## Preface
- Who Should Use This Guide? .......................................................... 10
- More Information ........................................................................ 10
- Feedback ...................................................................................... 10

## Chapter 1
**Introduction**
- Overview ..................................................................................... 12
- Administration Console .............................................................. 12
- Features ....................................................................................... 13
- Removable Media Manager ......................................................... 13
- Encryption Policy Manager ......................................................... 13
- Device Manager .......................................................................... 14
- DataScan .................................................................................... 14
- Program Security Guard ............................................................ 14
- Auditing and Alerts ..................................................................... 15
- Licensing Model .......................................................................... 15
- Additional Information ............................................................... 16

## Chapter 2
**Getting Started**
- Introducing the Administration Console ..................................... 18
- Administration Console User Interface ...................................... 18
- Launching the Administration Console ....................................... 21
- First Steps after Installation ....................................................... 22
- Connecting to a Remote or Local Server .................................... 23
- Configuring Media Encryption Server ......................................... 25
  - Media Encryption Server Properties ....................................... 25
  - General Properties Tab ......................................................... 26
  - Applications Tab .................................................................. 28
  - Security Tab ......................................................................... 38
  - Email Configuration Tab ...................................................... 42
  - Console Settings Tab ......................................................... 43
  - Server Key Tab .................................................................. 44
- Configuring Removable Media Manager ..................................... 45
- Recovering EPM Passwords ....................................................... 47
Chapter 3  Working with Profiles
Overview ........................................................................................................ 50
The Default Profile.................................................................................. 50
Profile Priority and Inheritance............................................................... 50
Profile Templates................................................................................ 51
Working with Profile Templates ................................................................. 51
Overview ................................................................................................... 52
Defining Profiles................................................................................... 52
General Settings................................................................................... 54
Device Manager Settings...................................................................... 55
Removable Media Manager Settings ....................................................... 58
Encryption Settings............................................................................... 61
Auditing Settings.................................................................................. 67
Program Security Guard Settings............................................................ 76
User Interface Tab ................................................................................ 81
Advanced Tab....................................................................................... 83
Exporting Profile Templates ...................................................................... 86

Chapter 4  Users and User Groups
Working with Users .................................................................................. 92
Working with User Groups ......................................................................... 95
Working with Existing Group Settings.................................................... 103
Working with Group Synchronization..................................................... 105

Chapter 5  Computers and Computer Groups
Working with Computers ......................................................................... 110
Computers View.................................................................................. 110
Filtering the Computer List .................................................................. 112
Working with Computer Settings........................................................... 112
Working with Computer Groups ............................................................... 115
Creating a New Computer Group........................................................... 116
Adding Computers to a Group .............................................................. 118
Working with Computer Group Properties .............................................. 119
<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Monitoring and Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts</td>
<td>................................................................. 124</td>
</tr>
<tr>
<td>Creating a New Alert</td>
<td>.............................................................. 124</td>
</tr>
<tr>
<td>Logs</td>
<td>................................................................. 126</td>
</tr>
<tr>
<td>Filtering the Log</td>
<td>............................................................. 129</td>
</tr>
<tr>
<td>Exporting Logs</td>
<td>............................................................ 129</td>
</tr>
<tr>
<td>Archiving Log Entries</td>
<td>......................................................... 130</td>
</tr>
<tr>
<td>Removable Media Log</td>
<td>......................................................... 131</td>
</tr>
<tr>
<td>Filtering RMM Log Events</td>
<td>......................................................... 132</td>
</tr>
<tr>
<td>Viewing Individual RMM Events</td>
<td>................................................. 132</td>
</tr>
<tr>
<td>CD and DVD Events Log</td>
<td>......................................................... 133</td>
</tr>
<tr>
<td>Removable Media Log Archival</td>
<td>..................................................... 133</td>
</tr>
<tr>
<td>Reports</td>
<td>................................................................. 134</td>
</tr>
<tr>
<td>Creating Reports</td>
<td>.......................................................... 134</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>DataScan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>..................................................... 140</td>
</tr>
<tr>
<td>Using DataScan</td>
<td>............................................ 141</td>
</tr>
<tr>
<td>Functionality</td>
<td>.................................................. 141</td>
</tr>
<tr>
<td>Understanding the XML Script</td>
<td>............................................. 143</td>
</tr>
<tr>
<td>DataScan installed files</td>
<td>................................................... 147</td>
</tr>
<tr>
<td>Command Line Parameters</td>
<td>.................................................. 148</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A</th>
<th>Glossary of Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>................................................................. 157</td>
</tr>
</tbody>
</table>
Preface

In This Chapter

Who Should Use This Guide?  page 10
More Information  page 10
Feedback  page 10
Who Should Use This Guide?

This guide is intended for Administrators using Media Encryption Server to manage device and port security for endpoint clients.

More Information

• For additional technical information about Check Point products, consult Check Point's SecureKnowledge at http://support.checkpoint.com.
• To view the latest version of this document in the Check Point User Center, go to: http://support.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com
Chapter 1

Introduction

This chapter provides an overview of Media Encryption feature and system requirements.

In This Chapter

- Overview page 12
- Licensing Model page 15
- Additional Information page 16
Overview

Check Point Media Encryption prevents unauthorized copying of sensitive data by combining port and device management, content filtering and centralized auditing with robust media encryption. Based on market-leading technologies, Check Point Media Encryption plugs potential leak points and logs data movement to and from any plug and play devices, providing comprehensive control of security policies.

Administration Console

Administrators use the Administration Console to manage Media Encryption Server. A familiar Microsoft Management Console (MMC) interface provides the ability to define and manage user profiles, deploy profiles to client computers, perform real-time monitoring and auditing, and configure Media Encryption options. User profile management and product configuration data are stored in an SQL database.
Features

Media Encryption is a unique policy driven solution for securing enterprise information and ensuring data integrity. It includes the following features.

Removable Media Manager

Media Encryption ensures that all removable media and other input/output devices are authorized before access is granted to client users. Authorization rules are defined by administrators as part of the profiles assigned to users.

Removable Media Manager (RMM) authorizes devices by means of a unique digital signature, which identifies them as authorized. Whenever contents are altered on a Media Encryption protected computer, the digital signature is automatically updated. If the contents are altered outside of the protected environment, the device will require re-authorization before it can be used in the protected environment.

Media Encryption ensures that all devices are scanned for viruses, malware and other prohibited content using the DataScan scanner and/or third-party anti-virus and anti-malware software. This prevents unauthorized transfer of sensitive data.

Encryption Policy Manager

Encryption Policy Manager (EPM) uses 256 bit AES encryption to provide unrivaled security for all types of removable storage devices in a manner that is transparent to the user. EPM grants trusted users offline access to encrypted media with password authentication. Users can also install a freely distributed EPM plug-in on non-protected computers as an alternative to password authentication.

Encryption Policy Manager includes the following features:

- Administrator defined access (full, read-only, or blocked) to encrypted removable media devices
- Password authentication to protected media on external computers without special software
- Extract encrypted data to non-encrypted data on target computers
- Secure deletion of encrypted documents on target computers
Features

**Device Manager**

Device Manager controls access to devices attached to endpoint computer ports, such as IrDA, COM, USB, Firewire, LPT, and network adapters. You can use Device Manager to control access to specific device types or all devices attached to a given port type.

By applying security rules to specific device types, you can manage access to Flash drives, memory sticks, CD/DVD drives, PDAs, Blackberrys, Bluetooth and USB hard disks. This feature prevents users from connecting unauthorized devices to the PC ports, such as modems and provides On/Off/read-only protection.

**DataScan**

DataScan a unique file-based protection feature that automatically prevents the introduction of potentially dangerous and undesirable file types on protected endpoint computers. Unlike traditional virus and malware scanners, DataScan does not scan files for known signatures or patterns. It allows or blocks access to files based on the file type as determined by its internal structure and extension.

DataScan is integrated with the Removable Media Manager and prevents authorization of removable media containing specific file types on local drives, network drives and removable media. By default this includes executables (.exe, .com, .dll), script files (.vbs, .scr, .js, etc.) and other files (.mpg, .mp3, .mov, etc.)

If DataScan is designated as a device scanner for Removable Media Manager, no media or device that contains prohibited files type can be authorized until the offending files are deleted.

**Program Security Guard**

Program Security Guard is a profile-based security feature that prevents users from creating, modifying or deleting specific file types on endpoint computers and network drives. Administrators create rules that specify which file extensions are prohibited as well as exceptions for trusted applications using prohibited extensions.
Auditing and Alerts

Media Encryption provides configurable, detailed logs stored in an SQL database. Administrators create structured queries and detailed reports to extract and analyze log contents.

Media Encryption also allows administrators to centrally monitor and audit file operations on protected removable devices. Administrators can also define email alerts to be sent to designated users based on certain events.

Licensing Model

A Media Encryption license is required for each server machine and covers a fixed number of connected endpoint computers. When the number of endpoints connected to a Media Encryption server exceeds the licensed quantity, you must purchase additional licenses. The following table describes the available license types.

<table>
<thead>
<tr>
<th>License Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Encryption</td>
<td>Standalone license including: Remote Media Manager, Program Security Guard and DataScan</td>
</tr>
<tr>
<td>Port Protection</td>
<td>Standalone License including: Encryption Policy Manager and Port Protection</td>
</tr>
<tr>
<td>Total Security</td>
<td>Full Endpoint Security license including all Media Encryption features together with Full Disk Encryption, firewall, anti-virus, anti-malware and VPN client.</td>
</tr>
</tbody>
</table>

If you plan to install a standalone Media Encryption Server with all features, you must purchase separate Media Encryption and Port Protection licenses. The Total Security license automatically includes both of these licenses.

It is possible that some endpoint computers have only Port Protection enabled, others have only Media Encryption enabled, and others have both features enabled. This is possible as long as the total number of endpoint computers do not exceed the maximum quantity on either license.
Additional Information

Media Encryption is supplied with fully indexed online help. In addition to these resources further information is available from the Check Point web site, http://www.checkpoint.com

The website provides a support area, http://support.checkpoint.com, including:

- A fully searchable support knowledge base that provides up to date information on the latest support problems and frequently asked questions
- Downloads of the latest software updates and patches for licensed customers
- The latest product documentation
- Discussion forums on Check Point products
Chapter 2
Getting Started

This chapter describes how to get started with Media Encryption, and also how to use the Administration Console and utilities.

In This Chapter

- Introducing the Administration Console  page 18
- Launching the Administration Console  page 21
- First Steps after Installation  page 22
- Connecting to a Remote or Local Server  page 23
- Configuring Media Encryption Server  page 25
- Configuring Removable Media Manager  page 45
- Recovering EPM Passwords  page 47
Introducing the Administration Console

The Media Encryption Administration Console allows administrators to centrally manage multiple endpoint client computers. You use the Management Console to perform the following tasks:

- Create and manage user and group-based policy profiles governing all Media Encryption features on endpoint clients
- Perform dynamic management of Media Encryption Client workstations
- View and process audit events
- Manage automated alerts
- Manage the Media Encryption infrastructure
- Manage removable media encryption settings (EPM)

Administration Console User Interface

The Media Encryption Administration Console provides a powerful, but user-friendly user interface based on the familiar Microsoft Management Console (MMC).
Windows

The Administration Console contains two windows by default. Each window can display different groups of settings and information. You can resize the Administration Console, open additional windows in the console and close open windows.

Each window contains a Details Pane that displays a list of detailed settings or information. The Console Tree Pane, which appears by default in the Main window and in new windows, provides convenient navigation to the various settings groups and information.

To open a new window, right-click on a branch in the Console Tree and select and select New Window from Here. The new window opens on top of the others.
The Toolbar

The toolbar provides convenient access to various Administration Console functionality.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>← →</td>
<td>Move backward and forward between data viewed in current window</td>
</tr>
<tr>
<td></td>
<td>Move up to higher level in Console Tree</td>
</tr>
<tr>
<td></td>
<td>Toggle display of Console Tree in current window</td>
</tr>
<tr>
<td></td>
<td>Refresh details view in current window</td>
</tr>
<tr>
<td></td>
<td>Export contents of current window details view to a text file</td>
</tr>
<tr>
<td></td>
<td>Display online help</td>
</tr>
<tr>
<td></td>
<td>Define filter for displaying records in current window details view</td>
</tr>
<tr>
<td></td>
<td>Toggle between filter and showing all records in details view</td>
</tr>
</tbody>
</table>

The Console Tree

The Console Tree provides convenient access to profile definition categories and to options for viewing log entries.

If the Console Tree does not appear, click the icon on the toolbar.

<table>
<thead>
<tr>
<th>Settings Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Endpoint users and user-specific profile definitions</td>
</tr>
<tr>
<td>Computers</td>
<td>Computers and computer-specific profile definitions</td>
</tr>
<tr>
<td>Groups</td>
<td>User and computer groups and group-specific profiles</td>
</tr>
<tr>
<td>Profile Templates</td>
<td>Templates for defining individual profiles</td>
</tr>
<tr>
<td>Alerts</td>
<td>Custom email alert definitions</td>
</tr>
<tr>
<td>Log</td>
<td>View log entries</td>
</tr>
<tr>
<td>Removable Media Log</td>
<td>View selected removable media log entries</td>
</tr>
<tr>
<td>Reports</td>
<td>Define and review reports based on log entries</td>
</tr>
</tbody>
</table>
Launching the Administration Console

To open the Administration Console, select **Start > Programs > Check Point > Media Encryption Server > Administration Console.**
First Steps after Installation

This section describes the procedures to be followed after installing Media Encryption Server for the first time.

1. **Connect to a server**
   Connect to a Media Encryption server using the Administration Console.

2. **Modify the predefined Default profile**
   This is the global profile that is assigned to all endpoint computers and users that have not yet been assigned a profile. The default profile should provide a high security level and contain settings that are unlikely to be changed by custom policies assigned to users, computers and groups.

3. **Create custom profile templates**
   Define custom profiles for administrators as well as for other user and computer groups.

4. **Create user and computer groups**
   Groups are an efficient way to define profiles and settings for users and endpoint computers sharing common security requirements. Profile settings assigned to a group apply to all members of a group unless overridden by a customized profile specific to a particular user.

5. **Define custom email alerts**
   Define custom email alerts to be sent to users for various events and actions.

6. **Configure Media Encryption Server Properties**
   Configure the application, security, email and console settings.

7. **Backup the media ID**
   Back up the media ID using the Export Media ID wizard.

8. **Export the default profile**
   Export the default profile to the Media Encryption Client installation folder.

9. **Install Media Encryption Client computers for testing**
   Test your default and custom profiles by installing Media Encryption client on several test computers. Perform various activities with removable media and devices to insure proper operation.

10. **Create and configure silent Media Encryption Client installation packages**
    Use the Endpoint Security Deployment Utility to create silent installation packages to install Media Encryption client in your production environment.

11. **Assign computers to groups**
    After you install Media Encryption Client on endpoint computers, they appear as computers on the Administration Console. Assign these computers to groups.
Connecting to a Remote or Local Server

The Administration Console supports local and remote server connections. You can install multiple administration consoles to manage one Media Encryption Server.

1. In the Administration Console, right-click the Media Encryption Server branch in the Console Tree. Select Connect to from the option menu.

2. In the Server Location window, select one of the following connections:
   - **Media Encryption Server on this computer**: Connect to the server on this computer.
   - **Remote Media Encryption Server**: Connect to a server located on a remote host. Enter the server host computer name or IP address and port number (default = 9738).

   **Warning** - You must configure both the client and server firewalls to allow UDO traffic over the designated port.
3. Click **Finish** to complete the connection. The following connection process message appears:

The current connection status appears on the title bar.

**Note** - Access privileges must be granted in the **Security Permissions** tab before you can connect to a remote server.
Configuring Media Encryption Server

In This Section

Media Encryption Server Properties page 25
General Properties Tab page 26
Applications Tab page 28
Security Tab page 38
Email Configuration Tab page 42
Console Settings Tab page 43
Server Key Tab page 44

Media Encryption Server Properties

This section presents procedures for configuring Media Encryption Server. To define Media Encryption Server properties:

Right-click the Media Encryption Server <server name> branch and select Properties. The Media Encryption Server Properties window opens, which contains a variety of settings grouped together on several tabs.
General Properties Tab

The General tab displays the server version and build number. You can also revoke authorization for previously authorized devices and add or remove server licenses.

To revoke authorization for previously authorized devices:
1. In the Media revocation section, click Revoke all.
2. Click Yes in the confirmation window.

**Note** - This process can be reversed by re-importing the media ID providing a backup was made during installation.
To add or remove server licenses:

1. Click License Manager. The License Manager window opens, showing license type (full or evaluation), number of clients, and expiration date.

2. Perform one or more of the following steps:
   - To add a new license, click Add from license file and navigate to the license file. Alternatively, you can click Add license and manually enter the license information.
   - To remove a license, select a license from the list and then click Remove.
   - To change the license string for an existing license, click Edit.
Applications Tab

The Applications tab contains configuration options for the Program Security Manager, Device Manager and Encryption Policy Manager features.

Program Security Guard (Expreset.ini)

Program Security Guard uses a database, the expreset.ini file, that contains protected file type definitions and a list of trusted applications that are permitted to create or modify protected file types.

We recommend that you periodically backup the expreset.ini file. You can also use this backup file to transfer Program Security Guard file type definitions to other Media Encryption servers.

To backup the expreset.ini file, click Backup. Enter a file name and navigate to the desired file location.

To restore the expreset.ini file, click Restore and navigate to the backup file.
Device Manager

Device Manager includes a default list of ports and device types. You can add new device classes and specific devices to achieve more granular control of various types of attached devices. Specific security rights can be assigned on a device class or a specific device.

To open the **Configuration Editor** window, click **Edit**.
Creating a New Device Class

To create a new device class:

1. In the Configuration Editor window, click Add device class. The Device Properties window opens.

2. In the Device Properties window, configure the following properties:

Device Information properties
- **Display Name**
  Specifies the device name as displayed in Device Manager.
- **Device GUID**
  Specifies the unique system identification for a device class. Each type or brand of device has its own unique ID. You can retrieve this information from the log after inserting a new device into an endpoint computer.

**Note** - A device class is a new type of device rather than a specific model or brand of existing device class.

3. **Device GUID**

   Specifies the unique system identification for a device class. Each type or brand of device has its own unique ID. You can retrieve this information from the log after inserting a new device into an endpoint computer.
Device Connection
Specifies the device connection type, which controls internal and/or external connections for a device class. For example, it may be desirable to block the use of external modems but permit the use of built-in modems on a laptop computer.

Extra Information
Specifies whether the device appears in Windows as a fixed disk device (Hard disk with master boot record) or as removable media (Media without master boot record).

Icon
Specifies the icon that appears in Device Manager.

Note - To access the following properties, click Show advanced options.

Device ID filter

Device ID String begins with
Specifies a filter string that determines device class membership by comparing it to device IDs. Devices are included in a class when the initial characters in the device ID match this filter string.

For example, if the filter string is ‘My_USB_ Stick’, then the following devices are members of the device class:

- ‘My_USB_ Stick_2MB’
- ‘My_USB_ Stick_4MB’
- ‘My_USB_ Stick_8MB’
- ‘My_USB_ Stick_SoBigThatEverythingFits’
Device capabilities

- **Can encrypt data with EPM**
  Specifies whether a device can be encrypted using the Encryption Policy Manager.

- **Can execute files directly from the device**
  Specifies whether the device supports the execution of programs directly from a device.

- **Can be used for reading and writing**
  Specifies whether a device can be read or written to.

- **Can be read only**
  Specifies whether the read-only option is available for a device.

- **Can generate audit event on arrival**
  Specifies whether a device can generate audit events when the Generate device arrival audit event option is enabled.

Default device access rights

These properties specify default options for newly created profiles or profile templates.

- **Default access**
  Specifies the default device access rights.

- **Generate device arrival audit event**
  Specifies the default Generate device arrival audit event option.

- **Encrypt device data with EPM**
  Specifies the default EPM status.
Adding a New Device to a Device Class

You can enhance granularity by defining specific device brands, models or types as separate devices within an existing device class. For example, you may decide to restrict flash memory drives to a specific make or model approved for your organization. New devices appear directly under the device class in the Device Manager list.

To create a new device within an existing device category:

1. Authorize the specific device you want to create.
2. Open the log and locate the authorized device event. In the Log Event window, click the Device information tab.
3. Click Add this device to device manager.
4. In the Configuration Editor window, click Add device ID.
5. In the Device Properties window, click Show advanced options.
6. Configure the properties as described in “Creating a New Device Class” on page 30.

   a. Make certain that you define the device ID filter as described in “Device ID filter” on page 31.

Default Device Classes

This section describes the device classes included by default in Media Encryption.

Warning - Incorrect device and device class definitions may cause unanticipated behavior such as blocking access to legitimate devices or granting access to dangerous or unwanted devices. Device class categories are typically assigned by Microsoft and other product vendors. Some devices may belong to a class that seems illogical based on the class name, but is, in fact, correct. Some devices may belong to more than one class, especially if you have defined custom classes.

Make certain that you thoroughly test all Device Management settings before deploying profiles to endpoints computers.

• Removable Media Devices
   Controls access to non-bootable USB and Firewire storage devices, such as flash drives, memory card readers, disk drives, etc. You can define separate permissions for encrypted and unencrypted devices as well as the ability for users to encrypt the device.
• **CD/DVD-ROM Drives**
  Controls access to CD, DVD drives, including write-capable devices. You can define separate permissions for encrypted and unencrypted devices as well as the ability for users to encrypt the devices.

• **External hard drives**
  Controls access to bootable external hard disk drives, including both USB and Firewire devices. You can define separate permissions for encrypted and unencrypted devices as well as the ability for users to encrypt the devices.

• **Floppy disks**
  Controls access to internal and external floppy disk drives.

• **Tape Drives**
  Controls access to tape drives.

• **Modems**
  Controls access using internal and external modems,

• **Printers (USB)**
  Controls access to USB printers,

• **Bluetooth**
  Controls access to various types of Bluetooth devices, including:
  – Radio transceivers
  – RIM devices
  – Mobile Phones
  – Bluetooth USB devices

• **Still image devices**
  Controls access by still image devices such as scanners and digital cameras.

• **Infrared devices (IrDA)**
  Controls access using infrared devices such as laptops, PDAs, Blackberries, and printers.

• **Smart card readers**
  Controls access to internal and external smart card readers.

• **PCMCIA Memory**
  Controls access to devices connected via PCMCIA ports including flash memory readers and removable hard disks.

• **USB Controllers**
  Controls access to generic devices USB devices.
• **Palm OS Devices**  
  Controls access to Palm Pilot PDAs and other Palm OS devices.

• **Windows CE Portable Devices**  
  Controls access to various Microsoft Windows CE PDA, including devices that connect using Microsoft Active Sync.

• **Ports (COM/LPT)**  
  Controls devices connected to COM and LPT ports.

• **Network Adapters**  
  Controls devices connected to Ethernet and WiFi network adapters.

• **Windows Portable Devices**  
  Controls access to certain types of USB portable devices such as MP3 players and video players.

• **Keyboards**  
  Controls access to USB and PS2 keyboards.

• **IEEE 1394 Bus Host Controller**  
  Controls access to devices connected to Firewall ports.
Encryption Policy Manager Site Identification

This section describes how to export and import site IDs to and from remote EPM sites and how to define new EPM sites.

Exporting the local EMP site ID

To export the local EMP site ID to remote sites, click Export this site ID and navigate to the remote location. By default, the local server name is assigned as the file name.

Importing a remote EMP site ID

To import a local EMP site ID:
1. Click Import ID of another site. The Import wizard opens.
2. In the File Name window, browse to the desired site ID file (*.esd).
3. In the Site Name window, assign a site ID name.
4. Click Finish to complete the import process.

Advanced Properties

You can manually add, remove and edit existing trusted EPM sites. To open the EMP sites configuration window, click Advanced on the lower section of the Applications tab.
To add a new remote site:
1. Click Add and enter the new remote site name and site ID in the designated fields.
2. Select a site from the list and click Remove.
3. Click Edit and edit the data as required.

Security Tab

This section describes the process of defining Media Encryption Server users and assigning permissions to them.

To work with the security settings:
1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select Properties.
2. In the Media Encryption Server, click the Security tab.
3. To add a new user, click Add. To modify permissions for a user, select the user. Configure permissions on the Basic and Advanced permissions tabs.

Upon installation, the default security permissions grant anyone in the Windows Administrator group full permissions to the Media Encryption Server. You can add and remove users and groups as well as assign permissions according to your own requirements.
Basic Permissions

The following options can be configured with the Basic permissions security tab:

- **Administrate**
  Allows users to manage the Media Encryption Server. The ability to change the media ID and delete log files is unavailable.

- **Manage Reports**
  Allows users to manage and generate reports within the Media Encryption Administration Console.

- **Special Permissions**
  Allows users to recover encryption keys and change the media ID. This option should only be selected for security administrators.
Advanced Permissions Tab

The Advanced permissions tab defines the following detailed permissions:

- **Change Permissions**
  Allows user to change security permissions for other users.

- **EPM Key Recovery**
  Allows user to recover encryption keys for media encrypted using the Encryption Policy Manager. Members of this group will have full access to all encrypted removable media. This option is only relevant if Encryption Policy Manager is enabled.

- **Change Media ID**
  Allows user to change the Removable Media ID. Changing the removable media ID is irreversible and can adversely impact endpoint users.

