CA DataMinder

Endpoint Integration Guide

Release 14.6

CA Technologies Product References

This document references the following CA Technologies products:

- CA DataMinder™

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: About Endpoint Integration

CA DataMinder endpoint agents are application plug-ins executing on the end user's workstation ('endpoint computers'). Endpoint agents monitor user activity, collect information, and implement capture and control actions in accordance with policy. Each endpoint agent is parented to a gateway server or directly to the central management server (CMS) itself.

Because all intelligence for identifying triggers and implementing actions is present on the endpoint computer, feedback to the end user (where stipulated by policy) is immediate. Furthermore, CA DataMinder can continue to operate as normal in the (temporary) absence of a connection to its parent gateway or CMS. Captured events and policy changes awaiting replication upwards are stored on the endpoint computer until its parent server is available again. Similarly, policy changes replicating down from the CMS are delivered as soon as the connection resumes.

Note: CA DataMinder servers and endpoint computers are organized into hierarchical branches, with the CMS as the top-level server. The CMS acts as a central repository for all policy details and captured data. Below the CMS, each branch of the hierarchy is optionally managed by a gateway server, and each gateway server can serve multiple endpoint computers.

This section contains the following topics:

Available Endpoint Agents

CA DataMinder supports the following endpoint agents:

Microsoft Outlook Agent

The Outlook endpoint agent can capture and control any Outlook-based email activity. On computers where both the Outlook and Internet Explorer endpoint agents are installed, CA DataMinder can also capture or control any web activity when Outlook is used as a web browser.

Lotus Notes Agent

The Notes endpoint agent can capture and control any Notes-based email activity.

File System Agent (CFSA)

You can use the Client File System Agent (CFSA), also known as 'Policy on Save', to control user attempts to copy files off the local hard disk. For example, the CFSA can monitor files being copied to removable storage devices (such as USB flash drives and SD cards), sync folders (such as DropBox), network locations, and writable CDs and DVDs. The CFSA can selectively block or allow a file and apply policy triggers based on a file's text content or properties. For example, it can force users to encrypt files being copied onto removable devices.

The CFSA can also scan the local hard disk and apply policy triggers based on a file's text content or properties. For example, it can categorize files based on their text content, and delete, replace or move unauthorized files.

Full details are in Client File System Agent (see page 45).

Print System Agent (CPSA)

The Client Print System Agent (CPSA), also known as 'Policy on Print', detects and controls attempts to print documents. It applies policy to the documents being printed and uses the results of policy processing to allow or block the print job. The CPSA can also disable the Print Screen button on a user's keyboard.

Full details are in Client Print System Agent (see page 85).

Network Agent

You can use the Client Network Agent (or 'network agent') to control web activity on endpoint computers. Specifically, the network agent can monitor HTTP requests. This activity includes attempts to post files and comments to web sites or to submit form data. It can also monitor attempts to check in files to SharePoint libraries.

Full details are in Client Network Agent (see page 95).

Application Agent

The Application endpoint agent can monitor usage of other desktop applications and capture application usage metrics.

More information:

Client File System Agent (see page 45)
Client Print System Agent (see page 85)
Client Network Agent (see page 95)

Endpoint Protection Continues Even If Parent Server is Unavailable

CA DataMinder continues to protect the endpoint if it is (temporarily) disconnected from its parent gateway or CMS.

All intelligence for identifying triggers and for implementing actions is present on the endpoint, and feedback to the end user (where stipulated by policy) is immediate.

Note: The encryption utility, CADLPEnc.exe, is also installed in the CA DataMinder installation folder on the endpoint. The CFSA uses this utility to encrypt and decrypt files that your users copy to removable devices such as USB drives.

What happens with non-replicated changes?

- Captured events and policy changes awaiting replication upwards are stored on the endpoint until its parent server is available again.
- Policy changes replicating downward from the CMS are delivered as soon as the connection resumes.

Note: For more information on replication behavior, see the Machine Administration chapter in the *Administration Guide*. For more information on the holding cache, see the Technical Information chapter in the *Platform Deployment Guide*.

More information:

Working Offline (see page 105)

Chapter 2: Endpoint Deployment

This section describes how to deploy CA DataMinder endpoint agents.

Note: Group Policy deployments are described in the next chapter.

This section contains the following topics:

Endpoint Requirements

The following are requirements for CA DataMinder endpoint computers:

Operating System

CA DataMinder endpoint agents are included in the client.msi and client_x64.msi installation packages.

Client.msi supports 32-bit versions of these operating systems:

- Windows XP (see note 1)
- Windows Vista (see note 2)
- Windows 7 (see note 2)
- Windows 8
- Windows Server 2003 (see notes 2 and 3)
- Windows Server 2008 (see notes 2 and 3)

Client_x64.msi supports 64-bit versions of these operating systems:

- Windows XP (see notes 1 and 2)
- Windows Vista (see note 2)
- Windows 7
- Windows 8
- Windows Server 2003 (see notes 2 and 3)
- Windows Server 2008 (see notes 2 and 3)
- Windows Server 2008 R2 (see note 3)
- Windows Server 2012 (see note 3)

Note 1: On XP computers, the Client File System Agent (CFSA) and Client Print System Agent (CPSA) require SP2 or later.

Note 2: We have not tested these operating systems with the current versions of client.msi and client_x64.msi.

Note 3: CA DataMinder endpoint agents support 'centralized applications' running on Windows Server. For these deployments, users access applications such as Outlook on a central server using, for example, Citrix or Remote Desktop Connection.

Important! For details about CA DataMinder and the Windows firewall, see the Known Issues section.

Memory

128 MB

Disk space

Allow approximately 45 MB for the CA DataMinder infrastructure plus an Administration console.

You also need sufficient free disk space to store captured data in a local database. (You can purge this captured data as soon as it has been replicated to the parent server.

Email integration

- Microsoft Outlook 2003, 2007, 2010, or 2013
- Lotus Notes 7, 8, or 8.5

Note: We recommend to use Outlook 2010 with "Cached Exchange Mode" enabled if the CA DataMinder client agent is installed. Disabling Cached Exchange Mode results in increased network traffic between the Outlook client and the Exchange Server.

Browser integration

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 8, 9, or 10

File system integration

The CFSA requires Windows XP SP2 or later.

Print integration

Before you install the CPSA, close any applications that are running.

For details, see Before Installing on Client Machines.

Consoles

To run the Administration console or Data Management console, you require:

- Microsoft Internet Explorer 7, 8, or 9

Note: If you are installing the Data Management console on Windows 2003 or XP, apply the hotfix described in the following Microsoft knowledge base article: http://support.microsoft.com/kb/950094.

Limitation of 32-bit Client.msi on 64-bit OS

When deploying a client package to a machine with a 64-bit operating system, you typically use client_x64.msi.

But if you want to use a single deployment across hosts with both 32-bit and 64-bit operating systems, you can deploy the 32-bit client.msi package to a 64-bit operating system. However, the client.msi package does not contain any 64-bit binary files. If you choose this deployment option, be aware that the following endpoint features are not supported:

- Client File System Agent
- Client Print System Agent
- Integration with 64-bit version of Microsoft Outlook
- Integration with 64-bit version of Microsoft Internet Explorer
- Application Monitor

Before Installing on Client Machines

Before you install CA DataMinder endpoint agents, note the following issues.

Create machine accounts before installing the client software

To simplify mass deployments, you can bulk create new client machine accounts and pre-assign machines to parent servers in advance of the CA DataMinder rollout. This enables you to deploy multiple client machines using a single source image (which identifies a single parent server) while ensuring that each client machine automatically connects to its 'correct' parent server immediately after installation.

To bulk create new accounts, use the Account Import feature to import the client machine details from a CSV file.

If deploying across multiple subnets

CA DataMinder is designed to operate across subnets. If some or all of your client machines are on a separate subnet to your CMS, computer name resolution must work in both directions.

Windows XP SP2 firewall

The firewall setting ‘Don’t allow exceptions’ must be turned off on the target machine. For details about CA DataMinder and this firewall, see the reference below.

Close all applications before installing the CPSA

Close down all applications that support printing before installing the CPSA, such as Microsoft Office applications. This ensures that the CPSA can detect print jobs sent from these applications. (If an application is already running when you install the CPSA, it will be unable to detect print jobs sent subsequently from that application.)

If you anticipate users printing .EMF files (a Windows graphics file format) directly from Windows Explorer, restart the endpoint computer after installing the CPSA to ensure that it can fully control attempts to print these files.

Client Machines - Manual Installations (setup.exe)

To manually install CA DataMinder endpoint agents

1. Verify that you have local administrator rights on the endpoint computer.
2. Find setup.exe in the root of your CA DataMinder distribution image. Run setup.exe to launch the CA DataMinder installation wizard.

   The Installation Type screen opens.
3. Click Advanced Installation.
4. In the Advanced Install Options screen, choose Endpoint Agents and then click Install.

   This launches the CA DataMinder client installation wizard in a separate window.
5. In the client installation wizard, navigate to the Custom Setup screen.
6. In the Custom Setup screen, select the components you want to install. If you choose:

   - File System Agent, you must configure your machine policies and user policies after installing.
   - Print System Agent, you must close down all applications before installing the agent.

   To install these components to a different location, click Change.

   To check whether the target volumes have sufficient free disk space for the selected components, click Disk Space.

   Important! If you install to a different location, the target path must not include folders whose names contain Far Eastern characters. The CA DataMinder infrastructure cannot handle these paths.
7. In the Connectivity screen:

   a. Choose the Enterprise Mode option. This installs the client machine as part of a general CA DataMinder deployment. You now need to specify the parent server.

      Note: Standalone Mode is described on Standalone installations.

   b. Enter the name or IP address of the parent server (either your CMS or a gateway server). The installation wizard tries to confirm that the specified server exists on the network. It does not check whether it is a valid CMS or gateway. If you specify the CMS or gateway by name instead of IP address, the client machine must be able to resolve this name.

   c. If the installation wizard is unable to connect to the specified parent server, for example, because it is not switched on or because you mistyped its address or name, the wizard adds a Bypass Server Validation check box to the screen when you click Next.

In this situation, either re-enter the correct parent server details or select this check box to bypass or skip the validation. If you choose to bypass the validation, make sure you correctly type the parent server name or IP address otherwise the installation will fail!

8. In the Service Accounts screen, specify the logon accounts used by the CA DataMinder service. By default, the infrastructure logs on using LocalSystem.
9. In the final wizard screen, click Install to start the file transfer.
10. Perform any necessary post-installation tasks before you start using CA DataMinder. See the reference below.

Server Name Resolution

When you deploy CA DataMinder to client machines, you will need to identify its parent server (the CMS or gateway) by name or IP address. If you specify the CMS or gateway by its *name*, you must ensure that the client machines can resolve this name. If they cannot do so, they will be unable to locate it. Choose a method of computer name resolution that suits the needs of your organization, for example, DNS or a WINS server.

Post-Installation Tasks

More information:

Customize the Intervention Dialog Banner (see page 19)
Customize the Intervention Banner (Network Agent) (see page 20)

Customize the Intervention Dialog Banner

(Optional) The endpoint intervention dialog displays a built-in banner with the CA Technologies logo. After installation, you can customize the banner image to display your company logo. The custom image can be in PNG, JPG, or BMP format. The recommended size is 419 pixels wide by 42 pixels high, but the dialog auto-adjusts to images with any widths within 402 and 800 pixels.

You can override the built-in dialog banner either by configuring the registry or by providing a file named CustomBanner.png. If the registry override is misconfigured, the built-in banner is used.

To use a custom image, do *one* of the following:

- Specify the path to the custom image, including filename, in the CustomBannerPath (REG_SZ) setting under both of the following keys. Create the key if it does not exist yet.

  32-bit:

  ```
  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA DataMinder
      \CurrentVersion\Userprocess
  ```

  64-bit:

  ```
  HKEY_LOCAL_MACHINE\Software\Wow6432Node\ComputerAssociates\CA DataMinder
      \CurrentVersion\Userprocess
  ```

- Name the image file CustomBanner.png and place it in both the <WGNINSTALDIR>\client folders:

  ```
  32-bit: C:\Program Files (x86)\CA\CA DataMinder\client\
  64-bit: C:\Program Files\CA\CA DataMinder\client\
  ```

Customize the Intervention Banner (Network Agent)

(Optional) The Client Network Agent (or 'network agent') displays a default intervention web page with built-in images. For example, the network agent displays an intervention web page when it blocks a data submission to a web site.

After installation, you can customize the images used, for example, to display your company logo. Provide your images in PNG format. You can override the built-in images by either configuring the registry, or by providing image files in a specific path.

If the registry override is misconfigured, the built-in images are used. The three default images are a "blocked" symbol, the CA DataMinder logo, and a wide background banner which allows the logo to appear to span the web page.

Image name	Registry Entry	Width x Height (pixels)
CustomLogo.png	CustomLogoPath	382 x 47
CustomRepeatingBanner.png	CustomRepeatingBannerPath	... x 47
CustomBlockedSign.png	CustomBlockedSignPath	99 x 90

To use custom images

Do *one* of the following:

- Specify the paths to your custom images, including their filenames, in the registry settings under *both* of the following keys. Create the registry values on the network agent host computer if they do not exist:

  On computers with 32-bit operating systems:

  ```
  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA DataMinder
      \CurrentVersion\Userprocess
  ```

  On computers with 64-bit operating systems:

  ```
  HKEY_LOCAL_MACHINE\Software\Wow6432Node\ComputerAssociates\CA DataMinder
      \CurrentVersion\Userprocess
  ```

- Name your custom image files CustomLogo.png, CustomRepeatingBanner.png, and CustomBlockedSign.png. Copy the images files to the \client subfolder on the network agent host computer. Find the \client subfolder below the CA DataMinder installation folder:

  On computers with 32-bit operating systems:

  ```
  C:\Program Files (x86)\CA\CA DataMinder\client\
  ```

  On computers with 64-bit operating systems:

  ```
  C:\Program Files\CA\CA DataMinder\client\
  ```

More information:

About the Client Network Agent (see page 95)

Command Line Operations

More information:

Installing with msiexec.exe (see page 21)
Uninstalling Client Machines (see page 23)

Installing with msiexec.exe

When using command lines to install CA DataMinder on client machines, you can use parameters to identify the parent server and specify a silent installation. You can also use transforms to prevent unauthorized uninstallations and install CA DataMinder Application Integration.

More information:

Identifying the Parent Server (see page 22)
Silent Installations (see page 22)
Other Available Transforms (see page 22)
Disabling Integration with the Outlook Browser (see page 23)

Identifying the Parent Server

When using command lines to install CA DataMinder on client machines, there are two possible methods for identifying the parent server (either the CMS or a gateway):

- **Using a property**

  The basic command line syntax for an installation is:

  ```
  msiexec /i <Path>\client.msi WGNPARENTSERVERNAME=<Server>
  ```

  Where <Server> is the name or IP address of the parent server. You can find details about the WGNPARENTSERVERNAME general variable in Command line parameters for Msiexec.exe.

- **Using the SetParentName.mst transform**

  You can use this transform file to identify the parent server. To create this transform, you run a provided script. Full instructions are given on Prevent automatic start-up: DisableAutostart.mst. The command line syntax is:

  ```
  msiexec /i <Path>\client.msi TRANSFORMS=SetParentName.mst
  ```

Silent Installations

Various msiexec.exe options let you specify silent or near-silent installations (or uninstallations). Full instructions are given in Command line parameters for Msiexec.exe.

For example, to specify a completely silent installation that requires no user interaction, the syntax is:

```
msiexec /i <Path>\client.msi /qn
```

Other Available Transforms

If necessary, you can use the ClientLockDown.mst transform to prevent users from uninstalling CA DataMinder with the Add/Remove Programs utility. The command line syntax is shown below.

```
msiexec /i <Path>\client.msi TRANSFORMS=ClientLockDown.mst
```

Disabling Integration with the Outlook Browser

You can use msiexec.exe variables to disable browser Integration in Outlook and Windows Explorer.

Outlook Browser

On computers where both the Outlook and Internet Explorer endpoint agents are installed, CA DataMinder can apply policy to web activity when Outlook is used as a web browser.

You can disable integration with Outlook *browsers* using the misiexec.exe variable WGNNOOUTLOOKBROWSER. For details, see the Technical Information chapter in the *Platform Deployment Guide*.

Windows Explorer Browser

The Internet Explorer agent can apply policy to web activity in Windows Explorer.

You can disable integration with Windows Explorer using the misiexec.exe variable WGNNOEXPLORER. For details, see the Technical Information chapter in the *Platform Deployment Guide*.

Uninstalling Client Machines

When uninstalling client machines, the syntax depends on whether you want to keep or delete the existing database:

- **Uninstall but keep the existing database**

  Use the following command line syntax:

  ```
  msiexec /x <Path>\client.msi
  WGNDELETEDATABASE=0
  ```

- **Uninstall and delete the existing database**

  Use the following command line syntax:

  ```
  msiexec /x <Path>\client.msi
  ```

- **Uninstall using the product code**

  You may need to do this if you cannot specify a path to the Client.msi file because, for example, the file is in a shared network folder but a network failure has made the folder temporarily unavailable. In the above commands, replace the reference to the source image, <Path>\client.msi, with this product code. Do include the {} brackets:

  {94FD0328-5120-432B-AE46-F30A312AEA95}

Snapshot Operations

This method involves taking a snapshot image of a CA DataMinder installation on a source machine, then transferring this image to multiple target machines (using a third-party tool).

There is no single term to describe this deployment method (or its variants). Other common names include ghost imaging, ghosting, disk-imaging and cloning, while the snapshot images themselves are also called wraps, wrappers or packages.

Snapshot installations break down into a six step procedure:

1. Prepare the source machine for a CA DataMinder installation.
2. Using your preferred software tool, create a baseline image of your source machine.
3. Install CA DataMinder.
4. Generate a snapshot image, based on the changes made by the installation wizard.
5. (Optional) To simplify any follow-up snapshots, we recommend you create and save a new baseline image at this stage.
6. Deploy the CA DataMinder snapshot image to your target machines.

These steps are described in the following sections.

More information:

Snapshot Considerations (see page 29)

Snapshot Installation

This section covers the general procedure for snapshot installations. The basic procedure is the same, regardless of which third-party tool you use. However, the exact procedure for generating the snapshot image will naturally vary depending on the tool.

Note: The snapshot image used when testing these instructions was a RapidInstall Package (RIP), created with Altiris RapidInstall 3.1. You may find other third-party tools to be equally effective but these have not been tested.

1. **Prepare the source machine**

   Some pre-configuration of the source machine is necessary to ensure that the final snapshot image contains the correct CA DataMinder installation information.

   a. Run the DisableAutostart.vbs script to generate the DisableAutostart.mst transform.

      Find this script in the \Support folder of the CA DataMinder distribution image.

      The transform prevents CA DataMinder starting automatically after installation. This is necessary to prevent your source machine starting the CA DataMinder service automatically after step 5.

   b. Run the following command:

      ```
      msiexec /i <path to client.msi> TRANSFORMS=<path to DisableAutostart.mst>
      ```

      Where client.msi is your administrative source image for client machines. Find a copy of client.msi in the \Windows folder in your CA DataMinder distribution image>.

   For details about DisableAutostart.mst and the TRANSFORMS property in Msiexec.exe commands, see the references at the end of this section.

2. **Create a baseline image**

   Using your preferred snapshot tool, create a baseline image of your source machine. This is an image of the machine before CA DataMinder has been installed.

   For example, if you are using RapidInstall 3.1, you can now set a baseline using the Altiris RIP creation wizard. Proceed to the Installing Applications screen, then stop and create a baseline image.

3. **Install CA DataMinder on the source machine**

   a. Launch the CA DataMinder installation wizard. To do this, run setup.exe in your CA DataMinder distribution image.

   b. In the Installation Type screen, choose Advanced Installation.

   c. In the Advanced Install Options screen, choose Endpoint Agents and then click Install.

      This launches the CA DataMinder client installation wizard in a separate window.

   d. In the Connectivity Screen, enter the name or IP address of the parent server.

      Alternatively, if you want a generic snapshot that can be easily customized and reused to install clients to different parent servers, you can enter a 'placeholder' IP address and select the Bypass Validation check box. This approach allows you to deploy several versions of the snapshot (for example, one for each department in your organization), with each version specifying a different gateway as the parent server.

      Note: The placeholder address can be the address of any real machine that is not a CMS or gateway server. You must specify a real machine, otherwise the installation will fail and the snapshot will be incomplete.

   e. The installation wizard now has all the information it needs. Click Install to start the file transfer. When this completes, go to step 4.

4. **Create a snapshot image of the CA DataMinder installation**

   Create a snapshot image of the changes made by the CA DataMinder installation wizard.

   For example, if you are using RapidInstall 3.1, you can resume the Altiris RIP creation wizard and proceed to the Build RIP screen.

   Typically, third-party tools let you configure the snapshot image, for example, to automatically reboot the target system after installation. Now is the time to configure the snapshot to meet your deployment requirements.

5. **Create a follow-up baseline image**

   If you anticipate a future need for follow-up snapshot images (for example, to install CA DataMinder features omitted from the original snapshot), we recommend you now create and save a follow-up baseline image at this stage. This is an image of the source machine *after* CA DataMinder has been installed. You can then retrieve and use this baseline to generate future follow-up snapshots.

6. **Deploy the CA DataMinder snapshot**

   To deploy the snapshot to your target client machines, choose any method that best suits your organization. For example, you can attach the snapshot to an e-mail and send it to your users; you can save the snapshot to a shared network location; or you can include it in a login script. However:

   - If you specified the actual parent server in step 2, no further steps are required. The snapshot is ready to be installed.
   - If you used a placeholder IP address in step 2, you (or the target users) must now modify the snapshot to replace the 'placeholder' address with the actual parent server. To do this, locate the startup.properties file once again. This is in the \System subfolder of the CA DataMinder installation folder. Find this line:

     ```
     default.parent=<placeholder parent>
     ```

     Where <placeholder parent> is the name of the machine whose IP address you specified in step 2. Now change this line to:

     ```
     default.parent=<actual parent>
     ```

     Where <actual parent> is the name or IP address of your CMS or a gateway server. See the previous column for an example file extract.

Follow-up Snapshot Installations

If required, you can deploy follow-up snapshot images to machines already running CA DataMinder. For example, if you initially chose not to deploy the Application Integration feature to client machines, you could configure a follow-up snapshot to have the additive, or cumulative, effect of installing Application Integration on top of existing CA DataMinder installations. The procedure is summarized opposite:

The basic idea is straightforward: On your source machine, you rerun the CA DataMinder installation wizard on your source machine and choose any new features you want; you then create and deploy a follow-up CA DataMinder snapshot. In detail, you must:

1. **Specify the follow-up baseline image**

   Using your preferred snapshot tool, start creating a new snapshot image. First, specify the baseline image.

   To ensure the follow-up snapshot only contains the latest modifications by the CA DataMinder installation wizard, you must generate the snapshot from a baseline image of your source machine *immediately after the original* CA DataMinder *installation*. This is why we recommend that you create and save a follow-up baseline image directly after creating the original snapshot. However, if you need to recreate this baseline, you must:

   a. Rebuild your source machine.

   b. Rerun the original CA DataMinder installation (step 5, If you want to customize the CA DataMinder installation, (for example, omitting the CA DataMinder consoles), do so in the Custom Setup screen; see step 3 in Manual installations (setup.exe).).

   c. Create a new baseline image.

2. **Modify the original CA DataMinder installation**

   Rerun the installation wizard and choose the new features you want to add (or the features you want to uninstall).

3. **Create a follow-up snapshot**

   Using your preferred snapshot tool, create a snapshot image of the changes made by the CA DataMinder installation wizard.

   Unlike the original snapshot, this time you do *not* need to edit startup.properties.

4. **Deploy the follow-up snapshot**

   Now deploy the snapshot to your target client machines, using any method that best suits your organization.

Snapshot Considerations

If you use snapshot deployment methods, we recommend that you generate a snapshot image on a source machine that has the same configuration as the target client machines. Specifically, the source machine must have the same operating system and same email application as the target machines.

Likewise, for Microsoft Outlook and Lotus Notes the source and target machines must use the same *version* of email application. For example, if the target client machines use Microsoft Outlook 2007, we recommend that the source machine is running Microsoft Outlook 2007 when you generate the baseline image.

SMS Operations

Note: CA DataMinder deployment has been tested using SMS 2.0 SP3 in conjunction with Windows 2000 SP2. CA DataMinder may deploy successfully using other versions of SMS and under other service packs, but these have not been tested.

You can remotely deploy CA DataMinder to client machines using Microsoft Systems Management Server (SMS). When deploying CA DataMinder using SMS, you base the deployment on a collection of machine accounts. Then you set up a software installation package for this collection. We recommend that you set up the package to use a scheduled, mandatory assignment; this ensures that CA DataMinder is installed to the client machines at the time when you want.

The SMS installation procedure comprises the following steps

1. Select a machine-based collection.
2. Create a new software installation package.
3. Specify the package folder containing the source files.
4. Define an installation program.
5. Choose the machines to act as package distribution points.
6. Create an advertisement containing the assignment schedule.
7. Deployment start time is defined by the assignment schedule.

These steps are described in the following sections.

Before Installing with SMS

Before using SMS to deploy CA DataMinder, there are some preliminary steps you must follow.

Discover the SMS Clients

Before installing with SMS, you must already have discovered the client machines and confirmed that the SMS client software has been installed on these machines.

Create an Administrative Installation Source Image: Client.msi

We recommend that you create an administrative installation source image (Client.msi) for your SMS clients to use. This enables client machines to install CA DataMinder directly from the network without generating excessive network traffic or requiring excessive free disk space on the client.

Create a Transform: SMSQuietUninstall.mst

Transform files let you apply customized configuration changes to a Windows Installer package. Here you can use a transform, SMSQuietUninstall.mst, to allow silent uninstallations. That is, the transform removes the need for user cooperation when uninstalling. If you require silent uninstallations, copy this transform into the same folder as Client.msi, your administrative installation source image (see above).

Note: To create this transform, you run a provided script.

SMS Installation

Note: These instructions apply to Microsoft Systems Management Server 2.0 SP3, in conjunction with Windows 2000 SP2. Other versions may successfully install CA DataMinder to client machines, but they have not been tested. For full details about using SMS, please refer to your SMS documentation. Of particular use is the white paper, 'Deploying Windows Installer setup packages with Systems Management Server 2.0'.

1. Open the SMS Administrator console and select the collection you want. This collection must contain all the client machines that require CA DataMinder. *Do not choose a user-based collection.*

   To add machines to a collection, you edit the Membership Rules. These are a property of the collection.

2. Now you must set up a new software distribution package. The simplest method is to use the Distribution Software Wizard.

   If you prefer to set up a package manually, the following steps provide the necessary details for the installation program, distribution points, and advertisement.

3. Create a new package and define its Data Source properties.
   - Select the folder containing your administrative installation source image.
   - Choose the option 'Always obtain files from source directory.' This permits you to change or update the source files in the administrative installation folder if necessary.
4. Create a new program for the package and define its properties:
   a. **General:** Enter the following program command line. This includes properties that identify the CMS or gateway server and apply a transform:

      ```
      msiexec /i <Path>\client.msi WGNPARENTSERVERNAME=<CMS>
      TRANSFORMS=SMSQuietUninstall.mst; ClientLockDown.mst; EnableAppmon.mst
      ```

      Note: Command line options for Msiexec.exe are defined on Command line parameters for Msiexec.exe.

      When you enter the program command line, note the following:
      - If you specify the CMS or gateway by name, you must ensure that the client machines can resolve its name.
      - If you will require silent uninstallations, you must include the SMSQuietUninstall.mst transform in the installation program.
      - If you want to prevent users from uninstalling CA DataMinder with the Add/Remove Programs utility, include the ClientLockDown.mst transform. Full instructions are given in Prevent automatic start-up: DisableAutostart.mst.
      - If you want to enable application integration (this enables CA DataMinder to monitor usage of desktop applications) include the Appmon.mst transform. Full instructions are given in Install application integration: EnableAppmon.mst.

   b. **Environment:** Specify when the program can run: Choose the option 'Whether or not a user is logged on'.
   c. **Advanced:** Specify the uninstall settings: Select the check box 'Remove software when no longer advertised', and enter the following registry key (the 'product code'). Do include the {} brackets:

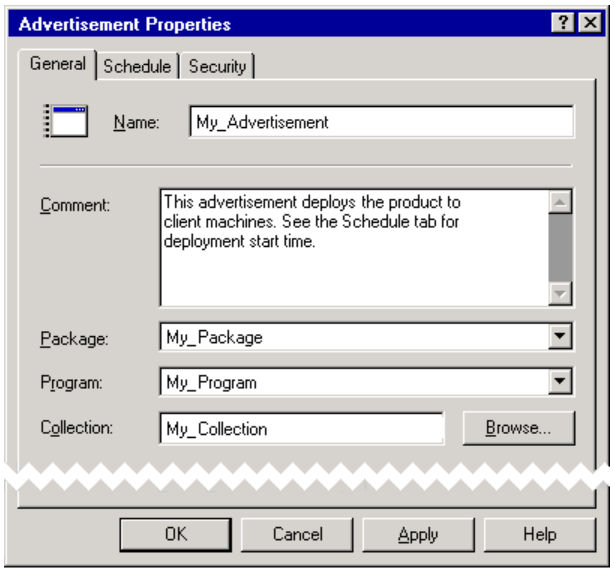
      ```
      {94FD0328-5120-432B-AE46-F30A312AEA95}
      ```

d. Now define the program distribution points for the package you created in step 2. These are the source machines from which SMS distributes the installation files contained within the package. To do this, use the New Distribution Points wizard:

```
Systems Management Server
- Site Database
  + Site Hierarchy
  + Collections
  - Packages
    - CA DataMinder Packages
      Access Points
      Distribution Points
      Programs
  - Advertisements
  - Product Compliance
```

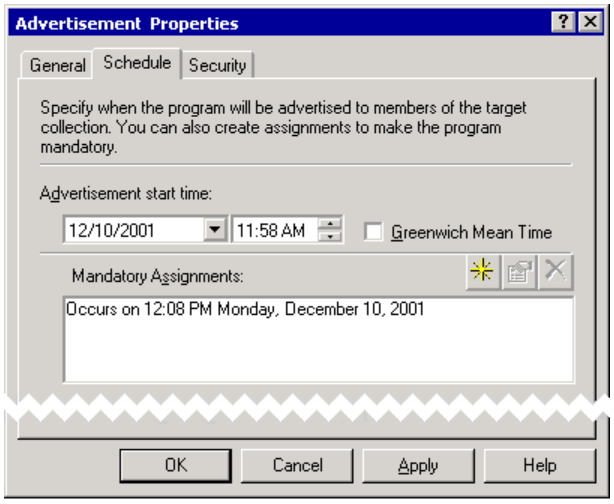
SMS Tree, Package distribution points and Advertisement

5. Now set up the package advertisement. First, define the General properties. You must select the Package (see step 2), the Program (step 4), and the Collection (step 1):



Advertisement Properties dialog, General tab

6. Next, define the advertisement Schedule properties. These specify when the package is advertised to SMS clients. We recommend that you schedule a Mandatory Assignment to ensure that CA DataMinder is installed on the target clients.



Advertisement Properties dialog, Schedule tab

7. When the advertisement is complete, SMS deploys CA DataMinder to the target clients as scheduled. Just before deployment, SMS warns users on the target machines that an installation is imminent.
8. As soon as the installation has completed, users must restart their browser, e-mail and other applications for the CA DataMinder integration features to start.

Note: Before you start using CA DataMinder, there are things you must do first.

More information:

Server Name Resolution (see page 19)
Before Installing with SMS (see page 30)
SMS Uninstallation (see page 34)

SMS Uninstallation

You can perform a standard uninstallation or a silent uninstallation.

Standard Uninstallation

You can use SMS to uninstall CA DataMinder from a client machine. Simply remove the machine account from the CA DataMinder collection. To do this, you edit the membership rules; these are a property of the collection. SMS then immediately uninstalls CA DataMinder from the target machines. If a browser or email application is open on a target machine, the uninstall goes ahead but does not complete until the user closes the application.

Silent Uninstallation

If you want to uninstall CA DataMinder silently, you must specify the SMSQuietUninstall.mst transform in the program command line when you set up the installation package. This transform removes the need for user cooperation when uninstalling.

More information:

Before Installing with SMS (see page 30)
SMS Installation (see page 30)

Integration with Centralized Applications

CA DataMinder can integrate with centralized applications running on a terminal server or accessed through a Citrix application server product.

Citrix Integration

More information:

Citrix Requirements (see page 35)
Command Line Installation for Citrix Endpoint Agent with SQL Server Database (see page 36)

Citrix Requirements

We have tested the following Citrix configuration.

Note: CA DataMinder may integrate successfully under other configurations, but they have not been tested.

Citrix Server

Product

Citrix MetaFrame XP Application Server for Windows, version 1.0 with Service Pack 2 and Feature Release 2.

Applications

Microsoft Internet Explorer 8 (8.0.6001.18702)

Microsoft Excel and Outlook 2007 SP2 (12.0.6425.1000)

Database

Microsoft SQL Server 2008

Note: Microsoft Jet is not a suitable database engine for CA DataMinder agents on Citrix servers.

Command Line Installation for SQL Server Databases

To configure CA DataMinder endpoint agents on a Citrix server to use a SQL Server database, run a command line installation.

The command line must use database variables to specify such parameters as the database type and name and the primary user credentials. See the next section for an example command.

Client Machines

Operating System

Windows 2003 Professional

Command Line Installation for Citrix Endpoint Agent with SQL Server Database

To configure CA DataMinder endpoint agents on a Citrix server to use a SQL Server database, run the following msiexec.exe command in restricted UI mode:

```
msiexec /i c:\client.msi
  WGNPARENTSERVERNAME=<parent>
  WGNDATABASETYPE=MSSQL
  WGNDATABASESERVER=localhost
  WGNDBPRIMARYUSERNAME=WGNUSER
  WGNDBPRIMARYPASSWORD=<password>
  WGNDBPRIMARYCREATEACCOUNT=1
  WGNDBSEARCHUSERNAME=WGNSEARCH
  WGNDBSEARCHPASSWORD=<password>
  WGNDBSEARCHCREATEACCOUNT=1
  WGNDBADMINUSERNAME=sa
  WGNDBADMINPASSWORD=<password> /qb
```

Where WGNDBADMINUSERNAME is the name of a database administrator login. For SQL Server databases, this login is typically 'sa'.

Note: Full msiexec.exe instructions and variable descriptions are available in the 'Technical Information' chapter of the *Platform Deployment Guide*.

Lotus Notes Integration

At install time, CA DataMinder modifies users' notes.ini configuration files to include the CA DataMinder Notes client agent as a Notes add-in. However, when Notes is running as a centralized application on a terminal server or accessed via Citrix, CA DataMinder is not always able to locate and update the relevant notes.ini files. If this problem is not addressed, this can mean that CA DataMinder integration fails for some Notes users, and that their Notes email activity is not monitored.

More information:

Updating notes.ini (see page 37)
Integration with a New Notes Installation (see page 37)
Integration with Existing Notes Installations (see page 37)

Updating notes.ini

To ensure that Notes integration operates correctly, you must ensure that each user's copy of notes.ini is updated to reference wgnemno.dll. Specifically, you must add this line:

```
EXTMGR_ADDINS=wgnemno.dll
```

Integration with a New Notes Installation

If you are deploying a centralized Notes installation for the first time, CA DataMinder amends the 'base instance' of notes.ini. You must then copy this base instance to all users' home drive (as recommended by IBM—see the note below).

1. Run a shared installation of Notes on the terminal server or Citrix server.
2. Install the CA DataMinder Notes client agent on the terminal server or Citrix server.
3. CA DataMinder uses the Path registry value to locate and edit the 'base instance' notes.ini. You do not need to manually update notes.ini to reference the wgnemno.dll add-in (see above).

   Find this registry value in the following registry key on the terminal server or Citrix server:

   ```
   HKEY_LOCAL_MACHINE\Software\Lotus\Notes\6.0
   ```
4. Copy the base instance notes.ini to each user's home drive.

Note: For Terminal Services and Citrix MetaFrame implemented on IBM Netfinitity Servers, IBM provide recommended installation procedures for Lotus Notes. For details, visit www.redbooks.ibm.com.

Integration with Existing Notes Installations

If you have already deployed a centralized Notes installation, you must install the CA DataMinder Notes client agent on the terminal server or Citrix server and then update each user's copy of notes.ini to reference the wgnemno.dll add-in (see above). You can do this manually or, more likely, by some automated method.

Uninstalling Endpoint Agents

This section describes how to manually uninstall CA DataMinder endpoint agents.

Follow these steps:

1. The uninstall procedure depends on the local operating system. For example:

   Windows 7 or Vista: In the Programs and Features applet, click Uninstall a program. In the resulting screen, right-click CA DataMinder Client'. Then click Change.

   Windows XP: In the Add or Remove Programs applet, click 'CA DataMinder Client'. Then click Change.

   Note: If you click Remove instead, you do not get the option to keep the CA DataMinder database (see step 3).

2. When the Installation Wizard starts, go to the Program Maintenance screen.

   Choose Remove to uninstall CA DataMinder from the current computer.

3. In the Remove the Program screen, you can keep or remove the local CA DataMinder database. If you keep the database, you can reconnect to it if you reinstall CA DataMinder.

   a. Select or clear the 'Delete CA DataMinder Database' check box, as required.

   b. Click Remove to being the uninstall.

4. (Applies to Client File System Agent and Client Print System Agent only) Restart the endpoint computer to finalize the uninstallation.

   Note: You only need to restart the endpoint computer if it was hosting the CFSA or CPSA. If these agents were not installed on the endpoint computer, you do not need to restart.

Chapter 3: Group Policy Deployments

This section describes how to deploy CA DataMinder to endpoint computers by using Windows Group Policy.

This section contains the following topics:

Group Policy Operations

You can remotely deploy CA DataMinder to endpoint computers by using Group Policy. Using this method, you must *assign to computers; y*ou must not assign to users.

Note: We recommend using the 'Assigned' deployment method because, unlike the 'Published' method which requires user cooperation, the 'Assigned' method enables you to enforce deployment.

The Group Policy installation procedure comprises the following steps

1. Select an organizational unit (OU) containing the machine accounts.
2. Create a new group policy object (GPO) to control the software installation package.
3. Filter the GPO security properties so they apply to the target machines.
4. Define the GPO package properties, including the MSI installation file, the deployment method ('Advanced assigned'), deployment options, and the MST transform file.
5. Deployment starts as soon as the client machines restart.

These steps are described in the following sections.

Before Installing with Group Policy

Before using Group Policy to deploy CA DataMinder endpoint agents, you must:

1. Create an administrative installation source image.
2. Create a Windows Installer transform file to specify the name of the parent CMS or gateway server.
3. Extract the source images for the Microsoft Visual C Runtime Libraries.
4. (Recommended) Disable InPrivate Browsing for Internet Exploter.

These steps are described in the following sections.

More information

Create an Administrative Installation Source Image (see page 40)
Create a Transform: SetParentName.mst (see page 41)
Extract the Source Images for the Microsoft Visual C Runtime Libraries (see page 42)

Create an Administrative Installation Source Image

To deploy CA DataMinder to client machines using command-line methods or managed methods such as Group Policy, we recommend that you first perform an administrative installation to your network. This enables client machines to install CA DataMinder directly from the network without generating excessive network traffic or requiring excessive free disk space on the client.

The administrative installation installs a source image of CA DataMinder onto the network in a target folder that you specify. The source image is called Client.msi. Store this source image in a network folder that all the target client machines can access.

To perform an administrative installation

Use the /a command-line option for Msiexec.exe.

- The syntax to create an administrative image for 32-bit client machines is:
  `msiexec /a <Path>\client.msi`
- The syntax to create an administrative image for 64-bit client machines is:
  `msiexec /a <Path>\client_x64.msi`

Note: See your Microsoft documentation for details about administrative installations.

Create a Transform: SetParentName.mst

Transform files let you apply customized configuration changes to a Windows Installer package. CA DataMinder typically provides scripts to create several useful transforms. Find the scripts to generate transforms in the \Support folder of your CA DataMinder distribution media.

For script-generated transforms, you must copy the script into the same folder as your administrative installation source image, Client.msi or Client_x64.msi. You need write access to this folder. You run the script by double-clicking it in Windows Explorer. The script generates the transform for the administrative installation source image.

Note: If no script is provided, you can obtain the transform from CA Support at http://ca.com/support.

.

For a Group Policy installation, you can use a transform to identify the name or IP address of the CMS or gateway that the client machines connect to.

To create the SetParentName.mst transform

1. Find this script in the \Support folder of your CA DataMinder distribution media:

   `CreateParentNameTransform.vbs`

2. Copy the script into the folder containing your administrative installation source image.

3. When you run the script, it prompts you for the name or IP address of the CMS or gateway and creates the transform file SetParentName.mst.

   Note: If you specify the CMS or gateway by name, you must ensure that the client machines can resolve its name (see Server name resolution).

Extract the Source Images for the Microsoft Visual C Runtime Libraries

The CA DataMinder distribution image includes two Visual C runtime libraries, vcredist_x86.exe and vcredist_x64.exe. These libraries must be present on the host machines before you can install CA DataMinder. If you need to include these libraries in your Group Policy deployment, you first must extract the 'double wrapped' .msi images and .cab files from the executables.

To extract the source image

1. Find vcredist_x86.exe and vcredist_x64.exe in the \redist folder of the CA DataMinder distribution image.
2. Extract the vcredist.msi and vcredis1.cab files.
   a. (All endpoint computers) Run this command and accept the license agreement:
   `vcredist_x86.exe /C /T:<path to output folder #1>`

   Where 'output folder #1' is the target folder for the extracted 32-bit source image.

   b. (64-bit endpoint computers only) Run this command and accept the license agreement:
   `vcredist_x64.exe /C /T:<path to output folder #2>`

   Where 'output folder #2' is a second target folder for the extracted 64-bit source image.
3. Copy these extracted files to the same location as the Client.msi file that you created as part of your administrative installation source image.

Group Policy Installation

For a Group Policy installation, select an appropriate Active Directory organizational unit (OU) that contains the target computer. Then define a group policy object (GPO) that contains a software installation package. As soon as the GPO is created, CA DataMinder is deployed to the target computers when they next reboot.

Note: For full details about Group Policy, refer to your Windows documentation.

To deploy using Group Policy

1. Open Active Directory Users and Computers.

   Find this application in the Administrative Tools folder.
2. Select an organizational unit (OU).

   This OU must contain *computers* targeted for CA DataMinder deployment (because you will base the GPO on computer accounts, not user accounts).

3. Create the GPO based on the Group Policy properties of your chosen OU, for example, ‘CA DataMinder Rollout’.
4. Edit the GPO Security settings to specify which machine accounts the GPO applies to.

   For each target computer, enable the Apply Group Policy permission.
5. Create a new software installation package for the GPO Computer Configuration (this is a Group Policy property of the OU).

   This installation package enables you to assign the software forcibly to target computers.

```
CA DataMinder Rollout Policy
- Computer Configuration
  - Software Settings
    Software Installation
  + Windows Settings
  + Administrative Templates
User Configuration
```

   GPO Computer Configuration, Software Installation
6. Configure the software installation package to point to the Client.msi file that you created as part of your administrative installation source image.

   If necessary, configure the package to point to the .msi files for the unwrapped Visual C runtime libraries (see the previous section).
7. Define the properties of the installation package.

   a. **Deployment method:** When prompted, click the ‘Advanced assigned’ method. You must select this method so that you can apply modifications to the package—see step 7.c.

   b. **Deployment options:** If you need the ability to:

      - Selectively uninstall CA DataMinder from client machines (see the Group Policy Uninstallation section), select the option Uninstall this application when it falls out of the scope of management.
      - Forcibly overwrite any existing versions of CA DataMinder on client machines, select the advanced option 'Remove previous installations of this product from computers if the product was not installed by Group Policy-based software installation'.

c. **Modifications:** Specify the following transforms:

- **SetParentName.mst:** This transform is essential! It enables the installation package to identify its nominated parent server correctly.

  Note: Without this transform, client machines cannot identify their parent server and CA DataMinder fails to install.

- **Appmon.mst:** (Optional) By default, a GPO installation performs a 'Typical' setup, which excludes CA DataMinder application integration. But you can specify this transform to install application integration.

  Note: Application integration enables CA DataMinder to monitor usage of desktop applications.

- **ClientLockDown.mst:** (Optional) This transform prevents users from uninstalling CA DataMinder with the Add/Remove Programs utility.

8. The GPO is now complete.

   CA DataMinder is deployed to the target client machines automatically when they next reboot.

More information:

Before Installing with Group Policy (see page 40)
Group Policy Uninstallation (see page 44)

Group Policy Uninstallation

If you installed CA DataMinder to a client machine using Group Policy, we recommend that you uninstall using Group Policy.

To do this, go to Active Directory Users and Computers and edit the GPO Security settings (see Group Policy Installation, step 4). For each client machine, remove the Apply Group Policy permission. CA DataMinder is uninstalled automatically when the client machine next reboots. Alternatively, delete the entire GPO. CA DataMinder is uninstalled from all client machines referenced by the GPO.

Chapter 4: Client File System Agent

This section describes the Client File System Agent (CFSA).

This section contains the following topics:

About the Client File System Agent

You can use the Client File System Agent (CFSA), also known as 'Policy on Save', to control user attempts to copy files off the local hard disk. For example, the CFSA can monitor files being copied to removable storage devices (such as USB flash drives and SD cards), sync folders (such as DropBox), network locations, and writable CDs and DVDs. The CFSA can selectively block or allow a file and apply policy triggers based on a file's text content or properties. For example, it can force users to encrypt files being copied onto removable devices.

The CFSA can also scan the local hard disk and apply policy triggers based on a file's text content or properties. For example, it can categorize files based on their text content, and delete, replace or move unauthorized files.

How Does CA DataMinder Protect Files on Removable Devices?

CA DataMinder can detect when a user tries to copy files to removable devices such as USB flash drives or SD cards.

Opening a file on a removable device

(Optional) When the CFSA detects a user trying to *open* a file on a prohibited device, it displays an Access Denied message. This message typically warns users that they are barred from saving file changes. You configure the Access Denied message in the user policy.

Note: A prohibited source is any removable device to which write access is denied. Write access may be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Copying a file to a removable device

When CA DataMinder detects a user trying to save a file to a removable device, it applies policy in the following sequence. The process is also summarized in the following flow chart (see page 48).

1. **CFSA checks whether the user is using a trusted application.**

   Settings in the machine policy identify 'trusted applications'. If the user is using:

   - A trusted application, the CFSA always allows the user to copy or save the file to a removable device. No further policy is applied.
   - Any other application, the CFSA checks the handling for the removable device or network location (see step 2).

2. **CFSA checks the handling for the removable device.**

   Settings in the machine policy define the ‘handling’ for removable devices. The available handling options are:

   Allow write access

   The user is allowed to copy files to this device.

   Set to read only

   The user is blocked from copying files to the device. That is, Write access to the device is disallowed.

   Apply user policy

   The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

   You can also configure default handling for unrecognized devices and custom handling for ‘special devices’.

3. **CFSA checks whether the user is using a policy-enabled application.**

   These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

   If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the device is set to Read Only.

   Warning! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. **CFSA applies Data In Motion triggers.**

   Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author. Each trigger can also apply a further device filter to monitor specific removable devices.

   If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file. You can also configure control actions to encrypt sensitive files being copied to a removable device (the user must supply a decryption password).

   If no control trigger fires, the user is allowed to copy the file.

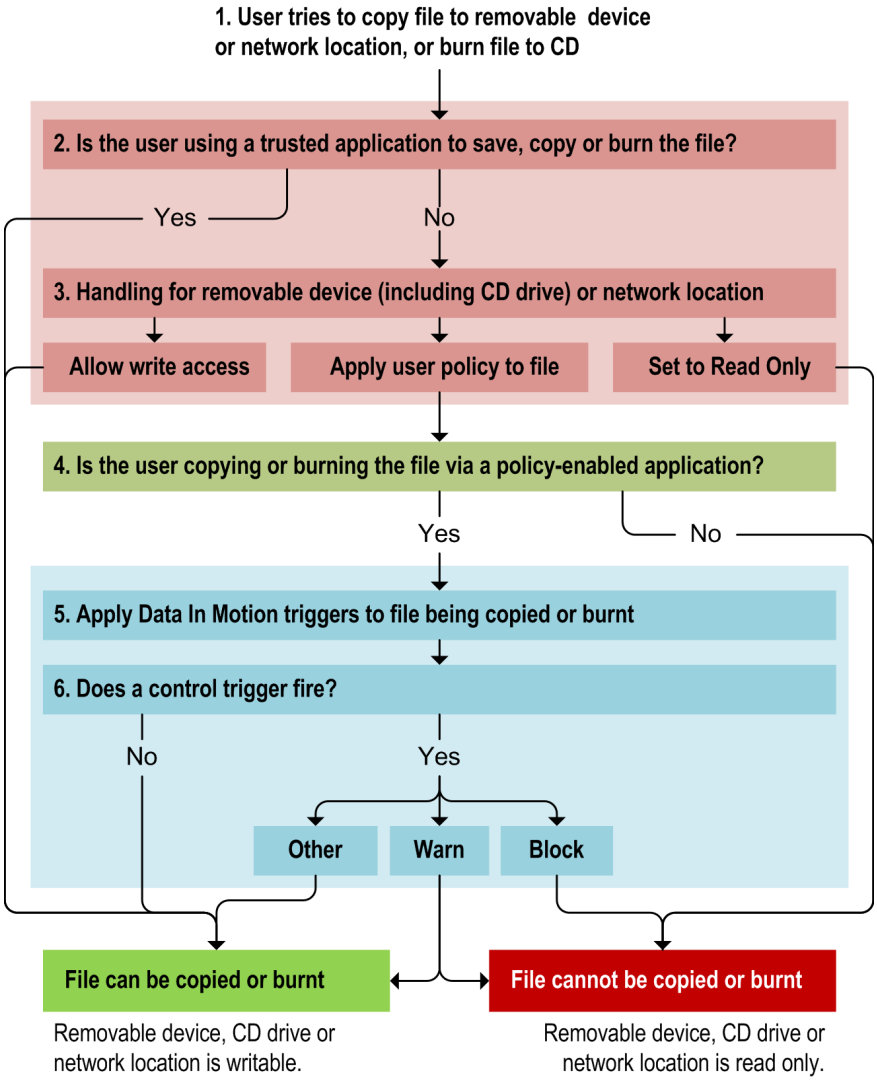
CFSA Flow Chart: Removable Devices, CD Drives, Network Folders

In the diagram below, a user tries to copy a file to a removable device or network location, or burn it to a CD (**1**). First, the CFSA checks whether the user is using a trusted application (**2**). If they are, it permits the file to be copied or burnt.

If the user is not using a trusted application, the CFSA checks the device, CD drive or location handling (**3**). If set to 'allow write access', file copying or burning is allowed; if it set to 'read only', the file is blocked.

Alternatively, if the handling is set to 'apply user policy', the CFSA checks whether a policy-enabled application is being used to copy or burn the file (**4**):

- If so, the CFSA applies policy triggers to the file (5). If a control trigger fires (6), this determines whether to block the file operation. If no control trigger fires, the file can be copied or burnt.
- If the user is not using a policy-enabled application, the file is blocked.


1. User tries to copy file to removable device or network location, or burn file to CD
2. Is the user using a trusted application to save, copy or burn the file?
Yes
No
3. Handling for removable device (including CD drive) or network location
Allow write access
Apply user policy to file
Set to Read Only
4. Is the user copying or burning the file via a policy-enabled application?
Yes
No
5. Apply Data In Motion triggers to file being copied or burnt
6. Does a control trigger fire?
No
Yes
Other
Warn
Block
File can be copied or burnt
Removable device, CD drive or network location is writable.
File cannot be copied or burnt
Removable device, CD drive or network location is read only.

How Does CA DataMinder Protect Files in Network Folders?

CA DataMinder can detect when a user tries to copy files to network locations such as shared folders.

Opening a file from a prohibited network location

(Optional) When the CFSA detects a user trying to *open* a file from a prohibited network folder, it displays an Access Denied message. This message typically warns users that they are barred from saving file changes. You configure the Access Denied message in the user policy.

Note: A prohibited source is any network location to which write access is denied. Write access may be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Copying a file to a network location

When CA DataMinder detects a user trying to save a file to a network location, it applies policy in the following sequence. The process is also summarized in the previous flow chart (see page 48).

1. **CFSA checks whether the user is using a trusted application.**

   Settings in the machine policy identify 'trusted applications'. If the user is using:

   - A trusted application, the CFSA allows the user to copy or save the file. No further policy is applied.
   - Any other application, the CFSA checks the handling for the network location (see step 2).

2. **CFSA checks the handling for the network location.**

   Settings in the machine policy define the 'handling' for network locations. The available handling options are:

   Allow write access

   Users can always save files to this network location.

   Set to read only

   Users are blocked from saving files to this network location.

   Apply user policy

   The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

   You can also configure custom handling for 'special locations'.

   Note: When you specify the network locations that you want to monitor, always enter the UNC path. For example:

   `\\UX-FILESVR-01\New Project\Reports`

   If a path contains spaces, do not enclose it in quotes.

3. **CFSA checks whether the user is using a policy-enabled application.**

   These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

   If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the target network folder is set to Read Only.

   Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. **CFSA applies Data In Motion triggers.**

   Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author.

   If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file.

   If no control trigger fires, the user is allowed to copy the file.

   Note: The CFSA cannot encrypt files being copied to network locations. Do not use Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

Local Drives Listed As Network Drives Over RDC

The CFSA can apply policy to local drives that have been added as network drives in a Remote Desktop Connection (RDC) session.

The Windows RDC feature allows users to use local disk drives in a remote session. For example, a user working from home connects to their office workstation using RDC. When the RDC session starts, the user can add their local C drive as a network drive on the remote workstation. This network drive represents a security risk, because the user can drag and drop sensitive files from their workstation onto their local C drive.

From a policy viewpoint, the CFSA handles these RDC network drives in the same way as other network locations. To apply policy to files being copied to this network drive in an RDC session, add one of the following values to the Special Locations List setting:

```
\\tsclient\C
\\tsclient\D
\\tsclient\*
```

These values apply policy to, respectively, the local C drive, local D drive, or all local drives mapped as network drives in an RDC session.

Find the Special Locations List setting in the following folder in the machine policy: `/Client File System Agent/Data in Use Protection/Network Locations folder.`

How Does CA DataMinder Stop Users Burning Files to CD?

CA DataMinder can detect when a user tries to burn a file to CD or DVD.

The CFSA automatically recognizes writable CD and DVD drives and handles these drives in the same way as removable devices.

Note: In this section, the term 'CD drive' also refers to DVD drives.

Burning a file to CD or DVD

First, the CFSA applies machine policy in real time to block unauthorized file operations. It can also apply Data In Motion triggers to analyze the file being copied. The process is summarized below and in the previous flow chart (see page 48).

1. **CFSA checks whether the user is using a trusted application.**

   Settings in the machine policy identify 'trusted applications'. If the user is using:

   - A trusted application, the CFSA allows the user to burn the file. No further policy is applied.
   - Any other application, the CFSA checks the handling for the CD drive (see step 2).

2. **CFSA checks the handling for the CD drive.**

   Settings in the machine policy define the ‘handling’ for writable CD drives. The available handling options are:

   Allow write access

   Users can always save files to this CD drive.

   Set to read only

   Users are blocked from saving files to this CD drive.

   Apply user policy

   The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

   Note: When configuring the CFSA machine policy settings, you do not need to add writable CD drives to the Treat These Drives As Removable setting. The CFSA automatically treats these drives as removable and applies the device handling to them. For example, to prevent any files being burnt to CD, you can set the device handling to 'Set to read only'.

3. **CFSA checks whether the user is using a policy-enabled application.**

   These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

   If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the CD drive is set to Read Only.

   Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. **CFSA applies Data In Motion triggers.**

   Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author. Each trigger can also apply a further device filter to monitor specific removable devices.

   If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file.

   If no control trigger fires, the user is allowed to burn the file.

   Note: 'Encrypt' control actions are not supported. You cannot encrypt files being burned to CD.

How Does the CFSA Protect Files in Sync Folders?

CA DataMinder can detect when a user tries to drag or copy files into sync folders such as DropBox. It also detects when a user tries to upload a file to a file sync website such as DropBox.com.

Note: When you drag and drop a file into a sync folder in Windows Explorer, CA DataMinder copies the file instead of moving it.

File Sync Methods: Application versus Web site

File sync providers such as DropBox typically provide two sync methods:

- Users can install a Windows Explorer plug-in on their workstation. This plug-in is the 'file sync application' (see below). The user launches Windows Explorer and drags or copies the file that they want to share into the sync folder.

  The CFSA can protect files being synced using this method.

- Uses can log in to file sync web site (such as DropBox.com) and upload the file that they want to share into the sync folder.

  The Client Network Agent (CNA) can protect files being synced using this method.

CA DataMinder provides Data In Motion protection for both file sync methods.

How Does CA DataMinder Protect Files Being Copied to Sync Folders?

1. **CFSA checks machine policy for file sync applications.**

   (Not applicable to files being uploaded to a file sync website.)

   First, the CFSA checks the local machine policy in real time to determine whether the file sync application is under policy control. By default, CA DataMinder can apply policy to files being synced to:

   - Box
   - DropBox
   - Google Drive
   - Microsoft SkyDrive

   If the file sync application is *not* under policy control, CA DataMinder allows the file to be synced.

   But if the file sync application *is* under policy control, CA DataMinder checks whether the user is using a policy-enabled application to copy the file.

2. **CFSA checks whether the user is using a policy-enabled application.**

   These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

   If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the sync folder is set to Read Only.

   Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

3. **CA DataMinder applies Data In Motion triggers.**

   The file sync method affects which CA DataMinder endpoint agent handles the policy analysis.

   Using a file sync application plug-in

   If an employee uses a Windows Explorer plug-in to copy files to a sync folder, the *CFSA* detects the sync operation and applies Data In Motion triggers.

   Verify that the Client File System Agent is selected in the Which Files Sources? setting.

   Using a file sync web site

   If an employee uploads a file to a file sync web site, the *Client Network Agent* detects the sync operation and applies Data In Motion triggers.

   Verify that the Client Network Agent for File is selected in the Which Files Sources? setting.

   In both cases, DIM triggers can analyze the text content to detect key phrases or check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author.

4. **CA DataMinder applies Data In Motion control actions.**

   If a trigger fires, you can configure control actions to block the file sync operation.

   Alternatively, if the user is using a file sync application, you can set up triggers to warn the user. Or you can allow the file sync operation but categorize or encrypt the file (the user must supply a decryption password).

   If no control trigger fires, the user is allowed to copy or upload the file.

How Does CA DataMinder Protect Files on the Local Hard Disk?

The CFSA can run scheduled scans of the local hard disk and apply Data At Rest triggers to targeted files. The process is summarized below and in the following flow chart (see page 58).

1. **CFSA applies machine policy.**

   Settings in machine policy determine when and how often the CFSA runs a local file scan.

   Other machine policy settings identify the files and folders that you want to scan. For example, you can specify local files or folders that you want to explicitly include or exclude from the scan. You can also choose to only scan files modified since the previous scan.

2. **CFSA applies user policy Data At Rest triggers.**

   When the scan runs, CFSA applies Data At Rest triggers in the user policy.

   These triggers analyze the scanned files and apply appropriate control actions. For example, they can categorize files based on their text content. They can also add smart tags to scanned items. The smart tags are either saved with the event matadata in the CMS database or, for Microsoft Office documents, you can apply smart tags to the original document.

   Finally, you can configure control actions to delete, replace, or move unauthorized files, or copy scanned files to another location for further investigation.

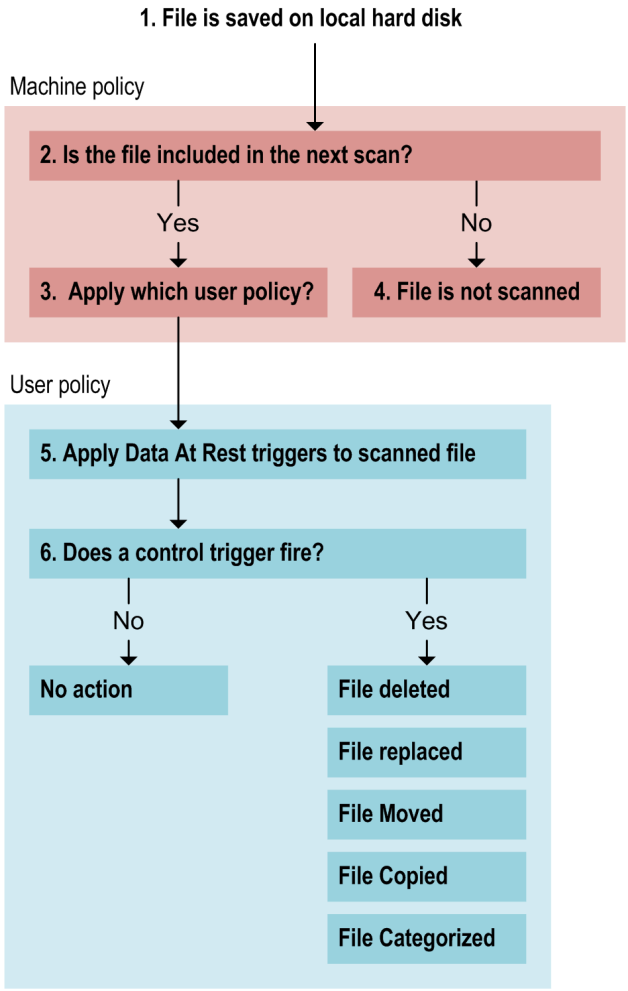
More information:

CFSA Flow Chart: Scanned Files on Local Hard Disk (see page 58)

CFSA Flow Chart: Scanned Files on Local Hard Disk

In the diagram below, a user saves a file to the local hard disk (**1**). When the next scheduled file scan runs, the CFSA checks machine policy to determine which files and folders to include (**2**) and which user policy to apply (**3**). Files implicitly or explicitly excluded are not scanned (**4**).

When the scan runs, CFSA applies Data At Rest triggers to the scanned files (**5**). If a control trigger fires, the CFSA applies an action to the scanned file (**6**). For example, they can categorize files based on their text content, and delete, replace or move unauthorized files.



CFSA Terminology

Note the following terminology:

CADLPEnc.exe encryption utility

CA DataMinder uses this utility to encrypt and decrypt sensitive files on *removable devices* (such as USB drives) or files in *sync folders*.

When a user copies a sensitive file, the encryption utility prompts for a password. CA DataMinder uses this password to copy an *encrypted* version of the file. CA DataMinder also copies the encryption utility onto the target device or sync folder.

When the user wants to copy the encrypted file from the removable device or sync folder onto a computer, the utility prompts for the original password. This time, it uses the password to copy a *decrypted* version of the file onto the computer.

Encryption

The CFSA can encrypt sensitive files being copied onto removable devices or sync folders. It uses the *CADLPEnc.exe encryption utility* to prompt the user for a password. It uses this password to encrypt and decrypt the file.

Encryption utility

See *CADLPEnc.exe*.

File system scan

You can optionally configure the CFSA to run scheduled scans of all targeted files and folders on the local hard disk. You can specify when and how often the scan runs. Machine policy settings allow you to target specific file types or folders.

Handling

This term refers to settings in machine policy that determine how the CFSA handles user attempts to copy files to removable devices, network locations, or sync folders. The available options are:

- Allow write access: The user is allowed to copy or save files to the target.
- Read only: The user is not allowed to copy or save files to the target unless they are using a *trusted application*.
- Apply User Policy To File: If the user copies or saves a file using a *policy-enabled application*, the CFSA applies Data In Motion triggers to the file.

Policy-enabled applications

These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

The CFSA uses a hard-coded list of policy-enabled applications; you cannot edit this list.

Note: The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

Policy handling

See *handling* above.

Prohibited devices

These are any removable devices to which write access is denied. Write access can be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Prohibited network locations

A prohibited network location is any network folder to which write access is denied by settings in the local machine policy.

S**pecial devices or special locations**

These are removable devices or network locations explicitly identified in machine policy. They can also include specified writable CD and DVD drives.

You can configure custom handling for these devices and locations. Conversely, you can configure default handling for unrecognized devices or network locations. For example, you may want to allow write access to authorized network folders but make other network locations read only.

Removable devices

These refer to any removable storage device, including USB flash drives, SD cards, writable CD and DVD drives, and external hard disks. The CFSA is designed to prevent unauthorized file copying to such devices.

Sync Folder

A sync folder refers to a folder used by file sync providers such as DropBox.

When a user creates a sync folder on one or more computers, their chosen file sync provider synchronizes the contents of this folder with the file sync provider's cloud-based storage. From a user's viewpoint, the same folder is available on each computer and contains the same files.

The CFSA can apply policy to files being copied to sync folders.

Trusted applications

For files being copied to removable devices or network locations,these applications are always exempt from CFSA control. If a user is using a trusted application to copy or save a file, they are always permitted to do so.

For files being copied to sync folders, the CFSA grants trusted applications access to file sync folders on the local computer.

Note: By default, lsass.exe is included in the Trusted Application List machine policy settings for the CFSA. Do **not** remove this application from the machine policy! This is the Local Security Authority System Service and is needed by Windows to perform security-related functions.

Deploy the CFSA

Before you deploy the CFSA, note the minimum Service Pack requirement when installing on Windows XP machines.

To install the CFSA

1. Find setup.exe in the root of your CA DataMinder distribution image. Run setup.exe to launch the CA DataMinder installation wizard.

   The Installation Type screen opens.

2. Click Advanced Installation.
3. In the Advanced Install Options screen, choose Endpoint Agents and then click Install.

   This launches the CA DataMinder client installation wizard in a separate window.

4. In the client installation wizard, navigate to the Customer Setup screen.
5. In the Custom Setup screen, choose File System Agent.
6. In the final wizard screen, click Install to start the file transfer.

   Note: The encryption utility, CADLPEnc.exe, is also installed in the CA DataMinder installation folder on the endpoint. The CFSA uses this utility to encrypt and decrypt files that your users copy to removable devices such as USB drives.

To configure the CFSA

See the following sections for full details. Briefly, you need to:

1. Edit the machine policy for the host machine.
2. Edit an appropriate user policy.

   In particular, you need to set up Data In Motion triggers, Data At Rest triggers, and the Access Denied message.

Which Policies Are Applied?

CA DataMinder applies both machine policy and user policy when assessing whether to allow files to be copied to removable devices or network locations.

Machine policy

CA DataMinder always applies the policy for the endpoint computer hosting the CFSA. BY default, the host computer inherits the *common client policy*, though you can customize policy for individual endpoint computers.

User policy

When applying Data In Motion triggers to files being copied, the CFSA always applies the policy for the CA DataMinder user currently logged onto the computer hosting the CFSA.

When applying Data At Rest triggers during a file scan, the CFSA always applies the user policy specified by the Default Policy for Data At Rest setting. This setting is defined in the machine policy.

To quickly roll out the CFSA across multiple client machines, edit the common client policy and the default user policy (or the policy for an appropriate user group). This ensures that the relevant policy settings replicate down to your end-users and their respective endpoint computers as soon as possible. Of course, you can still customize the policies for individual machines and users as necessary.

More information:

Data At Rest Protection Folder (see page 71)

PE Settings:

Policy Engine Folder (see page 72)

Configure the Local Machine Policy

To configure the CFSA, edit settings in the Client File System Agent folder of the machine policy on each endpoint computer. We recommend that you edit the Common Client Policy. You may also need to adjust settings in the Policy Engine folder.

The key machine policy settings are described in the following sections.

Data In Use Protection folder

Find this folder in the Client File System Agent folder.

Edit the Included Files and Excluded Files settings.

You also need to edit settings in the following subfolders:

Removable Devices folder

Edit settings in this folder to protect files files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

Network Locations folder

Edit settings in this folder to protect files files being copied to network locations. These network locations can include drives mapped over a Remote Desktop Connection (RDC).

File Sync Providers folder

Edit settings in this folder to protect files files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

Data At Rest Protection folder

Find this folder in the Client File System Agent folder.

Edit settings in this folder to determine which drives, folders and files are scanned, and which user policy is applied to scanned files.

File System Scan Configuration folder

Find this folder in the Data At Rest Protection folder.

Edit settings in this folder to specify how often the CFSA runs scheduled scans of the local hard disk.

Policy Engine folder

(Optional) For performance reasons, you may need to edit settings in this folder. Only edit these settings if instructed to do so by CA technical staff.

Data At Rest Settings:

Data At Rest Protection Folder (see page 71)
File System Scan Configuration Folder (see page 72)

Data In Use Protection Folder

Settings in this folder determine which files are monitored. This folder also includes the following subfolders: Removable Devices, Network Locations, and File Sync Providers.

In each case, you can define a list of trusted applications. If the user is using a trusted application, CA DataMinder always allows them to save or copy files to these targets.

Included Files; Excluded Files

These settings determine which files to monitor. By default, the Included setting lists all the common document types such as '*.doc' and '*.ppt'. No files are excluded by default, but if required you can use the Excluded list to omit specific file types such as .mp3 or .log files.

Note: The Excluded list takes precedence if there is a conflict. For example, you can include all spreadsheets ('*.xls') but exclude specific files such as 'Holiday_Form.xls'.

More information:

Removable Devices Folder (see page 66)
Network Locations Folder (see page 68)
File Sync Providers Folder (see page 70)

Removable Devices Folder

Edit settings in this folder to protect files files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

This folder contains the following settings:

Trusted Application List

These are applications that are exempted from CFSA control. That is, users are permitted to copy files to removable devices using these applications. For example, you may not need to monitor an in-house system application that always encrypts files when saving.

Add the applications you want to exempt from the CFSA. You must supply the executable or process name, such as Winword.exe.

Note: Trusted applications override any device filters. That is, a user can copy a file directly from a trusted application to a removable device, even if the handling for that device blocks such copy operations or applies policy to the file content.

lsass.exe always included

By default, lsass.exe is always included in this list—see the 'trusted application' definition in CFSA terminology.

Anti Virus Programs

If a client machine is protected by an anti-virus program, we recommend that you add the process name to the Trusted Application List. For example, add InoRt.exe if it is protected by CA eTrust Threat Management.

Treat These Drives As Removable

This setting instructs the CFSA to handle a fixed drive as if it were a removable drive. For example, some external hard disks declare themselves as being a fixed drive when in fact they are easily removable. Ordinarily, the CFSA would not apply policy to files being saved to these drives. To close this loophole, you can explicitly identify these drives as removable.

In the Treat These Drives As Removable setting, you can add the drive letter or the disk drive name (also called the 'volume identifier') set by the manufacturer. Drive letters must include a colon (such as D:). Disk drive names are shown in Windows Device Manager (such as IC25N020ATC504).

Note: The CFSA automatically treats writable CD and DVD drives as removable drives.

Default Handling

The handling determines whether a device is writable or read only. This setting controls attempts to copy files to unlisted devices (that is, any device not in the Special Device List). The available actions are exactly the same as the handling for special devices (see below).

Note: If no special devices are listed, the default handling is applied to all devices.

Special Device List

This is a list of removable devices that require specific handling by the CFSA. For example, you identify the devices you want the CFSA to control or the ones you want it to ignore.

In the Special Device List setting, type the names of the devices that require special handling. You can use ? and * wildcards if required. If a device name contains spaces, you do not need to enclose it in quotes.

Where can I find device names?

Device names are shown in the Windows Device Manager applet. You can also see them in Windows Explorer. When you view the properties of a removable drive, the device name is listed in the Hardware tab of the Properties dialog.

You can also check device names in Windows Device Manager. Note that Device Manager automatically appends 'USB Device' to device names. You must omit this appended text when you specify the device name in the machine policy or user policy. For example, if the Device Manager lists 'Unipraxis DataStick 2.0 USB Device', enter this in the policy as 'Unipraxis DataStick 2.0'.

Handling for Special Devices

This setting determines how the CFSA handles attempts by a user to copy files to any removable device included in the Special Device List. The available actions are:

Allow write access

The user is allowed to copy files to listed devices. Policy is not applied.

Read only

The user is not allowed to copy files to listed devices (unless they are using a trusted application). Policy is not applied.

Apply User Policy To File

If the user attempts to copy a file to a listed device using:

- A policy-enabled application, policy is applied to the file using Data In Motion triggers.
- A trusted application, copy operations are always permitted. Policy is not applied to the file.
- Any other application, the copy operation is blocked; that is, the device is set to read only.

Network Locations Folder

This folder contains the following settings:

Trusted Application List

These are applications that are exempted from CFSA control. That is, users can save files to any network location if they are using a trusted application.

For example, you may not need to monitor an in-house system application that always encrypts files when saving. By default, lsass.exe is always included in this list—see the *trusted application* definition in 'CFSA Terminology'.

In the Trusted Application List setting, add the applications you want to exempt from the CFSA. You must supply the executable or process name, such as Winword.exe.

Note: Trusted applications override any network location filters. Users can save files directly from a trusted application to any network location.

Default Handling

This setting determines how the agent handles attempts to copy files to unlisted network locations (that is, any not listed in Special Locations List). The available actions are exactly the same as for special locations (see below).

Note: If no special locations are listed, the default handling is applied to all network locations.

Special Locations List

This setting is a list of network locations that require specific handling by the CFSA. You can either list the locations you want the CFSA to control or the ones you want it to ignore.

When you specify a network location, you must supply the UNC path. This path must use a fully qualified domain name (FQDN). For example:

```
\\UX-FILESVR-01.UNIPRAXIS.COM\My Project\Reports
```

Local Drives Listed As Network Drives Over RDC

The CFSA can apply policy to drives mapped over a Remote Desktop Connection (RDC).

The Windows RDC feature allows users to use local disk drives in a remote session. For example, a user working from home connects to their office workstation using RDC. When the RDC session starts, the user can add their local C drive as a network drive on the remote workstation. This network drive represents a security risk, because the user can drag and drop sensitive files from their workstation onto their local C drive.

To apply policy to files being copied to this network drive in an RDC session, add one of the following values to Special Locations List:

```
\\tsclient\C
\\tsclient\D
\\tsclient\*
```

These values apply policy to, respectively, the local C drive, local D drive, or all local drives mapped as network drives in an RDC session.

Wildcards

When you specify a UNC path, you can use wildcards to specify the share name, folder name and file name. But do *not* use wildcards to specify the server. For example, this path is allowed::

```
\\UX-FILESVR-01.UNIPRAXIS.COM\My Project*\Report*
```

But this path is *not* allowed:

```
\\UX-FILESVR-*.UNIPRAXIS.COM\My Project*\Report*
```

Spaces

If a UNC path contains spaces, you do not need to enclose it in quotes.

Handling of Special Locations

This setting determines how the CFSA handles attempts to copy files to a network location listed in Special Locations. The available actions are:

Allow write access

The user is allowed to copy files to special locations. Policy is not applied.

Read only

The user is not allowed to copy files to special network locations (unless they are using a trusted application).

Apply User Policy To File

If the user attempts to copy a file to a special location using:

- A policy-enabled application, policy is applied to the file using Data In Motion triggers.
- A trusted application, copy operations are always permitted. Policy is not applied to the file.
- Any other application, the copy operation is blocked; that is, the location is set to read only.

File Sync Providers Folder

Edit settings in this folder to protect files files being copied to sync folders. These settings determine whether a user is allowed to copy files using a file sync application such as Dropbox.

In particular, these settings determine whether the file sync application is under policy control. If the file sync application *is* under policy control, CA DataMinder applies Data In Motion triggers to analyze the file being synced.

Note: These settings do *not* apply to files being uploaded to file sync websites.

Trusted Application List

This setting grants the listed application access to file sync folders on the local computer. For example, you may want to add virus scanners to this list. You can also use this setting to extend data protection to other file sync applications.

Type the executable names of any additional file sync applications that you want to include under CFSA control. You must also add the sync folder for the new file sync application to the Additional Sync Folders setting.

Which File Sync Applications?

This setting lists the default set of file sync applications supported by the CFSA. Select the file sync applications that you want the CFSA to monitor.

Additional Sync Folders

Use this setting to specify any additional sync folders that you want the CFSA to monitor.

You can use system variables such as %windir% when specifying folder paths.

Data At Rest Protection Folder

Settings in this folder control how often the CFSA runs scheduled scans of the local hard disk. They also determine which drives, folders and files are scanned, and which user policy is applied to scanned files. This folder also includes the File System Scan Configuration subfolder.

Included Folders; Excluded Folders

These settings determine which folders to scan. By default, the CFSA scans all local folders except the \Windows and \Program Files folders, but you can change these. For example, you can specify the main folders you want to scan the Included list, but then use the Excluded list to omit specific subfolders.

By default the Excluded Folders setting uses %SystemRoot% and %ProgramFiles% variables to exclude the \Windows and \Program Files folders.

Included Files; Excluded Files

These settings determine which files to scan within the included folders. By default, the Included setting lists all the common document types such as '*.doc' and '*.ppt'. No files are excluded by default, but if required you can use the Excluded list to omit specific file types such as .mp3 or .log files.

Note: The Excluded list takes precedence if there is a conflict. For example, you can include all spreadsheets ('*.xls') but exclude specific files such as 'Holiday_Form.xls'.

Default Policy for Data At Rest

This setting determines which user policy gets applied to scanned files. It defaults to 'DefaultClientFileUser'. A CA DataMinder user account with this name is created automatically when you install a CMS. This account is created specifically to apply policy to scanned files across all workstations. Or you can specify a different CA DataMinder user account (enter the user name, not the full name).

Enable File System Scan

Set this to True to set up regular scans of all included files on the local machine. If you do enable full scans, settings in the File System Scan Configuration folder allow you to set the scan frequency.

More information:

File System Scan Configuration Folder (see page 72)

File System Scan Configuration Folder

These settings determine when and how often the CFSA scans the local hard disk. They specify the time and day when the full scan begins, plus the number of days between each scan.

Start Time

This is specified as 'minutes after midnight', so enter 60 to specify a 1am start time.

Start Day

This can be any day of the week or 'Next'. This specifies when the scan first runs; when it next runs depends on the Frequency. If you choose Next, the scan starts at the next occurrence of the Start Time; this could be later today or tomorrow.

Frequency (days)

This specifies how often the scan runs. For example, to run a scan every Sunday, set the Start Date to Sunday and the Frequency to 7.

To set up daily file scans

1. Set the Start Time as required.
2. Set the Start Day to 'Next' and the Frequency to 1.

   Note: Do **not** set the Start Day to a specific day of the week; if the client machine is restarted, the next scan will not run until the next occurrence of the Start Day.

Policy Engine Folder

For performance reasons, you may need to amend these settings in the Policy Engines folder. You must only edit these settings if instructed to do so by CA technical staff:

Maximum Number of Concurrent Operations

Defines the maximum number of files that can be processed simultaneously by a policy engine.

Deadlock Detection Timeout (seconds)

Specifies how long a worker thread must be inactive while processing an event before the policy engine considers the thread to have stalled.

Configure the User Policy

Edit your user policies to complete the CFSA configuration.

Files being copied to removable devices, network locations, writable CD/DVD drives, and sync folders

To protect these files, edit Data In Motion triggers and control actions.

(Optional) Edit the the Access Denied Message. You can optionally display an explanatory message when CA DataMinder blocks a file being copied or saved because CA DataMinder infers the target is Read Only.

Files being synced to sync folders

To protect these files, edit Data In Motion triggers and control actions.

Files stored on the local hard disk

To protect these files, edit the Data At Rest triggers and control actions.

Key policy settings are described in the following sections.

Note: General instructions for editing user policies are in the *Policy Guide*.

Data In Motion Triggers

Data In Motion triggers include general settings that let you specify which types of data you want the CFSA, CPSA, or Client Network Agent to detect. This section focuses on the key Data In Motion settings for the CFSA.

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents.

Verify that the following sources are selected:

- Client File System Agent

  You *must* select this agent if you want to analyze files being copied to removable devices, network locations, or sync folders in Windows Explorer.

- Client Network Agent for File

  (Optional) Select this agent if you also want to analyze files being copied to file sync websites such as DropBox.com.

Which Targets?

(Not applicable to file sync operations and files copied to network folders. To specify network locations, edit the Top Level File Lists settings.)

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

For the CFSA, you can specify lists of included or excluded devices. These lists are similar to the Special Device List settings in machine policy.

Type the names of the devices that you want to include or exclude. Use ? and * wildcards if required. If a device name contains spaces, you do not need to enclose it in quotes.

If you set up the trigger to use:

- Included removable devices**,** the trigger only fires if a user tries to copy a file to a listed device using a 'policy-enabled application'.
- Excluded removable devices**,** these devices are exempted from control by the CFSA. But attempts to copy files to any other (unlisted) removable devices, via a policy-enabled application, *will* fire the trigger.

Where can I find device names?

Device names are shown in the Windows Device Manager applet. You can also see them in Windows Explorer. When you view the properties of a removable drive, the device name is listed in the Hardware tab of the Properties dialog.

You can also check device names in Windows Device Manager. Note that Device Manager automatically appends 'USB Device' to device names. You must omit this appended text when you specify the device name in the machine policy or user policy. For example, if the Device Manager lists 'Unipraxis DataStick 2.0 USB Device', enter this in the policy as 'Unipraxis DataStick 2.0'.

Top Level File Lists **(including network locations)**

All Data In Motion triggers include Top Level File Lists. Use these lists to detect normal files or zip files, or files in network locations.

Edit these lists to identify the names of files that you want to apply policy to. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, choose whether to use an Included, Excluded or Ignored file list.

Network Locations

You also use this setting to specify UNC network paths. This path must use a fully qualified domain name (FQDN). Use a wildcard to detect all files in the specified folder. For example:

```
\\UX-FILESVR-01\New Project\Reports\*.*
```

If a path contains spaces, you do not need to enclose it in quotes.

Individual/Embedded File List

If required, Data In Motion triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Intervention

In each Data In Motion control action, the Intervention setting determines how the CFSA handles files being copied to removable devices, network locations, or sync folders. The available options include Block, Warn, Inform, Categorize and Encrypt (the user must supply a decryption password).

Note: The CFSA cannot encrypt files being copied to network locations.

More information:

Access Denied Message Subfolder (see page 76)

Access Denied Message Subfolder

(Optional) You can display an explanatory message to users when the CFSA denies Write access to a specific target, such as a removable device or sync folder. This message typically warns users that they are not permitted to save files to the target.

When is This Message Shown?

The CFSA displays this message if Write access to the target is denied by machine policy *or* the user is not using a policy-enabled application:

- When is Write access denied by machine policy?

  The machine policy includes a Data In Use Protection folder plus subfolders. Settings in these folders determine the *handling* for removable devices, network locations, and sync folders. For example, CA DataMinder may handle a specific network folder as Read Only. Other settings in these folders identify 'trusted applications' which are exempt from policy control. If a user tries to save a file to the target using a trusted application, Write access is granted. If the user uses any other application, Write access is denied.

- What is a policy-enabled application?

  These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to ‘Apply user policy’, the CFSA applies Data In Motion triggers to the file.

  If the target handling is set to 'Apply user policy' but the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the target is set to Read Only.

  Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

Available Settings

Find the Access Denied Message subfolder in the \Extensions\Client File System Agent folder. This subfolder contains the following settings:

Title, Message

Use Title and Message settings to provide a notification message for users, explaining that they will be unable to save changes to the current file.

Frequency

The Frequency setting determines how often this message is shown. You can set the message to never display, or to display:

Once per login

A user only sees the message once in a Windows session. This happens the first time that CA DataMinder denies Write access when a user tries to copy or save a file to a target.

Once per volume mount

(Not applicable to file sync operations) The message is shown if a user plugs in a USB drive or SD card, for which the CA DataMinder device handling is Read Only. The user only sees the message when they first open a file from that device.

Once per application

A user sees the message when they open a file from a target for which the CA DataMinder handling is Read Only.

The message is shown only once per application per Windows session.

For example, the message is shown if a user opens a Microsoft Word document stored on a 'read only' USB drive. If the user restarts Word and opens the document again, the message is not shown.

Once per application instance

A user sees the message each time they open a file from a target for which the CA DataMinder handling is Read Only.

As above, the message is shown if they open a Microsoft Word document stored on a 'read only' USB drive. But if the user restarts Word and opens the document again, the message is shown again.

Data At Rest Triggers

Data At Rest triggers include settings that let you specify which types of document you want the CFSA to scan. For example, you can edit the triggers to detect specific file formats (such as Microsoft Word documents) and analyze a file's text content. This section focuses on the key Data At Rest settings for the CFSA.

Which File Sources?

In each Data At Rest trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents.

Important! Verify that the *Client File System Agent* check box is selected! This enables the trigger to analyze local files scanned by the CFSA.

Top Level File Lists

All Data At Rest triggers include Top Level File Lists. Use these lists to detect normal files or zip files. You edit these lists to identify the names of files that you want to apply policy to when a scan runs. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, you can choose whether to use an Included, Excluded, or Ignored file list.

Individual/Embedded File List

If required, Data At Rest triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Copy File to Location

Data At Rest control actions also support 'copy' actions, permitting you to copy scanned files to an alternative location (see page 80). When used in combination with a 'delete' actions (see below), a copy action effectively becomes a 'move file' action.

Intervention

In each Data At Rest control action, the Intervention setting determines how CA DataMinder handles scanned files. The available options allow you to categorize or delete scanned files. If necessary, you can specify DoD deletions; these ensure that deleted files cannot be recovered (see below). You can also replace deleted files with an explanatory stub file to alleviate any user concerns or categorize the resulting file event.

Note: DoD deletion is forensic deletion, so called because the storage media are purged to ensure that a file cannot be recovered and used to obtain evidence in legal discovery. 'DoD' is a reference to Department of Defense approved methods for purging storage media.

Copying Scanned Files

In addition to deleting or replacing files, you can also configure Data At Rest control actions to save a copy of the file in another location for further investigation. This includes Microsoft Exchange Public Folders and Microsoft SharePoint sites.

Each Data At Rest control action contains the following settings:

Copy File To Location

This setting specifies the target folder for copied files. It can be any valid UNC or local file system path. If set to a relative path, that path is combined with the original scan location (set in the job definition file) to form the actual copy location.

For example, if this setting is '..\output' and the original scan location is C:\root_folder\input, then files will be copied to C:\root_folder\output.

This setting also works in combination with the Copy Location Mode setting (see below) to create the final copy path.

Important! You must specify a path outside of the scan location defined in the job file, otherwise the copied files will get scanned again! In the associated topic, see example 5.

For this reason, we recommend a target location that begins '..\', such as ..\Review.

Copy Location Mode

This setting modifies the Copy File To Location folder. Set it to Absolute or Relative.

In Absolute mode, files are copied directly to the Copy File To Location folder, not to subfolders. In Relative mode, files are copied to a subfolder below the Copy File To Location folder; the subfolder matches the folder structure of the file's original location.

Based on the example above, if the scan finds a file in C:\root_folder\input\ScanFolder1, and Copy Location Mode is set to:

- Absolute, the file is copied to C:\root_folder\output
- Relative, the file is copied to C:\root_folder\output\ScanFolder1 (the subfolder path is preserved)

Note: If a file with the same name already exists in the given location, CA DataMinder uses the Copy Conflict Resolution setting (see below) to determine what action to take.

Copy Conflict Resolution

Specify what action you want to take if a file with the same name already exists in the target location. Set this to:

- Discard to discard the copied file and retain the existing file.
- Overwrite to overwrite the file already in the target folder.
- Create Copy rename the copied file (but adding a numeric suffix).

More information:

Examples of Copied Files (see page 81)

Examples of Copied Files

In the examples below, the FSA or the CFSA scans the C:\MyDocs\Projects folder. This contains the file Q1sales.mpp that you want to copy elsewhere. For these examples:

FSA

The scanning job definition is set up as follows:

```
<location path="C:\MyDocs"/>
<folders subfolders="yes">
<include>Projects</include>
</folders>
```

CFSA

The Data In Use Protection folder in the local machine policy is set up to identify C:\MyDocs\Projects* as the folder you want to scan.

To copy MyProject.mpp to a new location after it has been scanned, you need to edit the relevant settings in the Data At Rest control action as follows:

Example 1: Copy File to Location is set to ' ..\Review'

This is the method we recommend. Again, the target location is outside the scan location defined by the <location> tag in scanning job file.

- If Copy Location Mode is set to Relative, the file gets copied to: C:\Review\Projects\Q1sales.mpp
- If Copy Location Mode is set to Absolute, the file gets copied to: C:\Review\Q1sales.mpp

Example 2: Copy File to Location is set to 'C:\Evaluate'

The target location is C:\Evaluate, a subfolder outside the scan location defined by the <location> tag in the scanning job file.

- If Copy Location Mode is set to Relative, the file gets copied to: C:\Evaluate\Projects\Q1sales.mpp
- If Copy Location Mode is set to Absolute, the file gets copied to: C:\Evaluate\Q1sales.mpp

Example 2: Copy File to Location is set to 'Review'

Important! Avoid this situation!

Here, the target location is interpreted as a subfolder below the original scan location and so the file gets scanned again!

- If Copy Location Mode is set to Relative, the file gets copied to: C:\MyDocs\Review\Projects\Q1sales.mpp

More information:

Copying Scanned Files (see page 80)

Specifying File Names and Types

Each Data At Rest and Data In Motion trigger includes two types of file lists:

- Top Level File Names. These settings let you check for names of 'normal' files or zip files.
- Individual or Embedded File Names. These settings can detect named files contained within a zip file or embedded in a master file.

Both types of setting can detect specific files or types of file, including scanned files, files being copied to a removable device or network location, imported files and files entering or leaving the corporate network. Together, these settings allow you to specify different handling for unauthorized files depending on where the file was found.

Included, Excluded and Ignored file lists

For both the Top Level File Names setting and Individual or Embedded File Names setting, you can use an Included list or an Excluded list. For Top Level File Names settings, you can also use an Ignored list.

Example File Names

For example, you can specify:

- '*' to detect all files in a folder.
- '*.docx' to detect all Microsoft Word files.
- '%allarchives%' to search all archive file types. The %allarchive% variable refers to file types listed in the Archive File Extensions setting (see below).
- A list of specific .zip files. (This is only appropriate for Top Level File Names settings.)

Example: Conditional File Handling

If the CFSA detects the file Q1targets.docx saved in a public folder on your network, you may want to simply delete the file. But if it is found inside a zip file that contains other important data, you may prefer to simply move the zip file to safe location. To set this up in the user policy, you use two Data At Rest triggers and two control actions:

- The first trigger includes Q1targets.docx in the Top Level File Names setting and invokes a DoD Delete control action.
- The second trigger includes '*.zip' in the Top Level File Names setting and Q1targets.docx in the Individual or Embedded File Names setting. It invokes a 'Copy and Delete' control action, effectively moving the parent zip file to a new location.

Defining archive files

You can specify which file types CA DataMinder will recognize as 'archive' files. To do this, edit Archive File Extensions setting in the user policy. Find this setting in the \System Settings folder. Specify the archive file types, such as *.zip, *.pst, or *.gz.

What File Data is Captured?

The Capture File Details? setting in each Data In Motion and Data At Rest capture action determines what information is captured. You can choose to capture:

File attributes only

CA DataMinder captures various file attributes but not the file itself, such as: the file name and path; the host machine; the created and last modified dates; the document title and author (if available); plus other details in XML format.

Attributes and file data

CA DataMinder captures the attributes described above plus the file itself.

None

You can optionally set up the capture action to not capture any file details. This option is provided for testing purposes.

Chapter 5: Client Print System Agent

This section describes the Client Print System Agent (CPSA).

This section contains the following topics:

About the Client Print System Agent

A policy administrator can use the Client Print System Agent (CPSA) to control what information users are allowed to print. You can apply policy triggers when users try to print a file or document and you can also disable the Print Screen button on their keyboard.

The CPSA, or print agent, allows you to closely control the use of printers in your organization:

- If a user presses the Print Screen button, the print agent checks the user policy to determine whether the button is disabled.
- Alternatively, if a user attempts to print a document from an application (for example, by choosing File, Print), the print agent checks which application the user is using. If this is an 'ignored application', the user is allowed to print the document. For any other application, the print agent applies Data in Motion triggers.

  First, these triggers check whether the printer itself is excluded from policy control. If so, the print job is allowed to continue. Otherwise, the trigger examines the file's properties and text content. The results of this policy processing determine whether the print agent blocks or allows the print job.

Note: Before installing the CPSA, you must close down all applications that support printing. After installing the CPSA, you must configure it by editing CA DataMinder registry settings on the host machine and the Data In Motion triggers in your user policies.

When Do Triggers Activate?

The CPSA process is summarized below and in the following flow chart (see page 87).

1. **(Optional) CPSA checks whether the user is using a trusted application.**

   First, the CPSA checks which application the user is using. If this is:

   - If this is an 'ignored application' as defined in the registry, the CPSA allows the print job and no policy triggers are applied.
   - If the application is not listed in the registry, the CPSA does apply Data In Motion triggers to the file or document

2. **CPSA applies Data In Motion triggers.**

   Data In Motion triggers activate when the CPSA detects print jobs that match the specified criteria. For example, you can set up triggers to monitor (or exempt) specific printers on your network. You identify printers by their name, for example, 'HP Color LaserJet 4650 PCL 6 1st Floor'.

   When a file is sent to a printer, triggers can detect specific file names and file formats (such as Microsoft Word documents). They can analyze the text content to detect the key phrases or to check whether the file matches a particular document classification. They can also use XML Attribute data lookup commands to file attributes such as size, date created, date last modified, and the file author.

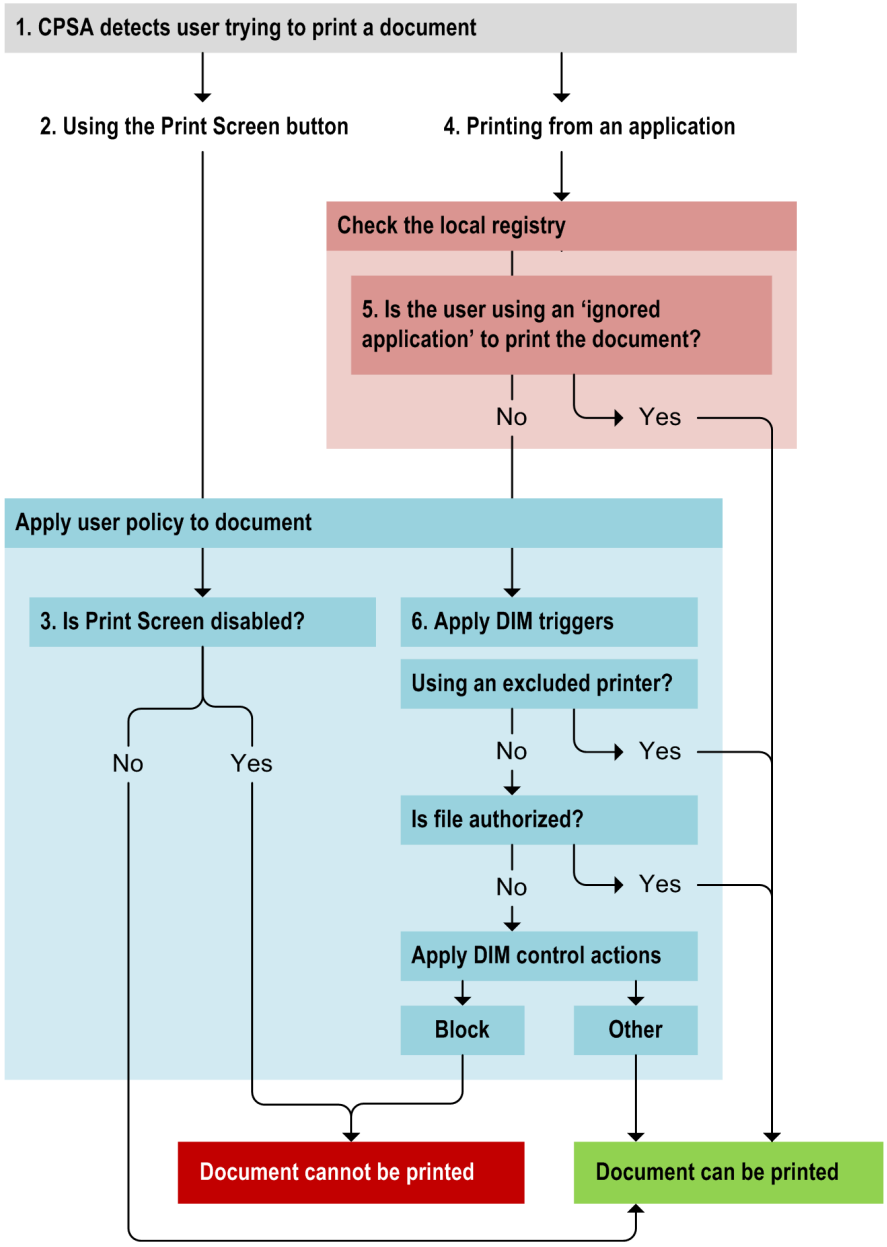
   Finally, you can configure triggers to block or allow the print job or to display a warning.

CPSA Flow Chart

In the diagram below, a user tries to print a file (**1**). First, the CPSA checks whether the user is printing from an application or is using the Print Screen button.

- If the user is using the Print Screen button to send the screen contents to a printer (**2**), the CPSA applies user policy to the print request to determine whether or not the Print Screen button is disabled (**2**).
- If printing from an application (**4**), the CPSA checks the registry to see whether the application is exempt from policy control (**5**). If so, the CPSA allows the file to be printed. If not, it applies Data In Motion policy triggers (**6**).

These triggers first check if an authorized printer is being used. If so, the CPSA allows the file to be printed. If not, the file's properties and text content are analyzed. If the file is not authorized, a control action determines whether to allow the print operation. If the file *is* authorized, the print operation is allowed.


1. CPSA detects user trying to print a document
2. Using the Print Screen button
4. Printing from an application
Check the local registry
5. Is the user using an 'ignored application' to print the document?
No
Yes
Apply user policy to document
3. Is Print Screen disabled?
6. Apply DIM triggers
Using an excluded printer?
No
Yes
Is file authorized?
No
Yes
Apply DIM control actions
Block
Other
No
Yes
Document cannot be printed
Document can be printed

Deploy the CPSA

Before installing the CPSA, close down all applications that support printing.

To install the CPSA

1. Find setup.exe in the root of your CA DataMinder distribution image. Run setup.exe to launch the CA DataMinder installation wizard.

   The Installation Type screen opens.

2. Click Advanced Installation.
3. In the Advanced Install Options screen, choose Endpoint Agents and then click Install.

   The CA DataMinder client installation wizard launches in a separate window.

4. In the client installation wizard, navigate to the Customer Setup screen.
5. In the Custom Setup screen, choose Print System Agent.
6. In the final wizard screen, click Install to start the file transfer.

To configure the CPSA

See the following sections for full details. Briefly, you need to:

1. Edit the machine policy for the host machine.
2. Edit an appropriate user policy. In particular, you need to edit Data In Motion triggers and (optionally) the Print Screen Denied settings.

More information:

Configure the User Policy (see page 90)

Which User Policy Is Applied?

Unlike the CFSA, the CPSA only applies user policy when assessing whether to allow a print job. The actual policy is always that of the user currently logged onto the client machine hosting the CPSA.

Configure the User Policy

To control what users can print, you must edit Data In Motion triggers in the user policy.

Note: Details about key policy settings are provided in the following topics.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. Edit the user policy.
   a. Expand the User Administration branch.
   b. Right-click a user or group and click Edit Policy.
3. Edit the Data In Motion triggers.

   You also need to set the Intervention option in the Data In Motion control actions.
4. (Optional) Disable the Print Screen button.
5. Save the user policy changes.

Data In Motion Triggers

Data In Motion triggers include general settings that let you specify which types of document you want the CPSA to detect. Edit your trigger settings as required. For example, you can specify search text to detect prohibited words or phrases in files being printed. Pay particular attention to these settings:

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents. Verify that the following agent is selected:

- Client Print System Agent

  You *must* select this agent if you want to analyze documents being printed.

Targets (printers)

Use the Targets settings to define the names of printers that you want to monitor or exempt. You can specify lists of included or excluded printers.

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

The printer name typically comprises the printer model plus customized location details. For example, 'HP Color LaserJet 4650 PCL 6 1st Floor'. We recommend that you specify the exact printer name. Printer names are shown in the Devices and Printers applet. You can also use ? and * wildcards, for example, to specify all printers by a specific manufacturer.

If you set up the trigger to use:

- Included printers, the trigger only fires if a user tries to send a document to a listed printer.
- Excluded printers, these printers are exempted from control by the CPSA. But attempts to send documents to any other (unlisted) printer will cause the trigger to fire.

Top Level File Names

The concept of a file name is *not* valid for CA DataMinder print events. For example, you can print a single page from an unsaved (and unnamed) document. