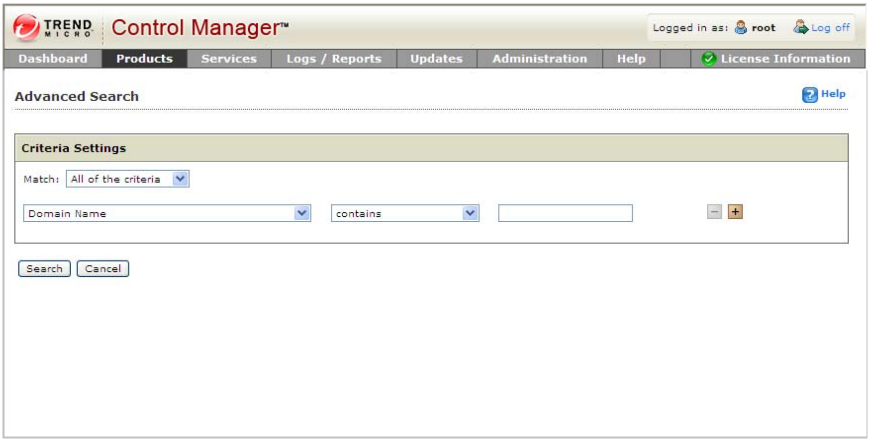
Use the Search button to quickly locate a specific managed product in the Product Directory.

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 your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
4. Click **Search** 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.

Chapter 7

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 2003 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 reinstall Control Manager on the server and retain all system information, such as agent registration, and user account data.

If you reinstalled 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 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 Server 2003**.

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)
- PHP
- FastCGI

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 computer, 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.

Remove 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, PHP, FastCGI, 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 Common CGI
- 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).

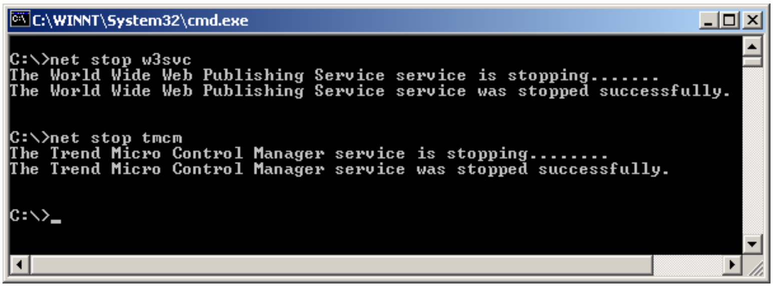
To stop Control Manager services:

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
```



```
C:\>net stop w3svc
The World Wide Web Publishing Service service is stopping.......
The World Wide Web Publishing Service service was stopped successfully.

C:\>net stop tmcm
The Trend Micro Control Manager service is stopping........
The Trend Micro Control Manager service was stopped successfully.

C:\>_
```

FIGURE 7-1. 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\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. On IIS 6 only:
   - **a.** Right-click the IIS website you set during installation.
   - **b.** Click **Properties**.
7. Click the **ISAPI Filters** tab.
8. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
9. 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

Removing Crystal Reports, PHP, FastCGI, TMI, and CCGI

Removal of PHP, FastCGI, TMI and CCGI is optional. Use Add/Remove Programs to uninstall Crystal Reports, PHP, and FastCGI.

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 PHP and FastCGI:

1. On Control Manager server, click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Scroll down to PHP, and then click **Remove** to remove PHP related files automatically.
3. Scroll down to FastCGI, and then click **Remove** to remove FastCGI related files automatically.

To remove TMI and CCGI:

1. Download the Microsoft service tool `Sc.exe` to the Control Manager server:

   http://support.microsoft.com/kb/251192/en-us
2. Run `Sc.exe` and type the following commands:

```
sc delete "TrendCGI"
sc delete "TrendMicro Infrastructure"
```

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`

- `...\PHP`
- `C:\Documents and Settings\All Users\Start Menu\Programs\PHP 5`
- `C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro Control Manager`

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 > 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 the website for Microsoft 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:

1. Download the Microsoft service tool `Sc.exe` to the Control Manager server:

   http://support.microsoft.com/kb/251192/en-us

2. Run `Sc.exe` and type the following commands:

```
sc delete "TMCM"
```

```
sc delete "TrendMicro_NTP"
```

Appendix A

Data Views

Database views are available to Control Manager 5 report templates and to Ad Hoc Query requests.

This appendix contains the following sections:

Understanding Data Views

Control Manager 5.5 allows direct queries to the Control Manager database. Data views are available to Control Manager 5 report templates and to Ad Hoc Query requests.

Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example the Virus/Malware Action/Result Summary has the following headings:

- Action Result
- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

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

TABLE A-1. Sample Data View

ACTION RESULT	ACTION TAKEN	UNIQUE ENDPOINTS	UNIQUE SOURCES	DETECTIONS

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

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

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. Product License Status Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Service	Displays the name of the managed product service. Example: 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.

TABLE A-3. Product License Status Data View

DATA	DESCRIPTION
Activation Codes	Displays the number of Activation Codes a managed products uses.
License Expiration	Displays the date the license expires for the managed product

Product License Information Summary

Displays detailed information about the Activation Code and information on managed products that use the Activation Code. Examples: seat count that the Activation Code allows, evaluation or full product version, user-defined description about the Activation Code

TABLE A-4. 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.
Products/Services	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
Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
License Expiration	Displays the date the license expires for the managed product
Seats	Displays the number of seats the Activation Code allows.

Detailed Product License Information

Displays information about the Activation Code and information on managed products that use the Activation Code. Examples: managed product information, evaluation or full product version, license expiration date

TABLE A-5. Detailed Product License Information Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Service	Displays the name of the managed service. Example: Web Reputation Service
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
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	Displays the date the license expires for the managed product.
Seats	Displays the number of seats the Activation Code allows.
Description	Displays the description for the Activation Code.

Managed Product Information

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. Product Distribution Summary Data View

DATA	DESCRIPTION
Registered to Control Manager	Displays the Control Manager server to which the managed product is registered.
Product Category	Displays the threat protection category for a managed product. Example: Server-based products, Desktop products
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Product Role	Displays the role the managed product has in the network environment. Example: server, client
Products	Displays the total number of a specific managed product a network contains.

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. Product Status Information Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product Host/Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The host name of a computer with a client (for example OfficeScan client) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with a client (for example OfficeScan client) installed.

TABLE A-7. Product Status Information Data View

DATA	DESCRIPTION
Managing Control Manager Entity	Displays the entity display name of the Control Manager server to which the managed product is registered.
Managing Server Entity	Displays the entity display name for a managed product to which an endpoint is registered. Control Manager identifies managed products using the managed product's entity display name.
Domain	Displays the domain to which the managed product belongs.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint client's connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Pattern Status	Displays the status of the pattern files/rules the managed product or a computer with a client (for example OfficeScan client) uses. Example: up-to-date, out-of-date
Engine Status	Displays the status of the scan engines the managed product or a computer with a client (for example OfficeScan client) uses. Example: up-to-date, out-of-date
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product client's version number. Example: OfficeScan **10.0**, Control Manager **5.0**

TABLE A-7. Product Status Information Data View

DATA	DESCRIPTION
Product Build	Displays the build number of the managed product. This information appears on the About screen for products. Example: Version: 5.0 (**Build 1219**)
Product Role	Displays the role the managed product or a computer with a client (for example OfficeScan client) has in the network environment. Example: server, client
Operating System	Displays the operating system of the computer where the managed product/agent installs.
OS Version	Displays the version number of the operating system of the computer where the managed product/agent installs.
OS Service Pack	Displays the service pack number of the operating system of the computer where the managed product/agent 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
Product Entity	Displays the entity display name for a managed product.
Domain	Displays the domain to which the managed product belongs.
Endpoints	Displays the number of endpoints in a domain.

TABLE A-8. ServerProtect and OfficeScan Server/Domain Status Summary Data View

DATA	DESCRIPTION
Patterns Out-of-Date	Displays the number of endpoints with out-of-date pattern files.
Patterns Up-to-Date Rate (%)	Displays the percentage of endpoints with up-to-date pattern files.
Engines Out-of-Date	Displays the number of endpoints with out-of-date scan engines.
Engines Up-to-Date Rate (%)	Displays the percentage of endpoints with up-to-date scan engines.

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. Product Event Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data about the managed product event.
Generated	Displays the time that the managed product generates data about the event.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**

TABLE A-9. Product Event Information Data View

DATA	DESCRIPTION
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

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. Engine Status Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.

TABLE A-10. Engine Status Data View

DATA	DESCRIPTION
Product Host/Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The host name of a computer with a client (for example OfficeScan client) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint client’s connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product client’s version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Product Role	Displays the role the managed product or a computer with a client (for example OfficeScan client) has in the network environment. Example: server, client
Engine	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine

TABLE A-10. Engine Status Data View

DATA	DESCRIPTION
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**
Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Engine Updated	Displays the time of the latest scan engine deployment to managed products or endpoints.

Pattern/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. Pattern/Rule Status Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product Host/Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The host name of a computer with a client (for example OfficeScan client) installed.

TABLE A-11. Pattern/Rule Status Data View

DATA	DESCRIPTION
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint client’s connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product client’s version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Product Role	Displays the role the managed product or a computer with a client (for example OfficeScan client) has in the network environment. Example: server, client
Pattern/Rule	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Pattern/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date

TABLE A-11. Pattern/Rule Status Data View

DATA	DESCRIPTION
Pattern/Rule Updated	Displays the time of the latest pattern file/rule deployment to managed products or endpoints.

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. Product Component Deployment Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their endpoints.
Pattern/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date
Pattern/Rule Deployment Status	Displays the deployment status for the latest pattern file/rule update. Example: successful, unsuccessful, in progress

TABLE A-12. Product Component Deployment Data View

DATA	DESCRIPTION
Pattern/Rule Deployment	Displays the time of the latest pattern file/rule deployment to managed products or endpoints.
Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Engine Deployment Status	Displays the deployment status for the latest scan update. Example: successful, unsuccessful, in progress
Engine Deployment	Displays the time of the latest scan engine deployment to managed products or endpoints.

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. Engine Status Summary Data View

DATA	DESCRIPTION
Engine	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit 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**
Up-to-Date	Displays the number of managed products with up-to-date scan engines.
Out-of-Date	Displays the number of managed products with out-of-date scan engines.

TABLE A-13. Engine Status Summary Data View

DATA	DESCRIPTION
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/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/Rule	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Up-to-Date	Displays the number of managed products with up-to-date pattern files or rules.
Out-of-Date	Displays the number of managed products with out-of-date pattern files or 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
Date/Time	Displays the time that the activity starts.
User	Displays the name of the user who initiates the activity.
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
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
Date/Time	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
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
Date/Time	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

TABLE A-17. Command Tracking Information Data View

DATA	DESCRIPTION
User	Displays the user who issued the command.
Updated	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
Date/Time	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
Product Entity	Displays the managed product to which the command was issued.
User	Displays the user who issued the command.

TABLE A-18. Detailed Command Tracking Information Data View

DATA	DESCRIPTION
Command Status	Displays the status of the command: successful, unsuccessful, in progress
Updated	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 endpoints 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	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Unique Endpoints	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. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2

TABLE A-19. Overall Virus/Malware Summary Data View

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

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 Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1.
Unique Endpoints	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. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2

TABLE A-20. Overall Virus/Malware Type Summary Data View

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware 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 Source Summary Data View

DATA	DESCRIPTION
Source Host	Displays the IP address or host name of the computer where viruses/malware originate.
Unique Endpoints	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. Unique Detections = 3
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

TABLE A-21. Virus/Malware Source Summary Data View

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware Endpoint Summary

Provides a summary of virus/malware detections from specific endpoints. Example: name of endpoint, number of specific virus/malware instances on the endpoint, total number of instances of viruses/malware on the network

TABLE A-22. Virus/Malware Endpoint Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of the computer affected by viruses/malware.
Unique Sources	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. Unique Sources = 2
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1

TABLE A-22. Virus/Malware Endpoint Summary Data View

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

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 endpoints 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
Date/Time	Displays the time that the summary of the data occurs.
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1
Unique Endpoints	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. Unique Endpoints = 3

TABLE A-23. Virus/Malware Detections Over Time Summary Data View

DATA	DESCRIPTION
Unique Sources	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. Unique Sources = 2
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

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
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE A-24. Virus/Malware Action/Result Summary Data View

DATA	DESCRIPTION
Unique Endpoints	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. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Detailed Information

Detailed 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 endpoint with viruses/malware

TABLE A-25. Detailed Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

TABLE A-25. Detailed Virus/Malware Information Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with a client (for example OfficeScan client) installed.
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE

TABLE A-25. Detailed Virus/Malware Information Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of the computer affected by viruses/malware.
Source	Displays the IP address or host name of the computer where viruses/malware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections =10
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

Endpoint Virus/Malware Information

Provides specific information about the virus/malware instances found on endpoints. Example: the managed product that detects the viruses/malware, the type of scan that detects the virus/malware, the file path on the endpoint to detected viruses/malware

TABLE A-26. Endpoint Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.

TABLE A-26. Endpoint Virus/Malware Information Data View

DATA	DESCRIPTION
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Endpoint	Displays the name of the computer affected by viruses/malware.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Scan Type	Displays the type of scan the managed product uses to detect the virus/malware. Example: Real-time, scheduled, manual
File	Displays the name of the file managed products detect affected by viruses/malware.
File Path	Displays the file path on the endpoint computer where managed products detect the virus/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Web Virus/Malware 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 endpoint that downloads the virus/malware.

TABLE A-27. Web Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Endpoint	Displays the IP address or host name of the computer on which managed products detect viruses/malware.
Source URL	Displays the URL of the web/FTP site which the virus/malware originates.

TABLE A-27. Web Virus/Malware Information Data View

DATA	DESCRIPTION
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Traffic/Connection	Displays the direction of virus/malware entry.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the viruses/malware originates.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Email Virus/Malware 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. Email Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

TABLE A-28. Email Virus/Malware Information Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Recipient	Displays the recipient of the email message containing viruses/malware.
Sender	Displays the sender of email message containing viruses/malware.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Subject	Displays the content of the subject line of the email message containing viruses/malware.
File	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.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE A-28. Email Virus/Malware Information Data View

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Network Virus/Malware 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. Network Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE A-29. Network Virus/Malware Information Data View

DATA	DESCRIPTION
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Endpoint	Displays the IP address/ host name of the computer affected by viruses/malware.
Source Host	Displays the IP address or host name of the computer where viruses/malware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
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
Endpoint Computer	Displays the computer name of the computer affected by viruses/malware.
Endpoint Port	Displays the port number of the computer affected by viruses/malware.
Endpoint MAC	Displays the MAC address of the computer affected by viruses/malware.
Source Computer	Displays the computer name of the computer where viruses/malware originates.
Source Port	Displays the port number of the computer where viruses/malware originates.
Source MAC	Displays the MAC address of the computer where viruses/malware originates.
File	Displays the name of the file managed products detect affected by viruses/malware.

TABLE A-29. Network Virus/Malware Information Data View

DATA	DESCRIPTION
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Spyware/Grayware Information

Summary Information

Overall Spyware/Grayware Summary

Provides overall specific summary for spyware/grayware detections. Example: name of spyware/grayware, number of endpoints 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	Displays the name of spyware/grayware managed products detect.

TABLE A-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Unique Endpoints	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. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2
Detections	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
Source Host	Displays the name of the computer where spyware/grayware originates.

TABLE A-31. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Detections	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. Unique Detections = 1
Detections	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. Detections = 10

Endpoint Spyware/Grayware Summary

Provides a summary of spyware/grayware detections from specific endpoints. Example: name of endpoint, number of specific spyware/grayware instances on the endpoint, total number of instances of spyware/grayware on the network

TABLE A-32. Endpoint Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the host name or IP address of the computer affected by spyware/grayware.

TABLE A-32. Endpoint Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Unique Sources	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. Unique Sources = 2
Unique Detections	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. Unique Detections = 1
Detections	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. Detections = 10

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 was collected, number of endpoints 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
Date/Time	Displays the time that the summary of the data occurs.

TABLE A-33. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Detections	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. Unique Detections = 1
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2
Detections	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. Detections = 10

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
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Sources	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. Unique Sources = 2
Detections	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. Detections = 10

Detailed Information

Detailed 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 endpoint with spyware/grayware

TABLE A-35. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.

TABLE A-35. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Endpoint	Displays the IPaddress or host name of the computer affected by spyware/grayware.
Source Host	Displays the IPaddress or host name of the computer where spyware/grayware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	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. Detections = 10

TABLE A-35. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
Entry Type	Displays the entry point for the spyware/grayware 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

Endpoint Spyware/Grayware

Provides specific information about the spyware/grayware instances found on endpoints. Example: the managed product that detects the spyware/grayware, the type of scan that detects the spyware/grayware, the file path on the endpoint to detected spyware/grayware

TABLE A-36. Endpoint Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

TABLE A-36. Endpoint Spyware/Grayware Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Endpoint	Displays the IPaddress or host name of the computer affected by spyware/grayware.
Source Host	Displays the IPaddress or host name of the computer where the spyware/grayware originates.

TABLE A-36. Endpoint Spyware/Grayware Data View

DATA	DESCRIPTION
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Scan Type	Displays the type of scan the managed product uses to detect the spyware/grayware. Example: Real-time, scheduled, manual
Resource	Displays the specific resource affected. Example: application.exe, H Key Local Machine\SOFTWARE\ACME
Resource Type	Displays the type of resource affected by spyware/grayware. Example: registry, memory resource
Security Threat Type	Displays the specific type of spyware/grayware managed products detect. Example: adware, COOKIE, peer-to-peer application
Risk Level	Displays the Trend Micro-defined level of risk the spyware/grayware poses to your network. Example: High security, Medium security, Low security
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted

Web Spyware/Grayware

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 endpoint that downloads the spyware/grayware

TABLE A-37. Web Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Endpoint	Displays the IP address or 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.

TABLE A-37. Web Spyware/Grayware Data View

DATA	DESCRIPTION
Traffic/Connection	Displays the direction of spyware/grayware entry.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the spyware/grayware originates.
User	Displays the user name logged on to the end-point computer when a managed product detects spyware/grayware.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	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. Detections = 10

Email Spyware/Grayware

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. Email Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Recipient	Displays the recipient of the email message containing spyware/grayware.
Sender	Displays the sender of email message containing spyware/grayware.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Subject	Displays the content of the subject line of the email message containing spyware/grayware.
File	Displays the name of the file managed products detect affected by spyware/grayware.

TABLE A-38. Email Spyware/Grayware Data View

DATA	DESCRIPTION
File in Compressed File	Displays the file name of the spyware/grayware occurring in a compressed file.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	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. Detections = 10

Network Spyware/Grayware

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. Network Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

TABLE A-39. Network Spyware/Grayware Data View

DATA	DESCRIPTION
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
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
Endpoint IP	Displays the IP address of the computer affected by spyware/grayware.
Endpoint	Displays the IP address or host name of the computer affected by spyware/grayware.
Endpoint Port	Displays the port number of the computer affected by spyware/grayware.
Endpoint MAC	Displays the MAC address of the computer affected by spyware/grayware.
Source IP	Displays the IP address of the computer where spyware/grayware originates.
Source Host	Displays the host name of the computer where spyware/grayware originates.

TABLE A-39. Network Spyware/Grayware Data View

DATA	DESCRIPTION
Source Port	Displays the port number of the computer where spyware/grayware originates.
Source MAC	Displays the MAC address of the computer where spyware/grayware originates.
User	Displays the user name logged on to the end-point computer when a managed product detects spyware/grayware.
File	Displays the name of the file managed products detect affected by spyware/grayware.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	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. Detections = 10

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	Displays the name of the policy that endpoints violate.
Filter Type	Displays the type of filter that triggers the violation. Example: content filter, phishing filter, URL reputation filter
Unique Senders/Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3
Unique Recipients	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. Unique Recipients = 2

TABLE A-40. Content Violation Policy Summary Data View

DATA	DESCRIPTION
Detections	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. Detections = 10

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
Sender/User	Displays the email message address or users sending content that violates managed product policies.
Detections	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. Detections = 10
Unique Recipients	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. Unique Recipients = 2

TABLE A-41. Content Violation Sender Summary Data View

DATA	DESCRIPTION
Unique Policies	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. Detections = 10

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 was collected, number of endpoints 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
Date/Time	Displays the time that the summary of the data occurs.
Unique Policies	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. Detections = 10
Unique Senders/Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3

TABLE A-42. Content Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Recipients	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. Unique Recipients = 2
Detections	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. Detections = 10

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	Displays the type of action managed products take against email message in violation of content policies. Example: forwarded, attachments stripped, deleted
Detections	Displays the number of violations with the specified action taken by managed products.

Detailed Information

Detailed 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 Content Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	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/User	Displays the email address or user sending content that violates managed product policies.
Subject	Displays the content of the subject line of the email that violates a policy.
Policy	Displays the name of the policy an email violates.
Policy Settings	Displays the settings for the policy that an email violates.
File Location	Displays the location of the file that violates a policy.

TABLE A-44. Detailed Content Violation Information Data View

DATA	DESCRIPTION
File	Displays the name of the file that violates a policy.
URL	Displays the URL in violation of the specified policy.
Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security
Filter Type	Displays the type of filter that detects the email in violation. Example: content filter, size filter, attachment filter
Filter Action	Displays the action the detecting filter takes against email in violation of a policy. Example: clean, quarantine, strip
Action	Displays the type of action managed products take against email in violation of content policies. Example: deliver, strip, forward
Detections	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 endpoints 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 Recipients	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. Unique Recipients = 3
Detections	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. Detections = 10

Spam Recipient Summary

Provides a summary of spam violations on specific endpoints. Example: name of endpoint, total number of instances of viruses/malware on the endpoint

TABLE A-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Recipient	Displays the name of the recipient who receives spam.
Detections	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. Detections = 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 was collected, number of endpoints 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 Domains	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. Unique Recipient Domains = 1

TABLE A-47. Spam Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Recipients	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. Unique Recipients = 3
Detections	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. Detections = 10

Detailed Information

Detailed 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 Spam Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE A-48. Detailed Spam Information Data View

DATA	DESCRIPTION
Product	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.
Subject	Displays the content of the subject line of the email containing spam.
Policy	Displays the name of the policy the email violates.
Action	Displays the type of action managed products take against spam found in email. Example: deliver, forward, strip
Detections	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. Detections = 10

Spam Connection Information

Provides specific information about the source of spam 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
Received	Displays the time that Control Manager receives data from the managed product.

TABLE A-49. Spam Connection Information Data View

DATA	DESCRIPTION
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Source IP	Displays the IP address of the mail server where spam originates.
Filter Type	Displays the type of filter that detects the email in violation. Example: Real-time Blackhole List (RBL+), Quick IP List (QIL)
Action	Displays the type of action managed products take against spam to prevent spam from entering the email server. Example: drop connection, bypass connection
Detections	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. Detections = 10

Policy/Rule Violation Information

Detailed Information

Detailed Firewall 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 Firewall Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with a client (for example OfficeScan client) installed, that is under attack.
Product	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
Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security

TABLE A-50. Detailed Firewall Violation Information Data View

DATA	DESCRIPTION
Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol the intrusion uses. Example: HTTP, SMTP, FTP
Source IP	Displays the IP address of the computer attempting an intrusion on your network.
Endpoint Port	Displays the port number of the computer under attack.
Endpoint IP	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	Displays the type of action managed products take against policy violations. Example: file cleaned, file quarantined, file passed
Detections	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. Detections = 10

Detailed 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 Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Endpoint	Displays the host name of the computer in violation of the policy/rule.
Endpoint IP	Displays the IP address of the computer in violation of the policy/rule.
Endpoint MAC	Displays the MAC address of the computer in violation of the policy/rule.
Policy/Rule	Displays the name of the policy/rule in violation.
Service	Displays the name of the service/program in violation of the policy/rule.
User	Displays the user name logged on to the endpoint when a managed product detects a policy/rule violation.

TABLE A-51. Detailed Endpoint Security Violation Information Data View

DATA	DESCRIPTION
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.
Detections	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. Detections = 10

Detailed 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 Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

TABLE A-52. Detailed Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Endpoint IP	Displays the IP address of the computer in compliance of the policy/rule.
Endpoint MAC	Displays the MAC address of the computer in compliance of the policy/rule.
Policy/Rule	Displays the name of the policy/rule in compliance.
Service	Displays the name of the service/program in compliance of the policy/rule.
User	Displays the user name logged on to the endpoint when a managed product detects a policy/rule compliance.
Description	Detailed description of the incident by Trend Micro.
Detections	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. Detections = 10

Detailed Application Activity

Displays overall information about application activity on your network. Example: the managed product which detects the security compliance, the name of the specific policy in compliance, the total number of security compliances on the network

TABLE A-53. Detailed Application Activity Data View

DATA	DESCRIPTION
Received	The time at which Control Manager receives data from the managed product.
Generated	The time at which the managed product generates data.
Product Entity	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	The name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Displays the VLAN ID (VID) of the source from which the suspicious threat originates.
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
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-53. Detailed Application Activity Data View

DATA	DESCRIPTION
Description	Detailed description of the incident by Trend Micro.
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Source IP	Displays the IP address of the source from which the suspicious threat originates.
Source MAC	Displays the MAC address of the source from which the suspicious threat originates.
Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group	Displays the IP address group of the source where the violation originates.
Source Network Zone	Displays the network zone of the source where the violation originates.
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.
Endpoint Port	Displays the port number of the endpoint the suspicious threat affects.
Endpoint MAC	Displays the MAC address of the endpoint the suspicious threat affects.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.
Policy/Rule	Displays the policy/rule the suspicious threat violates.

TABLE A-53. Detailed Application Activity Data View

DATA	DESCRIPTION
Detections	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. Detections = 10

Web Violation/Reputation 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-54. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Policy	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 Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4

TABLE A-54. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Unique URLs	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. Unique URLs = 1
Detections	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. Detections = 10

Web Violation Endpoint Summary

Provides a summary of web violation detections from a specific endpoint. Example: IP address of the endpoint in violation, number of policies in violation, the total number of web violations on the network

TABLE A-55. Web Violation Endpoint Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of endpoints in violation of web policies.
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1

TABLE A-55. Web Violation Endpoint Summary Data View

DATA	DESCRIPTION
Unique URLs	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. Unique URLs = 1
Detections	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. Detections = 10

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-56. Web Violation URL Summary Data View

DATA	DESCRIPTION
URL	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 Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4

TABLE A-56. Web Violation URL Summary Data View

DATA	DESCRIPTION
Detections	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. Detections = 10

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-57. 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
Detections	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. Detections = 10

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 was collected, number of endpoints in violation, the total number of web violations on the network

TABLE A-58. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4
Unique URLs	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. Unique URLs = 1
Detections	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. Detections = 10

Web Violation Detection Summary

Provides a summary of web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints in violation, the total number of web violations on the network

TABLE A-59. Web Violation Detection Summary Data View

DATA	DESCRIPTION
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4
Unique URLs	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. Unique URLs = 1
Unique Users/IPs	Displays the number of unique users or IP addresses of endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL from one user. Unique Users/IPs = 1

TABLE A-59. Web Violation Detection Summary Data View

DATA	DESCRIPTION
Unique User Groups	Displays the number of unique user groups for users in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL from one user group. Unique User Groups = 1
Detections	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. Detections = 10

Detailed Information

Detailed 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-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE A-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
URL	Displays the name of the URL that violates a web policy.
User/IP	Displays the user or IP address of the end-point that violates a policy.
User Group	Displays the user group for the user that violates a policy.
Endpoint	Displays the IP address or host name of the endpoint that violates a policy.
Product Host	Displays the IP address or host name of the managed product which detects the violation.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, web blocking
Blocking Rule	Displays the blocking rule preventing access to the URL in violation. Example: URL blocking
Policy	Displays the name of the policy the URL violates.
File	Displays the name of the file that violates the policy.
Web Reputation Rating	Displays the relative safety, as a percentage, of a website according to Trend Micro.

TABLE A-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
Action	Displays the type of action managed products take against policy violations. Example: pass, block
Detections	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. Detections = 10

Detailed Web Reputation Information

Displays overall information about application activity 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-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
Received	The time at which Control Manager receives data from the managed product.
Generated	The time at which the managed product generates data.
Product Entity	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	The name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Displays the VLAN ID (VID) of the source from which the suspicious threat originates.

TABLE A-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
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
Description	Detailed description of the incident by Trend Micro.
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Source IP	Displays the IP address of the source from which the suspicious threat originates.
Source MAC	Displays the MAC address of the source from which the suspicious threat originates.
Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group	Displays the IP address group of the source where the suspicious threat originates.
Source Network Zone	Displays the network zone of the source where the suspicious threat originates.
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.
Endpoint Port	Displays the port number of the endpoint the suspicious threat affects.

TABLE A-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
Endpoint MAC	Displays the MAC address of the endpoint the suspicious threat affects.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.
Policy/Rule	Displays the policy/rule the suspicious threat violates.
URL	Displays the URL considered a suspicious threat.
Detections	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. Detections = 10

Suspicious Threat Information

Summary Information

Overall Suspicious Threat Summary

Provides specific information about suspicious threats on your network. Example: the policy/rule in violation, summary information about the source and destination, the total number of suspicious threats on the network

TABLE A-62. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Policy/Rule	Displays the name of the policy/rule in violation.

TABLE A-62. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
Unique Endpoints	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. Unique Endpoints = 2
Unique Sources	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. Unique Sources = 3
Unique Recipients	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. Unique Recipients = 2
Unique Senders	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. Unique Senders = 3

TABLE A-62. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Detections	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. Detections equals 10.
Mitigations	Displays the number of endpoints Network VirusWall Enforcer devices or Total Discovery Mitigation Server take action against.
Cleaned Endpoints	Displays the total number of endpoints Total Discovery Mitigation Server cleans.
Clean Endpoint Rate (%)	Displays the percentage of endpoints Total Discovery Mitigation Server cleans compared to the total Detections.

Suspicious 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-63. Suspicious Source Summary Data View

DATA	DESCRIPTION
Source IP	Displays the IP addresses of sources where suspicious threats originate.
Unique Policies/Rules	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. Unique Policies/Rules = 1

TABLE A-63. Suspicious Source Summary Data View

DATA	DESCRIPTION
Unique Endpoints	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. Unique Endpoints = 2
Detections	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. Detections = 10

Suspicious Riskiest Endpoints Summary

Provides a summary of the endpoints 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-64. Suspicious Threat Riskiest Endpoints Summary Data View

DATA	DESCRIPTION
Endpoint IP	Displays the IP addresses of computers affected by suspicious threats.
Unique Policies/Rules	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. Unique Policies/Rules = 1

TABLE A-64. Suspicious Threat Riskiest Endpoints Summary Data View

DATA	DESCRIPTION
Unique Sources	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. Unique Sources = 3
Detections	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. Detections = 10

Suspicious 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-65. Suspicious Riskiest Recipient Summary Data View

DATA	DESCRIPTION
Recipient	Displays the email address of the recipient affected by the suspicious threat.
Unique Policies/Rules	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. Unique Policies/Rules = 1

TABLE A-65. Suspicious Riskiest Recipient Summary Data View

DATA	DESCRIPTION
Unique Senders	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. Unique Senders = 3
Detections	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. Detections = 10

Suspicious 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-66. Suspicious Sender Summary Data View

DATA	DESCRIPTION
Sender	Displays the email address for the source of policy/rule violations.
Unique Policies/Rules	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. Unique Policies/Rules = 1

TABLE A-66. Suspicious Sender Summary Data View

DATA	DESCRIPTION
Unique Recipients	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. Unique Recipients = 2
Detections	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. Detections = 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-67. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Protocol	Displays the name of the protocol over which the suspicious threat occurs. Example: HTTP, FTP, SMTP
Unique Policies/Rules	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. Unique Policies/Rules = 1

TABLE A-67. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Unique Endpoints	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. Unique Endpoints = 2
Unique Sources	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. Unique Sources = 3
Unique Recipients	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. Unique Recipients = 2
Unique Senders	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. Unique Senders = 3
Detections	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. Detections = 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 was collected, summary information about the source and destination, the total number of suspicious threats on the network

TABLE A-68. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
Unique Policies/Rules	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. Unique Policies/Rules = 1
Unique Endpoints	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. Unique Endpoints = 2
Unique Sources	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. Unique Sources = 3

TABLE A-68. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Recipients	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. Unique Recipients = 2
Unique Senders	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. Unique Senders = 3
Detections	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. Detections = 10

Detailed Information

Detailed 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-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Mitigation Host	Displays the host name for the mitigation server.
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
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.

TABLE A-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
Endpoint Port	Displays the port number of the endpoint the suspicious threat affects.
Endpoint MAC	Displays the MAC address of the endpoint the suspicious threat affects.
Source IP	Displays the IP address of the source where the suspicious threat originates.
Source Host	Displays the host name of the source where the suspicious threat originates.
Source Port	Displays the port number of the source where the suspicious threat originates.
Source MAC	Displays the MAC address of the source where the suspicious threat originates.
Source Domain	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.
Security Threat Type	Displays the specific type of security threat 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	Displays the policy/rule the suspicious threat violates.
Recipient	Displays the recipient of the suspicious threat.
Sender	Displays the sender of the suspicious threat.
Subject	Displays the content of the subject line of the email containing spyware/grayware.

TABLE A-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
URL	Displays the URL considered a suspicious threat.
User	Displays the user name logged on to the destination when a managed product detects a suspicious threat.
IM/IRC User	Displays the instant messaging or IRC user name logged on when Total Discovery Appliance detects a violation.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the suspicious threat originates.
Channel Name	Displays the protocol that the instant messaging software or IRC use for communication.
File	Displays the name of the suspicious file.
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.
Constraint Type	Displays the reason that a file cannot be scanned correctly.

TABLE A-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
Mitigation Result	Displays the result of the action the mitigation server takes against suspicious threats.
Mitigation Action	Displays the action the mitigation server takes against suspicious threats. Example: File cleaned, File dropped, File deleted
Source IP Group	Displays the IP address group of the source where the suspicious threat originates.
Source Network Zone	Displays the network zone of the source where the suspicious threat originates.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.
Detections	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. Detections = 10

Overall Threat Information

Network Security Threat Analysis Information

Displays information for overall security threats affecting your desktops. Examples: name of the security threat, total number of security threat detections, number of endpoints affected

TABLE A-70. Network Security Threat Analysis Information Data View

DATA	DESCRIPTION
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Security Threat	Displays the name of security threat managed products detect.
Entry Type	Displays the entry point for the security threat that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique computers where security threats/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3

TABLE A-70. Network Security Threat Analysis Information Data View

DATA	DESCRIPTION
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Network Protection Boundary Information

Displays information for a broad overview of security threats affecting your entire network. Examples: managed product network protection type (gateway, email), type of security threat, number of endpoints affected

TABLE A-71. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Product Category	Displays the category to which the managed product belongs. Example: desktop products, mail server products, network products
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2

TABLE A-71. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Unique Sources	Displays the number of unique computers where security threats/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Security Threat Entry Analysis Information

Displays information with the entry point of security threats as the focus. Examples: managed product network protection type (gateway, email, desktop), name of the security threat, time of the last security threat detection

TABLE A-72. Security Threat Entry Analysis Information Data View

DATA	DESCRIPTION
Entry Type	Displays the point of entry for security threats managed products detect. Example: Virus found in file, FTP, File transfer
Product	Displays the name of the managed product which detects the security threat. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE A-72. Security Threat Entry Analysis Information Data View

DATA	DESCRIPTION
Security Threat Category	Displays the specific category for security threats managed products detect. Example: Antivirus, Antispyware, Content filtering
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique computers where security threats/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Security Threat Endpoint Analysis Information

Displays information with affected endpoints as the focus. Examples: name of the endpoint, the broad range of how the security threat enters your network, number of endpoints affected

TABLE A-73. Security Threat Endpoint Analysis Information Data View

DATA	DESCRIPTION
Endpoint	Displays the name of the computer affected by the security threat/violation.

TABLE A-73. Security Threat Endpoint Analysis Information Data View

DATA	DESCRIPTION
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Security Threat Name	Displays the name of security threat managed products detect.
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10
Detected	Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.

Security Threat Source Analysis Information

Displays information with the security threat source as the focus. Examples: name of the security threat source, the broad range of how the security threat enters your network, number of endpoints affected

TABLE A-74. Security Threat Source Analysis Information Data View

DATA	DESCRIPTION
Source Host	Displays the name of the computer where the cause of the security threat/violation originates.
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Security Threat	Displays the name of security threat managed products detect.

TABLE A-74. Security Threat Source Analysis Information Data View

DATA	DESCRIPTION
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10
Detected	Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.

Index