- **Change Configuration Settings**
  Allows user to change various Administration console configuration options (excluding profiles and groups).

- **Change Profile template**
  Allows user to modify profile templates.

**Note** - Make sure that at least one user has permissions to modify each of the permission categories in this list.
– **Change Groups and Group Order**
  Allows user to define and modify groups and the order in which they appear in the Administration Console.

– **Create Reports**
  Allows user to create and run HTML reports.

– **Delete Reports**
  Allows user to delete existing HTML reports.

– **View Configuration**
  Allows user to view users, groups and profile sections the Administration Console. Administrators denied this permission cannot use the Administration Console.

– **View Logs**
  Allows user to view the audit logs in the Administration Console.

**Note** - The Media Encryption Server must be configured to support anonymous network connections in order to allow requests from clients when no interactive user is logged in.

You should configure anonymous logon accounts for client access permissions by default. Do not delete anonymous logon accounts under any circumstances.
Email Configuration Tab

This section describes the process of defining the SMTP settings for automatic email alerts.

To configure Email Media Encryption server for email alerts:

1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select Properties. The Media Encryption Server window opens. Click the Email configuration tab.

2. Define the following parameters:
   - **SMTP server name**
     Name of the server where SMTP is enabled for internal connections.
   - **Port**
     Port number on which the SMTP server can be connected to (default 25).
   - **SMTP user name**
     User account that has permission to connect to and send email alerts via SMTP.
   - **Password and Confirmation**
     The user account password.
   - **Server email address**
     Email address used to send Media Encryption alerts via the SMTP server.
– Alert message subject
  Text that appears in the message subject for alert messages.

– Send a test alert to
  Enables the system administrator to test SMTP configuration settings.

**Console Settings Tab**

Media Encryption is designed to be used on global infrastructures with many thousands of machines and workstations. To improve performance, you can restrict the number of users, computers and reports displayed on a given Administration Console.

To define Administration Console limits:

1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select Properties. The Media Encryption Server window opens. Click the **Console settings** tab.

2. Enter the desired parameters and click OK to continue.
Server Key Tab

In Novell Netware installations, a Server Key tab appears. Media Encryption Server uses an RSA key to encrypt client/server communication across the network. You must export this RSA key to the client installation folder prior to installing Media Encryption Server. Alternatively you can run the .reg file from any previously installed clients.

Note - If the server key is not exported to the client install disk on Novell server installations the client-server communication will not function correctly.

To export the RSA key:
1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select Properties. The Media Encryption Server window opens. Click the Server key tab.
2. Click Create client registry file to export the serverkey.reg file to the root directory of the client installation folder.
Configuring Removable Media Manager

During installation the Media Encryption Server generates a unique signature media ID. This unique ID is used during media authorization and ensures that media authorized within other Media Encryption protected environments are not valid within this protected zone and vice versa.

On occasions it can be desirable to use the same media signature ID on multiple sites/servers. This means that devices authorized within one protected environment can also be recognized as authorized in other environments. This can be achieved using the Import/Export Media ID feature.

**Importing and Exporting Remote Media ID**

1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select Removable Media Manager > Import/Export Media ID.

2. On the Welcome screen, click Next.
3. On the Task screen, select Import media ID or Export media ID as desired.

4. On the File Name screen, enter or navigate to the file that you wish to import or export to.

5. Click Finish to complete the process.
Recovering EPM Passwords

Encryption Policy Manager allows administrators to remotely recover encrypted device passwords, using a challenge/response wizard.

To recover EPM passwords:

1. Right-click the Media Encryption Server <server name> branch in the Console Tree and select EPM Key Recovery. Click Next on the wizard welcome page.

2. In the Information window, enter the challenge code provided by the user.

3. Media Encryption Server authenticates the challenge code and generates a response code in the next wizard window.

4. Provide the response code to the client user.

5. Click Next to complete the process.
Chapter 3
Working with Profiles

This chapter presents a reference to Media Encryption profiles and their settings and options. Procedures for defining profiles as well as deploying them to client computers are also presented.

In This Chapter

Overview .................................................. page 50
Working with Profile Templates ................. page 51
Exporting Profile Templates ....................... page 86
Overview

Profiles are collections of security rules and settings that govern encryption and user access to removable devices. The security policy that applies to endpoint client users is defined by one or more profiles assigned to that user.

The Default Profile

The default profile automatically applies to users who do not belonging to any user groups or who connect to the server without a user definition in the server database. This profile should be restrictive in nature, preventing undefined users from accessing removable devices and most ports.

All user groups must contain the default profile.

Profile Priority and Inheritance

Profiles are assigned to client users by the groups they belong to. A user profile can also contain settings defined a custom profile that applies only to that user. Custom profile settings always override inherited settings.

Typically, the security policy governing a given user consists of settings inherited from multiple profiles arranged in a predefined hierarchy.

For example, the above user profile consists of policy settings applied in the following order of precedence:

1. Settings explicitly defined in the Custom profile
2. Settings explicitly defined in the Developers profile
3. Settings explicitly defined in the MySampleTemplate profile, but not in the Developers or Custom profiles
4. Settings contained in the Default profile not explicitly defined elsewhere
Profile Templates

Profile templates are a convenient way to manage policy settings and assign them to endpoint users. Since policy templates are assigned to user groups, any changes made to profile template settings automatically apply to all users belonging to groups using that profile.

Working with Profile Templates

In This Section

Overview page 52
Defining Profiles page 52
General Settings page 54
Device Manager Settings page 55
Removable Media Manager Settings page 58
Auditing Settings page 67
Program Security Guard Settings page 76
User Interface Tab page 81
Advanced Tab page 83
Overview

This section presents the process of defining profile templates and also serves as a reference to the many individual settings that comprise a profile. Each profile consists of several settings groups, categorized as follows:

- General settings
- Device Manager settings
- Removable Media Manager settings
- Encryption settings
- Program Security Guard settings
- Client User Interface settings
- Auditing and Alert settings
- Advanced Settings

Each settings group appears on a separate tab in the template Properties window.

Defining Profiles

To create a new profile template:

1. In the Console Tree, right-click Profile Templates and select New > Profile template.
2. In the Template Properties window, enter a profile name in the General tab and define other policy settings as required.
3. Assign the new profile to user and computer groups.
4. In the Profile Templates details window, right-click the new profile and select force profile reload. This action downloads the profile settings to all applicable users.
To modify an existing profile template:

1. In the **Profile Templates** details window, double click a profile template or select a template and click the **Properties** link.

   ![Template Properties window](image1)

   The Template Properties window opens.

2. Modify profile settings as required.

3. In the **Profile Templates** details window, right-click the new profile and select **force profile reload**. This action downloads the profile settings to all applicable users.

   ![MyProfile Properties window](image2)
Policy Definition Modes

You can implicitly define a particular setting or settings group in the current profile or inherit settings from other profiles that are lower in the hierarchy. To switch from one policy definition mode to the other, toggle the lock icon as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Lock Icon]</td>
<td><strong>Current Profile Mode:</strong> Setting is explicitly defined in the current profile and overrides all inherited settings</td>
</tr>
<tr>
<td>![Unlock Icon]</td>
<td><strong>Inherited Mode:</strong> Setting is inherited from other profiles that are lower in the hierarchy</td>
</tr>
</tbody>
</table>

Settings in the inherited mode, may appear grayed out on a tab.

General Settings

In both cases, the Profile Properties window opens, displaying the General tab.

Profile name: profile name

Notes: Explanatory notes.
Device Manager Settings

Device Manager settings define the level of protection provided for each specific port type. The settings for removable devices also determine whether encryption is optional or required.

For example, in the following illustration, access to Apple iPods and external hard drives hard is blocked unless they are encrypted. Unencrypted DVD and CD drives may only be read, but users can burn DVDs and CDs if they encrypt them. Other removable devices have full access and may be encrypted by end users.
**Device**

This column displays the defined device classes and devices.

*Warning* - Incorrect device and device class definitions may cause unanticipated behavior such as blocking access to legitimate devices or granting access to dangerous or unwanted devices. Device class categories are typically assigned by Microsoft and other product vendors. Some devices may belong to a class that seems illogical based on the class name, but is, in fact, correct. Some devices may belong to more than one class, especially if you have defined custom classes.

Make certain that you thoroughly test all Device Management settings before deploying profiles to endpoints computers.

**Define**

This column specifies the policy definition mode for each device.

To switch from one policy definition mode to the other, toggle the lock icon.

Table 3-2 Setting modes

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="Current Profile Mode" /></td>
<td><strong>Current Profile Mode</strong>: Setting is explicitly defined in the current profile and overrides all inherited settings</td>
</tr>
<tr>
<td><img src="Image" alt="Inherited Mode" /></td>
<td><strong>Inherited Mode</strong>: Setting is inherited from other profiles that are lower in the hierarchy</td>
</tr>
</tbody>
</table>

Settings in the inherited mode, may appear as unavailable.

See “Policy Definition Modes” on page 54 for details.

**Audit**

This column shows whether or not logging and/or alerts are enabled for the device. Auditing actions are defined on the **Auditing** tab.

To enable or disable logging and alerts for each device, click the appropriate checkbox. See “Logs” on page 126 and “Alerts” on page 124 for details.

**Plain text**

This column specifies access rights for non-encrypted devices. Some access rights types may be unavailable for certain devices.
The access rights types are described below:

- **No access**
  All access attempts are blocked.

- **Read only**
  Users can read and copy data from authorized devices, but cannot write data or execute files.

- **Read only, No network**
  Users can read and copy data on authorized devices but these devices cannot be shared over a network, regardless of NTFS/Share level security permissions.

- **Read only, Execute**
  Users can read data, copy data and execute files from authorized devices, but cannot write data.

- **Full access**
  Users can read and write data on authorized devices, but cannot execute files.

- **Full access, no network**
  Allows users to read from and write data on authorized devices, but cannot execute files. Devices cannot be shared over a network, irrespective of NTFS/Share level security permissions.

- **Full access, Execute**
  Users can read, write, and execute files on authorized devices.

- **Full access, Execute, no network**
  Users can read, write, and execute files on authorized devices. These devices cannot be shared over a network, irrespective of NTFS/Share level security permissions.

**Encrypted**

This column specifies access rights for devices encrypted using the Encryption Policy Manager feature.

- **Access**
  Users can access encrypted devices according to permissions granted on the Encryption (EPM) tab.

- **Access, Create**
  Users can encrypt and decrypt the device as well as access its contents. If

  **Tip** - If you define the Plain text permission for a device as “No access” and the Encrypted permission as “Access, Create”, users will be required to encrypt the device before access is allowed.
Removable Media Manager Settings

This section provides a reference to Removable Media Manager (RMM) settings. The Removable Media Manager governs access to removable devices, by ensuring that all removable devices are authorized. The authorization process and the options available to users are defined on the Removable Media Manager tab.

The following options are available:

- **No media authorization check**
  Removable Media Manager is disabled. Users can access any devices that are permitted by the **Device Manager**.

![Removable Media Manager Settings](image_url)
• **Automatic media authorization**
  RMM attempts to authorize devices automatically by scanning them for viruses and other prohibited content. RMM automatically detects compatible anti-virus scanners.

  If the scan is successful, RMM authorizes the device and allows access. If the scan detects a virus or other prohibited content, access is blocked.

  **Note** - Automatic authorization fails if no anti-virus scanner or DataScan is detected.

• **Automatic Media authorization with an option to delete files**
  RMM attempts to authorize devices automatically by scanning them for viruses and other prohibited content. RMM automatically detects compatible anti-virus scanners.

  If the scan is successful, RMM authorizes the device and allows access. If the scan detects a virus or other prohibited content on the device, the user is given the option of deleting the prohibited content. If the user deletes the prohibited content, the device is authorized and access is allowed.

  **Note** - Automatic authorization fails if no anti-virus scanner or DataScan is detected.

• **Allow users the following rights**
  Enable one or more of the following authorization options:

  – **User can authorize removable media**
    Allows users to authorize devices interactively. If this option is disabled, RMM blocks access and users receive an error message.

  – **User can select scanners**
    Users can select which scanner to use when authorizing devices. The user must select at least one scanner. If your organization policy requires the use of DataScan to prevent access to specific content, it is recommended that you do not enable this option.

  – **User can skip media scan**
    Allows users to bypass scanning and allow infected or unauthorized content onto the system. This option is recommended only for testing under controlled conditions.
- **User can delete files on unauthorized media**
  If the scan is successful, the device is authorized and access is allowed. If the scan detects a virus or other prohibited material on the device, the user is given the option of deleting prohibited content. If the user deletes the prohibited content, the device is authorized and access is allowed.

  This option is useful when using DataScan.
Encryption Settings

In This Section

Authentication Methods page 62
Automatic Access to Encrypted Media Settings page 62
Access to Password Protected Media Settings page 63
Advanced Settings page 64

The Encryption tab provides a reference to profile settings governing the Encryption Policy Manager (EPM) feature. This tab is available only if the Encryption Policy Manager is enabled.
**Authentication Methods**

Users can authenticate by either of the following methods:

- **Automatic Access**
  Users authenticate automatically when connected to a Media Encryption Server. Automatic access is only available for endpoint clients that are connected to a Media Encryption Server.

- **Password Access**
  Users authenticate by entering a password. Password access may be available when automatic access is not allowed, typically when an endpoint client is not connected to a Media Encryption Server. You can require separate passwords for full access and read-only access.

  **Note** - The settings on the Encryption tab only govern devices encrypted using the current policy. Encryption Policy Manager is always active in the background on client computers, allowing all authorized users to access encrypted devices.

**Automatic Access to Encrypted Media Settings**

This section contains a list of user groups eligible for automatic authentication and the access permissions assigned to each group. Users receive the access permissions assigned to the highest group in the list to which they belong.

To add a user group, click Add. In the Media Origin window, select one or more groups.

To change the priority of a group, select a group or groups and click Move Up or Move Down.

The following access permissions are available:

- **Full Access**
  Full read/write access including the ability to copy, create, modify and delete files

- **Read Only Access**
  Read only access where users cannot copy files to or from the device, nor can they create, modify or delete files

- **No Automatic Access**
  No automatic authentication, but users can authenticate by entering a password
Access to Password Protected Media Settings

This section contains a list of external sites that can encrypt removable devices, together with the access permissions assigned to that site. Sites are identified by a remote site ID assigned by Media Encryption. Media Encryption block access to all devices encrypted by any site not specifically defined in this list with full access permission.

To add a new site to the list:
1. Click Sites.
2. In the EPM Sites Configuration window, click Add.
3. In the EMP Site Information window, enter a name for the remote site and the remote site ID in the designated fields. We recommend that you copy and paste the site ID if possible.

To import a new site to the list:
1. Click Sites.
2. In the EPM Sites Configuration window, click Import. The Site ID Import wizard opens.
3. In the File Name window, browse to the desired site ID file (*.esd).
4. In the Site Name window, enter a site ID name.
5. Click Finish to complete the import process.

To assign access permissions to a site:
1. Select a site and then click the access setting for that site.
2. Select an access permission from the list. The following permissions are available:
   - **Full Access**
     Full read/right access including the ability to copy, create, modify and delete files
   - **No Access**
     Access is blocked
Access with Profile Templates

Access Permission Strategies

Access strategies for password protected encrypted devices

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to password protected media created within the current site only</td>
<td>Set This site to Full access and all other sites to No access.</td>
</tr>
<tr>
<td>No access to any password protected media, regardless of site</td>
<td>Set This site and all other sites to No access. This is the most restrictive option.</td>
</tr>
<tr>
<td>Allow access to the media from specific sites only</td>
<td>Set only those specific sites to Full access.</td>
</tr>
</tbody>
</table>

Advanced Settings

The Advanced Settings section contains several settings governing encryption and the use of passwords to access encrypted devices offline.

- **Protect media with a password for full access in offline mode**
  Allows access to encrypted devices using password authentication.
  - **Protect with a password for read-only access in offline mode**
    Enable to specify a separate passwords for read-only access.
  - **Users can change read-only**
    Enable to allow end users to change their read-only password.

- **Copy the EPM Explorer to encrypted media for offline access**
  EPM automatically copies the EPM Explorer utility to devices after encryption. EPM Explorer allows users not connected to the Media Encryption network to work with data on an encrypted device.

- **Users can change size of encrypted media**
  Allows users to change the percentage of device capacity that is encrypted.

- **Users can create media for other users**
  Allows users to create encrypted devices for other users.

- **Users can recover their password using challenge/response**
  Allows users to recover lost passwords via remote help using challenge/response authentication.

- **Users can remove EPM encryption from media**
  Users can decrypt removable devices.
Defining Password Constraints

The Password constraints window defines acceptable password criteria. EPM will not accept passwords that do not conform to these criteria. Two tabs contain the various settings.

Constraints tab

This tab contains minimum and maximum password length settings as well as the minimum and maximum number of several character types that a password must contain. The Test Password block can be used to confirm that the password settings are correctly implemented.
Advanced tab

This tab contains password retry rules.

- **Password note**
  Explanatory text regarding password constraints that is displayed to users.

- **Password retries**
  Retry rule settings
  - **Password attempts**
    The maximum number of unsuccessful password attempts allowed before access is temporarily blocked. 0=infinite password attempts.
  - **Block access for**
    How long device access is blocked (in minutes) after the maximum number of password retry attempts has been exceeded.
  - **Lock drive completely after (attempts)**:
    The maximum number of unsuccessful password attempts allowed before access is permanently blocked. Access to a permanently blocked device can only be restored by an administrator or by recovering the password using Remote Help. 0=infinite password attempts.
Auditing Settings

In This Section

- Audit Events Section page 68
- Removable Media Audit Rules Section page 72
- Automatic Access to Encrypted Media Settings page 62

This tab defines which events are recorded in the logs and/or generate alerts. In addition, you can define custom auditing rules for specific events.
Audit Events Section

In This Section

- Event types
- Log Contents:
- Media Audit Rule Window
- Condition Types

This section contains a list of Media Encryption events that you can choose to log or generate alerts. The following settings govern event logging:

- **Ignore**
  Do not log this event or generate an alert

- **Register**
  Record this event in the local audit log and upload it to the server according to the log synchronization schedule.

- **Immediate**
  Upload this event immediately to the Media Encryption Server log (if available). This mode can be used in conjunction with email Alerts, see “Alerts” on page 124.
Event types

You can enable auditing for the following event types:

- **Authorized Device Event**
  Access to authorized devices. Log information for this event can be used to add new devices to Device Manager.

- **Encrypted Removable Media Exported**
  An EPM encrypted device has been decrypted.

- **Endpoint Security Media Encryption DataScan Event**
  Any event generated by DataScan, including detection of unauthorized file types.

- **Fixed Hard Disk Configuration Changed**
  Physical changes to hard disk configuration, including the addition of a new disk or the removal of an existing disk. You can block such events using the Device Manager.

- **Removable Media Scan Was Skipped**
  User skips the Removable Media Manager scan (if allowed by the profile).

- **Removable Media Was Encrypted**
  User encrypts a removable device.

- **Scanner Event**
  Results of anti-virus scan (if supported by the scanner).

- **Service Startup Error**
  Media Encryption Client service fails to start during the client computer boot process. If the service does not start, all devices are subject to the default profile. This event is recorded in the logs the next time that the service starts successfully.

- **Successful Media Authorization**
  A device has been authorized successfully.

- **Suspected key logger detected**
  A suspected key logger or suspicious keyboard configuration changes were detected.

- **Unauthorized File Operation (PSG)**
  Unauthorized file operations detected by the Program Security Guard feature. This information can be used to create new PSG application exemptions.

- **Unauthorized Device Event**
  Unauthorized device access attempts. This information can be used to add new devices to Device Manager directly from the log.
• **Unauthorized Execution Attempt**  
  File execution blocked by Program Security Guard (PSG).

• **Unauthorized Removable Media Found**  
  Unauthorized removable device has been detected.

• **Unsuccessful Media Authorization**  
  Removable device authorization failed.

• **User has disabled a system component**  
  A client user has disabled a core Media Encryption client component  
  (Removable Media Manager, Device Manager, Encryption Profile Manager or  
  Program Security Guard).

• **User has enabled a system component**  
  A client user has enabled a core Media Encryption client component  
  (Removable Media Manager, Device Manager, Encryption Profile Manager or  
  Program Security Guard).
Log Contents:

The audit log contains the following information:

- **ID**
  Sequent ally assigned Media Encryption database record number

- **Unique ID**
  Unique ID assigned to each audit event

- **Time**
  Time and date that the event occurred

- **Event**
  Event name

- **Alert**
  Email alert generated (Yes/No)

- **User ID**
  User ID as defined in the Media Encryption user database

- **User Name**
  Logged on Windows user name

- **Host Name**
  The machine name on which the event occurred

- **Source**
  The source of the audited event (for example, PSG, RMM, DM, etc.)

- **Message**
  Other relevant information about the event, (for example, virus infection details, unauthorized file audits, etc.)
Working with Profile Templates

**Removable Media Audit Rules Section**

The **Removable Media Audit Rules** section allows administrators to define customized rules that capture specific removable device events and record them in the server log and optionally generate email alerts.

![Removable Media Audit Rule](image)

**To log all removable media events:**

Click **Log all**. This option deletes all existing removable media audit rules.

**To add a new removable media**

Click **Add**. The **Media Audit Window** opens. Define a rule as described in “Media Audit Rule Window” on page 73.

**To delete specific removable audit rules:**

Select the desired rules in the click **Remove**.

**To modify a removable audit rule:**

Select the desired rule and click **Edit**. Modify the rule as described in “Media Audit Rule Window” on page 73.
Media Audit Rule Window

This section describes the settings available in the Media Audit Rule window.

- **Media rule name**
  Unique name for the rule.

- **Recorded in server log**
  Record events in the server log.

- **Recorded in server log and raised alert**
  Record events in the server log and trigger an alert email. Select an appropriate alert type from the list.

  **Warning** - Use this feature with care. This option can potentially generate a large number of alert email messages, which could overwhelm your email server.

You can build complex rules using criteria in the **Conditions** section.

**To define a condition:**

1. Select an operation type from the list. Refer to "Condition Types" on page 74.
2. Select a condition from the list as follows.
   - **Is**: Is equal to (for example, Filename is Mydata.doc)
   - **Is not**: Is equal to (for example, Process is not test.exe)

You can use an asterisk (*) as wild card entry for ‘IS’ and ‘IS NOT’ expressions.
Condition Types

- **Date**
  Time and date when the audit event occurred

- **Computer Name**
  Machine name on which the event occurred

- **Operation Type**
  Select operation performed on removable device:
  - **Create**
    Create a new file on removable device
  - **Open for Write**
    Open a file on removable devices for writing (may generate multiple events for each file opening)
  - **Move/Rename**
    Move or rename files on removable device
  - **Delete**
    Delete files from removable device
  - **CD/DVD audit**
    Burn data to CD or DVD media
  - **EE Copy Out**
    Copy files from encrypted devices to unencrypted disks
  - **EE Copy In**
    Copy files to encrypted devices
  - **EE Read File**
    Read files using EPM explorer
  - **EE Rename**
    Rename files using EPM explorer
  - **EE Delete**
    Delete files using EPM explorer
  - **EE Create**
    Create new files using EPM explorer
  - **EE Audit Log was tampered with**
    Attempted tampering with EPM explorer log

- **Filename1**
  File name and extension (For rename operation, the old file name)
• **Filename2**  
  New file name after rename operation

• **Process**  
  Process name generating the event (e.g. Winword.exe, Explorer.exe etc.)

• **User ID**  
  User logon name

• **User**  
  Domain and user name of user generating the event
Program Security Guard Settings

In This Section

- Working with the File Type Blacklist: page 77
- Working with the Trusted Application Whitelist: page 78
- Other Settings on the PSG Tab: page 80

This Program Security Guard tab contains settings and definitions for this feature. PSG blocks all files contained in the active blacklist of filetypes unless it is accessed by a trusted application as defined in the active whitelist.
Working with the File Type Blacklist

This section presents

To modify the Program Security Guard file type blacklist:

1. Click **Configure file types**. The **Unsafe File Types** window opens.

2. Add or remove file types from the active blacklist as follows:
   a. Enable a file type to include it in the active blacklist.
   b. Clear a file type to remove it from the active blacklist.
   c. Click **Add** to define a new file type.

   ![Unsafe file types](image)

   Enter the file extension and description in the designated fields.
   d. Select a file type and click **Remove** to delete it from the list altogether.
   e. Select a file type and click **Edit** to modify the file extension or description.
Working with the Trusted Application Whitelist

To modify the Trusted Application whitelist:

1. Click **Configure applications**. The **PSG Exemptions** window opens.

![PSG Exemptions Window]

2. Add or remove file types from the active blacklist as follows:
   
   a. Enable an application to define it as trusted and include it in the active whitelist.
   
   b. Clear an application to remove it from the active whitelist.
   
   c. Click **Add** to define a new file type and add it to the active whitelist.

   ![PSG Product Declaration Window]

   i. Enter a description in the designated field.
ii. Click **Add** and enter the program executable in the designated field.

![Profile Templates](image)

**Note** - Exercise caution when exempting an application with the **Any account** option selected. This option, if used incorrectly, could leave PSG insecure, (for example, avoid adding `explorer.exe`, `setup.exe` etc.).

iii. Select the user account for which this exemption applies.

d. Select a file type and click **Remove** to delete it from the list altogether.

e. Select a file type and click **Edit** to modify the file extension or description.

Please note that the new extension will not be enabled unless the option is selected. New file types will appear in all profiles but will be deselected by default.

**Note** - Only file extensions with a length of three characters are currently supported as other types typically form part of an installation package that PSG will prevent from being renamed to executable code, therefore this will stop the execution of non three character extensions.
Other Settings on the PSG Tab

- **Disable Process Executable Check**
  Enable this option to block the execution of non-executable file extensions. By default, PSG will only allow the execution of .exe, .com, and .sys file types.

- **Exempt Internet Explorer Trusted Zones**
  Enable this option to exempt all Internet Explorer trusted zones from Program Security Guard file protection.

- **PSG will turn on automatically if unsafe file types are defined**
  Program Security Guard is enabled automatically if any blacklisted file types are detected. This happens even if Program Security Guard is disabled on the Configuration tab in the Computer Properties window.

- **Disable PSG even if there are defined unsafe file types**
  Program Security Guard remains disabled (if disabled on the Configuration tab in the Computer Properties window) even if blacklisted file types are defined.
User Interface Tab

This tab contains settings that define alert messages and allow users to disable Media Encryption features.

Setting the Tray Icon Appearance

To set the appearance of the tray icon, choose one of the following options from the list:

- **No Icon**
  The tray icon and all messaging are hidden

- **Icon Only**
  The icon is displayed but does not show messaging or the client menus. The tray icon must be visible to provide pop-up messaging.
Working with Profile Templates

- **Icon and short menu**
  The tray icon is displayed as well as an abbreviated right-click option menu.

- **Icon and full menu**
  The Media Encryption system tray icon is displayed together with a full right-click option menu, providing access to the Device Manager, Removable Media Manager, Program Security Guard (PSG) and Encryption Policy Manager menus.

**Program Security Guard Alerts**

Program Security Guard messages may be intrusive to users. Enable the **Display PSG alerts as balloon notifications** option to display these messages as pop-up alerts that automatically close after 10 seconds and require no user interaction.

**Disabling Media Encryption Features**

You can allow client users to disable the following features via the client UI window:

- Removable Media Manager (RMM)
- Program Security Guard (PSG)
- Device Manager (DM)

**Warning Messages**

You can define customized warning messages and contact information for Program Security Guard and Remote Media Manager in this section.
Advanced Tab

The advanced tab contains settings for the following advanced features:

- Anti-tampering
- Client profile reload
- Client log synchronization
- WebRH support
**Anti-tampering**

To enhance security, you can include anti-tampering protection for Media Encryption clients. When enabled, this feature prevents users with local administrator rights from modifying or deleting key Media Encryption registry keys or system files.

*Note* - We recommend that you disable this feature for system administrators as it prevents debugging of the Media Encryption client installation.

**Client profile reload**

By default the Media Encryption client only connects to the Media Encryption server at logon or when a manual profile reload is instigated from the client or the server. Additional options can be configured to ensure that the profile applied is always current and based on location and status:

- **Only reload the profile on logon or network connection change**
  A profile reload will automatically be performed on logon and if the network connection status is changed, for example when changing from a wired network to wireless.

- **Check for updated profile every XXX minutes**
  An automatic profile reload can be performed at scheduled intervals to ensure that the Media Encryption policy is always up to date. This feature is particularly applicable where users do not log off of workstations/laptops regularly.

**Client log synchronization**

- **Immediately after an event occurs**
  With this option, selected the client workstation will perform an immediate connection to the Media Encryption Server (if available) and upload the latest audit log information.

- **Every day at _____**
  The client workstation can be configured to upload the latest log information every day at a defined time.

- **Every _____ minutes**
  The client workstation can be configured to upload the latest log information at defined intervals.
**WebRH support**

The Use WebRH profile for challenge/response option allows users to remotely recover or reset passwords for EPM encrypted devices. Perform the following steps to import the webRH profile:

1. Enable **Use webRH profile for challenge/response** and then click **Import**.
2. Select and open the desired webRH profile.
3. Enter the webRH profile security password.
Exporting Profile Templates

You can export profile templates for backup purposes and for installing standalone and remote users.

1. In the Administration Console, right-click a Profile Template and select Export. The Profile Export Wizard opens.

2. On the Profile Type page, select a profile export format:
   - **DNP Format**
     The DNP format enables the system administrator to export a profile to a protected file that can be applied by the user to enable remote and temporary profile changes.
   - **XML Format**
     The XML format is used for manual profile changes only. This format can only be applied by system administrators. This format should also be used when updating the default.xml prior to client installation.
3. On the **Computer Profile** page, select one of the following options that determine which specific computer group profile(s), if any, are applied to the exported profile.

- **Export profile as if loaded on any computer**
  No computer group profile is applied to this profile

- **Export profile as if loaded on a specific computer**
  Click **Browse** to select a computer using the filter window. The profile associated with the computer group to which this computer belongs is applied to this profile.

  Click **View** to see the resulting composite profile
Exporting Profile Templates

4. On the **DNP Restrictions** page, specify endpoint computers that are authorized to import this profile.

   ![Profile Export Wizard](image)

   Enable one or more of the following options as required:
   - **Profile can be loaded only on a machine with a specified name**
     This profile can be imported only to computers specified in the designated field, which contains a comma-separated list containing the NETBIOS computer names. You can use the '*' and '?' wildcard characters to specify multiple computers.
   - **The exported profile will expire on a specified date**
     This profile is valid only during the period specified in the designated fields. Once the expiration time is passes, the computer reverts to the previously applied profile.
   - **Apply only to some users of the machine**
     This profile can only be imported by the user type selected in the drop-down list.

5. On the **DNP Password** page, enter and confirm the user import password.

6. On the **File Name** page, browse to or enter a fully qualified path and file name for the exported file.
7. On the **Completing Profile Export Wizard** page, click **Finish** to confirm and complete the export,

For standalone client installations, you can copy the exported profile to the Media Encryption Client installation folder (default.xml). This profile will be used for future installations when a Media Encryption Server is not present.

**Note** - To update an existing default policy (XML format) the machine must be logged on with local administration rights.
Chapter 4

Users and User Groups

This chapter describes the process defining and working with users and user and user groups.

Media Encryption Server is designed for use with Windows and Novell NDS domain networks. Typically, new users are defined automatically during the process of synchronizing Media Encryption user groups with domain groups.

Before defining users and user groups, it is essential that you first define the default profile and appropriate custom profiles. Refer to “Working with Profile Templates” on page 51 for details.

In This Chapter

- Working with Users
- Working with User Groups

page 92

page 95
Working with Users

This section describes the process of working with individual Media Encryption users. Individual users normally belong to one or more user groups, from which they inherit their profile settings. You can also define custom profile settings for individual users that override inherited settings.

Media Encryption Server is designed for use on Windows domain and Novell NDS networks. New users are normally created automatically by the process of synchronizing Media Encryption groups with their domain group counterparts. Refer to “Working with Group Synchronization” on page 105 for details.

Defining New Users

Since individual users are imported from Windows or NDS domains, you select the new users to import from the domain user database.

To define new users:
1. Right-click the Users branch in the Administration Console.
2. In the Select Users or Groups window, enter the user name or a part of the user name as a search criteria in the Enter the object names field.

You can click Advanced to work with more complex search criteria.
3. Click **Check Names** (or **Find Now** if using the advanced criteria). If more than one name meet your search criteria a window opens showing all matching users.

4. Select one or more names from the list and click **OK**.

5. Click **OK** in the **Select Users or Groups** window to complete the operation.
Creating Custom User Profile Settings

You can create custom profile settings for individual users, which override inherited settings.

To Create custom profile settings for an individual user:

1. Right-click on the desired user in the Administration Console and then elect Properties from the option menu.

2. In the User Properties window, click the Profile tab.

3. Enable the Define custom settings option and click Edit.

4. Define the individual profile settings as required. Refer to “Working with Profile Templates” on page 51 for details.
Working with User Groups

This section describes the procedures for defining user groups. You can create a Windows domain or Novell NDS user group using the New Group Wizard or you can create a group automatically when synchronizing Windows domain or Novell NDS groups. In either case, the process creates the group and automatically creates user

In This Section

Creating a User Group using the Wizard page 96
Creating a User Group by Synchronizing with a Domain page 99
Custom Profiles for Users and Groups page 101
Adding Users to Groups page 101
Offline Users page 102
Creating a User Group using the Wizard

Note - You should define your profile templates prior to defining users and user groups.


2. In the Name window, enter a suitable group name and group description.

3. In the Configuration window, select one or more profiles and then click >> to apply them to this group. You must assign at least one profile to the group.
When assigning multiple profiles to a group, profile settings apply according to the hierarchy as described in “Profile Priority and Inheritance” on page 50.
4. In the **Users** window, add users to this group.

- To create an empty group, select **Create an empty group** and click **Next**.
- To add users from a Windows domain or a Novell NDS group, select **add all users from a domain/NDS group** and click **Browse**. Search for and/or select the domain and group you wish to import using the Windows or Novell windows.
- Enable the **Synchronize this Media Encryption Group with domain/NDS group** option to ensure that the Media Encryption group remains synchronized with the Windows Domain group or Novell NDS group. New users added to the domain group and users who are removed from the Windows or NDS domain group are automatically synchronized with the Media Encryption database.
5. Click **Finish** to complete the definition process.

---

**Creating a User Group by Synchronizing with a Domain**

1. Right-click the Group branch and choose New > Group of users synchronized to domain/NDS group.

2. In the **Select Group** window, select the domain or NDS group:
3. Select the required group options including automated synchronization in the **Group** tab:

![Group tab screenshot]

4. On the **Profiles** tab, select the desired profiles from the list and click **Add**.

5. If you wish to define custom profile settings for this group, select the **Define custom settings for this group** option and then click **Edit**.

![Profiles tab screenshot]
Custom Profiles for Users and Groups

You can define custom profile settings for individual users and groups, which override all templates assigned to a user. Users that with custom profile settings are automatically added to the Special Users group.

Note - As long as users remain in the Special Users group they maintain their custom profile settings despite synchronization with their original domain groups.

If the system administrator later wishes to reassign the original group profile to the user, the following can be done:

a. Drag and drop the user back into the original Media Encryption group.

b. Delete the user from the Users with custom profiles group and either run a manual domain synchronization or wait for the next scheduled synchronization every XX minutes, as specified.

Adding Users to Groups

1. Right-click a user group and select Add users to group.

2. In the Select Group window, select the Windows domain or Novell NDS group to import:

3. Click OK to complete the task.

Note - You cannot add users to existing groups in this manner if the Synchronize with Windows/Novell Domain option is enabled. If you wish to manually add users to a group, define a group and disable the Synchronize with Windows/Novell Domain option for that group.
**Offline Users**

Media Encryption can be configured to assign different access rights when machines are on and off the network. This is particularly desirable for laptop users where different access rights are required. For example, disabling WiFi access when the laptop is on the network and enabling it when offline.

Offline profile settings can be edit by right-clicking and selecting Properties. Either the default profile can be applied or Define custom settings for this user can be selected:
Working with Existing Group Settings

This section describes the process for viewing and modifying settings and profiles for user and computer groups.

To Work with group properties:
1. Right-click the group and select Properties. The Group Properties window opens.
2. On the Group tab, edit the group name and description. The configuration profile can be changed and domain synchronization settings modified.
3. On the Profiles tab, specify the profiles that apply to the current group together with their order of precedence (hierarchy).

   ![Management Properties dialog box]

   **Note** - You can edit the selected profile by clicking **Edit**. Use this capability with caution, since any modifications made to a profile apply to all groups and users sharing the modified profile.

   a. To add a new profile, click **Add** and select a profile from the list.
   b. To delete a profile, select it and click **Remove**,
   c. To change the order of precedence, select a profile and click the **Up** or **Down** to move it to the desired location.
Working with Group Synchronization

Windows domain group synchronization ensures that user groups remain synchronized with Windows and NDS domain user groups. Synchronization settings determine the frequency at which Media Encryption groups are synchronized with their corresponding Windows or NDS domain groups.

You can also choose to allow users to be members to belong to more than one Media Encryption group and define the group profile priority when users belong to more than one group.

To work with group synchronization settings:

Right-click on the User Groups tab and select Properties. The User Groups Properties window opens.
Defining Synchronization Frequency

To define the frequency at which Media Encryption groups are synchronized:

1. In the User Groups Properties window, click the Advanced tab.

2. Enable the Synchronize every option and specify the time (in hours or minutes) between synchronizations in the designated fields.

3. Click Synchronize now to synchronize groups immediately.
Working with Multiple User Groups

By assigning users to multiple Media Encryption groups, you apply profile settings according to priorities as described in “Profile Priority and Inheritance” on page 50.

**Warning** - do not assign users belonging to multiple Windows or NDS domain groups to multiple Media Encryption groups. In this scenario, such users will, during synchronization, be automatically assigned to the last user group in the precedence order and removed from all other Media Encryption groups.

To allow users belong to multiple Media Encryption user groups:

1. In the User Groups window, click the Advanced tab.
2. Enable the **User can be a member of multiple Media Encryption groups** option.
3. The groups to which the user belongs appear on the **Group Order** tab. Use the **Move Up** and **Move Down** buttons to define the group profile priority.

![User Groups Properties](image)

**Note** - As long as the user remains in the **Users with custom profiles** group, their custom profile settings will always override settings that apply to groups profiles.

To require that users belong to only one Media Encryption group:

1. In the User Groups window, click the Advanced tab.
2. Enable the **User can be a member of one Media Encryption group** option.
This chapter describes the process defining and working with computers and computer groups.

In This Chapter

Working with Computers  page 110
Working with Computer Groups  page 115
Media Encryption automatically recognizes client computers when they connect to the protected network. New endpoint computers receive default configuration settings and do not belong to any computer group. You can change these settings as required.

Computers View

To view details of connected client computers, click on the Computers branch in the Administration Console.

The following information appears in the details pane:

- **Computer Name**: Computer NETBIOS name
- **Last Known IP**: Last known IP address of this client computer
- **Last connection time**: Time and date of the last successful profile download from the server
- **User account**: User name of the last user to log on to this computer
- **Logged on?**
  Indicates if a user is currently logged on

- **Installed drivers**
  Currently installed Media Encryption components:
  DM = Device Manager
  PSG = Program Security Guard
  RMM = Remote Media Manager

- **Active drivers**
  Current status of installed Media Encryption components

- **Client version**
  Media Encryption client version number

- **Group Name**
  Name of the computer group that this computer belongs to

- **License Status:**
  Indicates whether the selected computer is covered by a license

- **License Features:**
  Features licensed for this computer
  PM = Port Manager
  ME = Media Encryption

Endpoint computers with one or more Media Encryption components disabled are marked with a light blue icon. Endpoint Computers with no license are marked with a red circle and white cross. This can happen if there are more endpoint computers connected than permitted by your license.

The following actions are available on the right-click option menu:

- **Refresh Host**
  Forces the selected computer(s) to re-register with the server.

- **Reload Profile**
  Forces the selected computer(s) to download the currently assigned profile,

**Note** - Reloading the profile on all computers simultaneously is recommended because it may cause excessive network traffic.
Filtering the Computer List

On large networks, it is often desirable to display a subset of connected computers according to defined criteria. Media Encryption provides a useful filter utility for this purpose.

To filter the list of connected computers:
1. Click the **Filter** toolbar icon.
2. In the **Configure Filter** window define filter criteria as appropriate.
   a. Select a category and comparison type from the designated lists.
   b. Enter or select a comparison value as appropriate.
3. To create additional filter criteria, select either **And** or **Or** then click **More**.
4. Click **OK** when finished. Only computers matching the filter criteria appear in the details pane.

Working with Computer Settings

You can modify default or previously defined computer settings. To do so, right-click on the desired computer in the details pane and select **Properties**. The **Computer Properties** window opens.
The **General tab** displays the following information:

- **Client ID**
  Client machines unique identifier

- **Client Version**
  Media Encryption client version

- **Computer name:**
  Selected computer NETBIOS name

- **Last known IP**
  Last known client computer IP address

- **Connection Time**
  Time and date of the last client connection

- **Last User**
  Name of the last user who logged onto this client computer

- **Is Logged on**
  Whether the selected computer is currently logged onto the network

- **License Status:**
  Indicates whether the selected computer is covered by a license.
License Features
Features licensed for this computer
PM = Port Manager
ME = Media Encryption Configuration

Configuration Tab
You can disable or enable the following Media Encryption features for the selected computer:

- Program Security Guard
- Removable Media Manager
- Device Manager

Note - When disabling these features, they cannot be re-enabled until the current user reboots or logs off. Alternatively, you can re-enable these features by selecting them and clicking Apply.

After disabling any of the features, you may experience a slight delay in updating the selected client machine. To view the current status of a machine right-click on the computer and select Refresh. The Drivers column will display the current feature status.
Media Encryption typically assigns profiles based on the user name supplied when logging on. However, in many cases it is preferable to assign computer specific profile settings. Computer specific settings are useful where devices on specific computers must be accessible to any user that logs on (for example, printers, scanners, network accessible storage, etc.).

Computers automatically appear in the Administration Console when connected to the Media Encryption server. The profile settings that apply to a specific computer are determined by the computer group to which it belongs. Computer group profile settings may be defined to override user and user group profiles. If a computer does not belong to any groups, the user profile settings apply.

**Tip** - Since computer group profile settings may be configured to override user settings, make certain that computer group profiles contain settings that guarantee access to safe devices appropriate for public use. Avoid using computer group profiles to block access to devices unless you intend to block access for everyone using the computer.

Avoid assigning user group profiles to computer groups unless you are absolutely certain that you want to apply these settings to everyone using the computer.
Creating a New Computer Group

To create a new computer group:


2. In the Name window, enter a suitable group name and group description.

3. In the Configuration window, select one or more profiles and then click >> to apply them to this group. You must assign at least one profile to the group.
4. Click **Finish** to complete the definition process.
Adding Computers to a Group

Computer based profiles can be assigned to machines that have already registered with the Media Encryption Server and appear in the computers node.

Searching for Computers

You can add one or more computers to a group by searching all connected computers using filter criteria.

To add a computer to a computer group:

1. In the Administration Console, right-click the desired computer group and select **Add computers to group**.

2. In the **Select Media Encryption Client Computer window**, enter search criteria for and click **Find matching computers**. The computer name, last known IP address and/or last known user name are available as search criteria. You can use ‘*’ as a wildcard character.

3. Select one or more computers from the resulting list and click OK to add them to the group.

Using Drag and Drop

To add computers to a group from the Administration Console, simply select the computers and drag them to the desired computer group.
Working with Computer Group Properties

You use the Computer Group Properties window to manually edit computer group properties, many of which are not available when using the wizard.

To work with computer group properties:

In the Administration Console, right click on a group and select Properties. The Group Properties window opens.

Group Tab

- **Name and Description:**
  Enter or edit the group name and description as required

- **Computer group profile priority**
  - **User profile overrides computer profile**
    With this option selected the computer based profile will be applied first and the user based profile will override settings if defined.
  - **Computer profile overrides user profile**
    The computer based profile will override user and user group profiles if settings are defined.
• **Offline Profiles**
  
  – **Disconnected computers use cached profiles (Default)**
    Use the last downloaded profile when unable to connect to the Media Encryption Server.
  
  – **Disconnected computers use offline profiles**
    Use the offline users policy when unable to connect to the Media Encryption Server.

**Profiles Tab**

You can assign existing profiles to this group and optionally assign custom settings that override all other profiles.

**To assign profiles:**

1. In the **Properties** window, click the profile tab.

![Profiles Tab Image]

2. On the **Profiles** tab, select the desired profiles from the list and click **Add**.
3. If you wish to define custom profile settings for this group, select the **Define custom settings for this group** option and then click **Edit**.
**Licensing Tab (Enabling and Disabling Features)**

In the **Licensing** tab, you can enable or disable the Port Management and Encryption Profile Management features for computer groups.

To disable a feature, enable the designated check box. To enable the feature, clear the check box.

If neither of these check boxes are enabled, both Port Management and Media Encryption are enabled for the computers in this group.
Chapter 6

Monitoring and Auditing

This chapter describes how to monitor installed Media Encryption clients, create alerts and reports, view logs and audits etc.

In This Chapter

Alerts  page 124
Logs  page 126
Removable Media Log  page 131
Reports  page 134
Alerts

Media Encryption Server can generate email alerts sent to specified administrators or managers for administrator-defined events.

Note - It is important to note that Alerts will only occur instantly if the client log synchronization for the alerted events has been set to Alert or client log synchronization is set to Immediately after an event occurs within the Audit Events tab.

Creating a New Alert

To create a new alert:

1. Right-click on the Alerts node and select New > Alert.

2. On the General tab, enter a suitable alert name in the designated field.

3. Enable the Alert on selected events option and then enable one or more events that will trigger an alert. Clear those events that you do not want to trigger alerts.

   Warning - Never enable the Alert on all events option. This will create a massive volume of unwanted email with the potential to overwhelm your email server.

   Make certain that the actions that do generate alerts do not create an excessive email alerts.
4. On the **User Groups** tab and enable one of the following options:
   - **All Groups**
     Monitor all user and computer groups.
   - **Selected Groups**
     Monitor selected groups only. For large organizations, it is advisable to create custom alerts for each group.

5. On the **Action** tab, click **Add** to add a new email address where the alerts are sent. Enter the required email address and click **OK**. Repeat this process for all required email addresses.

   You can edit or remove email addresses by clicking the designated buttons.
Logs

Media Encryption logs contain entries for selected events as defined in profiles. Refer to “Auditing Settings” on page 67 for details regarding selecting events for logging. Log entries are initially stored on client computers and then uploaded to the server at predefined intervals. The log displays only those entries that have been uploaded to the server.

To display the log and individual log entries:


Each log entry is assigned a unique ID number. The type of alert and its severity is symbolized by the color of the icon. Detailed information of a log can be viewed by double-clicking on the event. The following information is displayed:

2. Navigate to and double-click the desired entry to display details of the event.
Log Event Tab

- **ID**
  Sequential record number assigned to each event

- **Unique ID**
  Unique ID assigned to each event

- **Time**
  Time and date at which the event occurred

- **Event**
  Event type

- **Alert Sent**
  Indicates whether an email alert was sent

- **User ID**
  User logged on when the event occurred

- **User Account**
  Full domain user name logged on when the event occurred

- **Computer Name**
  Network computer name

- **Event Source**
  Media Encryption feature generating the event

- **Message**
  Specific information describing the event.
**Device Information Tab**

The **Device information** tab shows additional information from the Device Manager audit log. This information details authorized and blocked devices and can be used to add new device IDs.

To add a new device to the **Device Manager** tab click **Add this device to device manager**, this will open the Device Manager Configuration Editor, see section “**Device Manager**” on page 29.
Filtering the Log

You can filter the log to more easily view entries of particular interest.

To filter the log:

1. Click the Filter toolbar icon.
2. In the Configure Filter window define filter criteria as appropriate.
   a. Select a category and comparison type from the designated lists.
   b. Enter or select a comparison value as appropriate.
3. To create additional filter criteria, select either And or Or and then click More.
4. Click OK when finished. Only computers matching the filter criteria appear in the details pane.

Exporting Logs

It is possible to export a copy of the log files to a .txt or .csv file format for use in other applications or for backup purposes.

1. Right-click the Logs branch in the Administration Console and select Export List.
2. Choose the desired export file type (.txt or .csv) and filename.
3. Click Ok to complete the export process:
Archiving Log Entries

Over a period of time, logs files may become large, containing many thousands of entries. It is advisable to periodically archive and then delete older events. You can configure Media Encryption to automatically archive older events according event age or manually archive them.

To automatically archive log entries:
1. Right-click the Logs branch in the Administration Console and select Properties.

2. In the Log Properties window, set the Archive Period to archive events older than the specified number of days. (default = 30 days)

3. Enable the Archive log automatically option and set the day of the week and starting time for the archive process.

4. Enter the path to the log archive folder in the designated field.
Removable Media Log

Media Encryption maintains a log of file operations on removable media and CDs/DVD devices. The log includes file creation, deletion, move, rename, read and write events.

To display the Removable Media Log:
1. Select the Removable Media Log branch in the Administration Console. The default view shows a summary of the top ten active users and active computers as shown below:

   ![Removable Media Log Summary](image)

   - To display the full log, right-click Removable Media Log and select View > Complete log.
   - To return to the summary view right-click Removable Media Log and select View > Summary.

2. To view user or computer details and/or modify the applicable profile, select an item from the summary list and then click the Properties button to the right of the pane.

3. To view the event list for a user or computer, select an item from the summary list and then click the Events button to the right of the pane.
Filtering RMM Log Events

The Removable Media Manager log provides powerful filter capabilities that display specific events according to filter criteria.

Predefined Filter Criteria
Select one of the following from the Media events to process list:

- Last 24 hours
- Last 7 days
- Last 30 days

Custom Filters
To filter the RMM log:

1. Click the Filter toolbar icon or click the Edit button in the upper right-hand corner for the RMM Log window.
2. In the Configure Filter window define filter criteria as appropriate.
   a. Select a category and comparison type from the designated lists.
   b. Enter or select a comparison value as appropriate.
3. To create additional filter criteria, select either And or Or and then click More.
4. Click OK when finished. Only entries matching the filter criteria appear.

Viewing Individual RMM Events
To view details on an individual RMM event:
Double-click an event. The Log Event window opens.
CD and DVD Events Log

Because of the large number of CD and DVD events, a separate log file is maintained outside of the SQL database.

Removable Media Log Archival

Over a period of time, logs files may become large, containing many thousands of entries. It is advisable to periodically archive and then delete older events. You can configure Media Encryption to automatically archive older events according event age or manually archive them.

To automatically archive log entries:

1. Right-click the Removable Media Log branch in the Administration Console and select Properties.

2. Click the Log Archival tab.

3. In the Log Properties window, set the Archive Period to archive events older than the specified number of days. (default = 30 days)

4. Enable the Archive log automatically option and set the day of the week and starting time for the archive process.

5. Enter the path to the log archive folder in the designated field.

6. On the CD Audit tab, enter the path to the separate log archive file.
Reports

Media Encryption includes a comprehensive reporting engine that generates fully configurable HTML reports. A set of predefined report templates is included, which can serve as the basis for customized reports.

Creating Reports

To create a new custom report:

1. Right-click the Reports branch in the Administration Console and select New.
2. On the **Report Type** page, select a predefined report from the list.

3. The Report Parameters page contains a list of customizable parameters. The available parameters varies according to the report type. Select a parameter and click **Edit**.
4. On the **Set report parameter value** page enter a value or select a value from the list as appropriate. The list includes values appropriate for the chosen event.

5. On the **Generation Time** page, Select one of the following options:

- **Generate this report immediately**
- **Generate this report at the specified time**
  
  Select the date and time for the report to run.
6. On the **Summary** page, Review the definition and click **Next** to create the report.

![New Report Wizard](image)

If you selected **Generate this report immediately**, the report generator begins immediately. A progress bar shows the report generation progress.

**Note** - For large network, report generation may take a long time. Report generation runs in the background enabling normal operation of the administration console.
Reports
Chapter 7
DataScan

This chapter describes how to work with the DataScan feature.

In This Chapter

Introduction  page 140
Using DataScan  page 141
Understanding the XML Script  page 143
DataScan is a unique file-based protection feature that automatically prevents introducing potentially dangerous and undesirable file types on protected endpoint computers. Unlike traditional virus and malware scanners, DataScan does not scan files for known signatures or patterns. It allows or blocks files based solely on its file type as determined by both its internal structure and extension. In this way, the scanning algorithm effectively prevents introduction of prohibited files by simply changing the file extension.

Data Scan prevents users from creating, modifying or copying specific file types on local drives, network drives and removable media. By default this includes executables (.exe, .com, .dll), script files (Microsoft Office macros .vbs, .scr, .js, etc.) and other undesirable files (.mpg, .mp3, .mov, etc.)

If DataScan is designated as a device scanner for Removable Media Manager, no media or device that contains prohibited file types can be authorized until the offending files are deleted.
Using DataScan

DataScan is enabled by default as one of the scanners by which users can authorize removable media. Since DataScan is configured by default to block all executables, whether or not they are malicious, you may wish to substitute another anti-virus/malware product (such as those included in Check Point Endpoint Security Client) if you need to authorize some executable files on removable media.

You can run DataScan command line options to refine your level of detection as detailed in the section “Command Line Parameters” on page 148. This gives exact details of how to call DataScan to operate as desired. A general overview of its functionality is detailed in the next section named “Functionality”.

Functionality

Unzipping ZIP Files

ZIP files are automatically expanded and their contents examined for executable/unauthorized code. If not specified, any ZIP files will automatically fail a DataScan scan as their content is obviously unknown. If they are investigated and found to be free of executables, they will pass the scanning process and a disk that might otherwise have failed a DataScan scan will be authorized.

Microsoft Office Macros

DataScan can be configured to fail all macros (by default), or just viral macros when performing a scan.

Microsoft Outlook Files

Any Microsoft Outlook messages that are saved to a media device can be scanned for attachments with executable code. No matter how deep the executable code is buried, DataScan will find it. For example, if someone were to attach an executable to an email, send it to themselves, save this message to their hard disk, place this message in a zip file, which they then sent to themselves again and saved once again to hard disk, then DataScan would fail the resulting file if scanned. No matter how complicated the paper trail, DataScan will unearth the executable code.
Log File

If specified, a log file will be produced from the DataScan scan. If this scan then results in a failure, the offending file(s) can be identified and appropriate action taken in order for the media to be signed and therefore authorized access past the DataScan security wall. This saves any guesswork on the part of the user as to what files are preventing the disk being authorized, that is, assumed file deletions and unnecessary aggravation.
Understanding the XML Script

DataScan has a new XML data file containing the file definitions (XML is a mark-up language for documents containing structured information). The previous store for file binary information was a raw hex data file. However, by now using XML the source is open and easy to understand for all who use and may need to amend this file to better suit their requirements.

CheckDat.XML Contains All Possible File Types

The XML file in question is CheckDat.XML. This file contains information structures of all the possible file types DataScan needs to know about and whether they can be authorized or not. Having this XML file separated from the main executable files allows the ability to update the file types it can identify as necessary without requiring a rebuilt master binary file. Following this understanding, the XML file is stored uncompressed in the Check Point MetaIP Getting Started Guide setup suite to allow for an amended copy to replace the master pre-rollout.

File Types Checked in Order

There are currently 85 distinct file types to compare against a scanned file and these are detailed in the section “The XML script” on page 144. The file types are listed in the order in which they are checked for together with whether they pass or fail a media scan. The final column contains the structure type, of which there are 11; see the section “Structure Types” on page 147 for further details.

Looking at the list of file types, you can see most of DataScan’s file type detection is based on checking file signatures to determine type. The most common file types are the first types checked for, more complex file types - specifically more complex structure types - are located towards the end of the XML file. It is a balance for optimum performance.

Checking File to be not an Disguised COM File

If DataScan has compared all but the last four file types without identifying the scanned file, it then ensures that the file is not a disguised COM file with the final four file type checks. If the file is not identified after all 85 checks, DataScan is satisfied that the file is safe and reports it as being so.

Add In-house File Types

If you have an in-house file type that you want to be recognized by DataScan, you may edit CheckDat.XML accordingly, see the “Structure Types” on page 147 section for help and further details.
### The XML script

#### Table 7-1

<table>
<thead>
<tr>
<th>#</th>
<th>File Type</th>
<th>Pass/Fail</th>
<th>Structure Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>EXE file</td>
<td>FAIL</td>
<td>2</td>
</tr>
<tr>
<td>2.</td>
<td>COM file</td>
<td>FAIL</td>
<td>2</td>
</tr>
<tr>
<td>3.</td>
<td>Renamed EXE file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>4.</td>
<td>NetWare NLM</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>5.</td>
<td>PKZIP file with password protection</td>
<td>FAIL</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>PKZIP file with password protection (method #2)</td>
<td>FAIL</td>
<td>3</td>
</tr>
<tr>
<td>7.</td>
<td>PKZIP file (PASS/FAIL as zip contents are checked and result of the scan reflects that)</td>
<td>PASS/FAIL</td>
<td>1</td>
</tr>
<tr>
<td>8.</td>
<td>HYPER file (signature #1)</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>9.</td>
<td>HYPER file (signature #2)</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>10.</td>
<td>ARC or PAK file</td>
<td>FAIL</td>
<td>10</td>
</tr>
<tr>
<td>11.</td>
<td>PAK file</td>
<td>FAIL</td>
<td>10</td>
</tr>
<tr>
<td>12.</td>
<td>ZOO file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>13.</td>
<td>ARJ file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>14.</td>
<td>RAR file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>15.</td>
<td>Microsoft Expand file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>16.</td>
<td>Microsoft CAB file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>17.</td>
<td>S and S compressed file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>18.</td>
<td>S and S NT compressed file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>19.</td>
<td>XTREE ZIP file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>20.</td>
<td>LHA file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>21.</td>
<td>BAT file</td>
<td>FAIL</td>
<td>2</td>
</tr>
<tr>
<td>22.</td>
<td>Microsoft Outlook file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>23.</td>
<td>Microsoft Office file</td>
<td>PASS</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Microsoft Office file</td>
<td>FAIL</td>
<td></td>
</tr>
<tr>
<td>24.</td>
<td>Lotus Ami Pro file with auto-executing macros</td>
<td>FAIL</td>
<td>5</td>
</tr>
<tr>
<td>25.</td>
<td>Lotus Ami Pro file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>File Format</td>
<td>Status</td>
<td>Category</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>26.</td>
<td>Lotus Symphony / Windows Icon file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>27.</td>
<td>WinWord 1.0 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>28.</td>
<td>WinWord 2.0 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>29.</td>
<td>WinWord 6.0 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>30.</td>
<td>PCX v2.5 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>31.</td>
<td>PCX v2.8 file (with palette)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>32.</td>
<td>PCX v2.8 file (without palette)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>33.</td>
<td>PCX v3.0 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>34.</td>
<td>GEM Metafile</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>35.</td>
<td>Tag Image File Format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>36.</td>
<td>PC Paint file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>37.</td>
<td>JPEG/JFIF file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>38.</td>
<td>Windows 2.0 Paint file(Sig 1)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>39.</td>
<td>Windows 2.0 Paint file(Sig 1)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>40.</td>
<td>Windows 2.0 Paint file(Sig 2)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>41.</td>
<td>Windows 2.0 Paint file(Sig 2)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>42.</td>
<td>Windows 3.x format file / OS/2 Picture file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>43.</td>
<td>OS/2 Icon file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>44.</td>
<td>OS/2 Cursor file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>45.</td>
<td>OS/2 Color Icon file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>46.</td>
<td>OS/2 Color Pointer file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>47.</td>
<td>Clipboard file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>48.</td>
<td>Windows Card file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>49.</td>
<td>Excel file (Biff 2)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>50.</td>
<td>Excel file (Biff 3)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>51.</td>
<td>Excel file (Biff 4)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>52.</td>
<td>MS-Word file (v3/4/5)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>53.</td>
<td>WordPerfect file(v5.0/5.1)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>54.</td>
<td>Interchange file format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>55.</td>
<td>Sun Raster format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>56.</td>
<td>Creative Music Format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Result</td>
<td>Count</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>57</td>
<td>Soundblaster Instrument Format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>58</td>
<td>Soundblaster Instrument Bank format</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>59</td>
<td>MIDI file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>60</td>
<td>Windows 3.x group file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>61</td>
<td>Windows WAV file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>62</td>
<td>Data Interchange Format file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>63</td>
<td>Adobe Photoshop file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>64</td>
<td>Lotus 123 WK3 File marker</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>65</td>
<td>Lotus 123 Pic File Header</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>66</td>
<td>GIF file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>67</td>
<td>GIF file (signature #2)</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>68</td>
<td>Windows write program</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>69</td>
<td>Windows 3.x Calendar file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>70</td>
<td>HTML file containing 'Object' tag(s)</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>71</td>
<td>HTML file containing 'Script' tag(s)</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>72</td>
<td>HTML file containing 'IFrame' tag(s)</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>73</td>
<td>HTML file containing 'Embed' tag(s)</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>74</td>
<td>HTML file containing 'Applet' tag(s)</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>75</td>
<td>HTML file</td>
<td>PASS</td>
<td>2</td>
</tr>
<tr>
<td>76</td>
<td>Word 2 file with auto-executing macros</td>
<td>FAIL</td>
<td>4</td>
</tr>
<tr>
<td>77</td>
<td>Word 2 file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>78</td>
<td>Microsoft Works file</td>
<td>PASS</td>
<td>1</td>
</tr>
<tr>
<td>79</td>
<td>VBScript</td>
<td>FAIL</td>
<td>2</td>
</tr>
<tr>
<td>80</td>
<td>Not a renamed COM file</td>
<td>PASS</td>
<td>6</td>
</tr>
<tr>
<td>81</td>
<td>Data file</td>
<td>PASS</td>
<td>3</td>
</tr>
<tr>
<td>82</td>
<td>COM file (near jump detected)</td>
<td>FAIL</td>
<td>3</td>
</tr>
<tr>
<td>83</td>
<td>COM file (3 byte jump detected)</td>
<td>FAIL</td>
<td>7</td>
</tr>
<tr>
<td>84</td>
<td>COM file (call instruction detected)</td>
<td>FAIL</td>
<td>7</td>
</tr>
<tr>
<td>85</td>
<td>COM file (INT 21h function detected)</td>
<td>FAIL</td>
<td>8</td>
</tr>
<tr>
<td>86</td>
<td>MP3 file</td>
<td>FAIL</td>
<td>1</td>
</tr>
<tr>
<td>87</td>
<td>MP3 file</td>
<td>FAIL</td>
<td>2</td>
</tr>
</tbody>
</table>
**Structure Types**

The simplest types are '1' and '2', whereby '1' is checking the file signature and '2' is checking against the file extension. The remaining 9 structures are more complex, with formulas and embedded engines working on their sometimes complex instructions.

If you have in-house file types that you would like to be recognized by DataScan, we can create a custom XML 'file definitions' file for you, please contact Check Point [http://www.checkpoint.com/services/contact/](http://www.checkpoint.com/services/contact/).

**DataScan installed files**

As part of the Media Encryption software suite, all the files will be installed in the same install folder.

Additionally, DataScan now utilizes XML to store its file definitions and as such we have two new XML system DLLs in the master.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Platform</th>
<th>Installed to</th>
</tr>
</thead>
<tbody>
<tr>
<td>CheckDat.dll</td>
<td>Scanning engine</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;</td>
</tr>
<tr>
<td>ChkDat32.exe</td>
<td>Data Scan executable</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;</td>
</tr>
<tr>
<td>Cunzip32.dll</td>
<td>File unzipping engine</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;</td>
</tr>
<tr>
<td>Xmlparse.dll</td>
<td>XML system file</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;</td>
</tr>
<tr>
<td>Xmitok.dll</td>
<td>XML system file</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;</td>
</tr>
<tr>
<td>CheckDat.XML</td>
<td>XML file types store</td>
<td>All</td>
<td>&lt;Media Encryption file path&gt;CheckDatProfiles</td>
</tr>
</tbody>
</table>
Command Line Parameters

The DataScan command line parameters are as follows:

- **/NONSTOP parameter**
  if used, DataScan will not stop at the first executable file it finds, it will continue the scan through the entire media.

- **/UNZIP parameter**
  unzips pkzip files.

- **/VMACROS parameter**
  will only fail viral macros in Microsoft Office documents. The default is to fail all macros.

- **/NOHEADER parameter**
  will not create a header for the local log file, if specified. The default is to create a header.

- **/NOMAPI parameter**
  For the Microsoft Outlook .msg file scanning functionality to work properly machines must have MAPI support, (that is, Mapi32.dll on the machine). If, however, you know your machine(s) do not have this file, you can use this parameter and DataScan will not check for its presence.

- **/NEWRETURN parameter**
  returns '2' instead of '0' to stop users pressing Ctrl+Alt+Del and bypassing the scan process to illegally validate a disk, i.e., this key-press combination will terminate DataScan and return '0' by default.

  **Note** - Please note that this return code is strictly for communication between DataScan's scanning DLL and its calling program, you will not get a '0' return code. See section "DataScan Return Codes" on page 149 for more information.

- **/TIMEOUT parameter**
  the default time to pause after a bad scan or a scan with errors is five seconds, this allows you to see what the problem was in good time. If this is not sufficient, specify the number of seconds you wish the dialog to pause for.

  For example: /TIMEOUT=10 will pause for ten seconds.

- **/LOG parameter**
  specify a local log file path.

  For example: /LOG="c:\mylogfile.txt"
DataScan Return Codes

The .DLL that does the actual scanning will return a precise code to its calling program, ChkDat32.exe. In most cases, this will, in turn, either return a simple Disk passed or Disk has executables return code. However, if there were problems, ChkDat32.exe will add the hex sum 0x500 to the actual return code from the DLL, so we know that anything above this figure is an error.

ChkDat32's return codes

34 (0x22) DISK_PASSED
68 (0x44) DISK_HAS_EXES
1280+ (0x500+) - ERRORS.

To get the exact error, subtract 1280 from the return code, the result translates as:

XML Data File Errors

16 COULDN'T_OPEN_XMLFILE
17 COULDN'T_READ_XMLFILE
18 COULDN'T_GET_XMLFILE_FILESIZE
19 ERROR_SETTING_XMLFILE_PTR
20 NOT_ALL_XMLFILE_BYTES_READ
32 XMLFILE_CORRUPTED
33 XML_LOAD_FAILED

FILE Scanning Error

48 COULDN'T_OPEN_FILE
49 COULDN'T_READ_FILE
50 COULDN'T_GET_FILE_FILESIZE
51 ERROR_SETTING_FILE_PTR
52 NOT_ALL_FILE_BYTES_READ

General

256 OUT_OF_MEMORY
Appendix
Glossary of Terms

AES encryption
Advanced Encryption Standard using Rijndael block cipher. The industry standard for strong encryption.

Anti-Virus
Refers to software used for detecting computer virus infected code.

Anti-Virus Definition Files (DEF Files)
These type of files contain the latest virus information for use with the Sherlock Anti-Virus Scanner.

Authentication
The process for verifying that an entity or object is who or what it claims to be. Examples include confirming the source and integrity of information, such as verifying a digital signature or verifying the identity of a user or computer.

COM port
An interface on the computer that allows asynchronous transmission of data characters one bit at a time. Also called a communication port or com port.

.csv
The CSV (Comma delimited) file format saves only the text and values as they are displayed in columns of the active log. All rows and all characters in each entry are saved. Columns of data are separated by commas, and each row of data ends in a carriage return. If a cell contains a comma, the cell contents are enclosed in double quotation marks.
Default profile

The default profile is the profile that will be used by any users which logon to a Media Encryption Client machine that are not listed within the Media Encryption Server users/groups.

Digital signature

A string of code that is written to removable media devices to mark as authorized. The digital signature includes a checksum or the information stored on the device encoded with a customer ID.

Drivers

Refers to the Media Encryption Enterprise Client device drivers that provide the backbone to the security infrastructure.

Exempt Applications

Program Security Guard (PSG) prevents the introduction and authorized modification of defined file types. It is possible to build a list of applications that are exempt from PSG protection.

Filter

For Indexing Service, software that extracts content and property values from the Media Encryption database in order to index them.

Graphical User Interface (GUI)

Refers to the Media Encryption user interface on the client software.

Group Synchronization

The ability to synchronize Media Encryption Server user groups with groups within a Windows Domain network.

Host name

Details the workstation name on which an event was created.

ID

Is a unique identifier assigned to each log entry sequentially generated.

IP address
A 32-bit address used to identify a node on an IP internetwork. Each node on the IP internetwork must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). In this version of Windows, you can configure the IP address statically or dynamically through DHCP.

.iss

Is an InstallShield Silent response file used for storing silent installation configuration data.

LPT port

The input/output connector for a parallel interface device. Printers are generally plugged into a parallel port.

Master Boot Record (MBR)

The first sector on a hard disk, which starts the process of booting the computer. The Master Boot Record (MBR) contains the partition table for the disk and a small amount of executable code called the master boot code.

Media authorization

Media authorization defines the ability to grant access to a removable media device. Media authorization will often require certain criteria to be met before a digital signature is written to the device.

Media ID

During authorization of removable media a unique digital signature is written to the device. This digital signature is made up of a check sum of the information and a unique Media ID generated during installation of the server software.

MMC

You can use Microsoft Management Console (MMC) to create, save, and open administrative tools (called MMC consoles) that manage the hardware, MMC software, and network components of your Windows system. MMC can be run on the various Windows operating systems. MMC does not perform administrative functions, but hosts tools that do. The primary type of tool you can add to a console is called a snap-in. Other items that you can add include ActiveX controls, links to Web pages, folders, taskpad views, and tasks. There are two general ways that you can use MMC: in user mode, working with existing MMC consoles to
administer a system, or in author mode, creating new consoles or modifying existing MMC consoles. For more information about the differences between user and author mode.

**Profile template**

A profile template is a collection of Media Encryption Client settings that can be applied to users/groups.

**Program Security Guard (PSG)**

Program Security Guard provides a fully scalable method for preventing the introduction or new, and the modification of existing defined file types. The administrator can define the list of file types from the Media Encryption Server.

**RDS**

Check Point Deployment Server is a low cost software deployment tool.

**Removable media**

The term removable media describes any removable device that can be used to store and transport data/files. These devices include floppy disks, zip drives, memory sticks, USB flash memory, digital cameras.

**Service**

A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level. When services are provided over a network, they can be published in Active Directory, facilitating service-centric administration and usage. Some examples of services are the Security Accounts Manager service, File Replication service, and Routing and Remote Access service.

**SMS**

Microsoft® Systems Management Server 2.0 includes detailed hardware inventory, software inventory and metering, software distribution and installation, and remote troubleshooting tools. These integrated features make Systems Management Server 2.0 the most scalable way to reduce the cost of change and configuration management for Windows® based desktop and server systems. Systems Management Server 2.0 is built on industry-standard management protocols, ensuring compatibility with complementary management tools. Systems Management Server 2.0 is tightly integrated with Microsoft SQL Server™ and Microsoft Windows Server operating system, making it easier than ever to install, configure, and maintain Systems Management Server in any size network.
**Simple Mail Transfer Protocol (SMTP)**

When you're exchanging electronic mail on the Internet, SMTP is what keeps the process orderly. It is a protocol that regulates what goes on between the mail servers.

**TCP/IP**

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most popular network protocol, and the basis for the Internet. Its routing capabilities provide maximum flexibility in an enterprise-wide network. In Windows XP TCP/IP is automatically installed.

On a TCP/IP network, you must provide IP addresses to clients. Clients may also require a naming service or a method for name resolution. This section explains IP addressing and name resolution for Network Connections on TCP/IP networks. It also describes the FTP and Telnet tools that are provided by TCP/IP.

**Unique ID**

Is the unique ID number assigned to each event.

**Universal Naming Convention (UNC)**

A convention for naming files and other resources beginning with two backslashes (\), indicating that the resource exists on a network computer. UNC names conform to the `\SERVERNAME\SHARENAME` syntax, where SERVERNAME is the server’s name and SHARENAME is the name of the shared resource. The UNC name of a directory or file can also include the directory path after the share name, with the following syntax: `\\SERVERNAME\SHARENAME\DIRECTORY\FILENAME`

**USB - Universal Serial Bus**

An external bus that supports Plug and Play installation. Using USB, you can connect and disconnect devices without shutting down or restarting your computer. You can use a single USB port to connect up to 127 peripheral devices, including speakers, telephones, CD-ROM drives, joysticks, tape drives, keyboards, scanners, and cameras. A USB port is usually located on the back of your computer near the serial port or parallel port.
**User ID**

Details the user name of the user who was logged on when an alert was generated.

**VPN**

A VPN is an extension of a private network that encompasses links across shared or public networks such as the Internet. VPN connections leverage the IP connectivity of the Internet and use a combination of tunneling and data encryption to securely connect remote clients and remote offices.
create new computer
group 115
create synchronized to
domain group 99
synchronization order 107
synchronization settings 105
synchronization,
definition 152

H
Hard drive(s), external 35
Host name, definition 152

I
ID
definition 152
media ID, export 45
media ID, import 45
site ID, import 37
Import
media ID 45
site ID 37
Infrared port(s) (IrDA) 35
Installation
Datscan 141
Internet Explorer trusted sites 80
IP address, definition 152
Iss file, definition 153

K
Key recovery, see EMP key recovery

L
License(s)
handling, overview 15
Log
archival 130
archival, removable
media 133
Datscan 142
export 129
removable media log 131
synchronization 84
LPT port, definition 153

M
Machine-specific settings 115
Master Boot Record (MBR),
definition 153
Media authorization
automatic 59
definition 153
Media ID
definition 153
export 45
import 45
MMC, definition 153
Mode
offline 64
Modem(s) 35

O
Offline
access 64
mode 64
profile 120
Optical device(s), see CD/DVDs

P
Password(s)
Attempts 66
constraints 65
recovery 85
PCMCIA memory 35
Ports
COM 36, 151
IrDA 35
LPT 36, 153
Predefined filters 132
Printer(s) 35
Profile template(s)
Advanced tab 83
Auditing tab 67

R
RDS, definition 154
Read-only access 32, 57
Reload profile 84, 111
Removable media
definition 154
Removable media log
archival 133
overview 131
predefined filters 132
Removable Media Manager
disable by user 82
overview 45
Report(s)
create 134
schedule 136
RMM, see Removable Media
Manager

S
Server properties
Applications tab 28
Console settings tab 43
E-mail Configuration tab 42
General tab 26
licensing information 27
Security tab 38
Advanced permissions
User/group configuration 95
Utilities
system 25

V
VPN, definition 156

W
Windows CE Portable
Device(s) 36
Windows Portable Device(s) 36

X
XML format 86
XML script 143

T
Tape drive(s) 35
TCP/IP, definition 155
Trusted site ID
add 37
remove 37
Trusted sites, see EPM site
identification

U
Unique ID, definition 155
Universal Naming Convention
(UNC), definition 155
USB drive(s) 34
see also Removable media
USB, definition 155
User(s)
add to group 101
belonging to more than one
group 107
custom profile 101
ID, definition 156
offline 102

System utilities 25

WEB RH 85

V
VPN, definition 156

W
Windows CE Portable
Device(s) 36
Windows Portable Device(s) 36

X
XML format 86
XML script 143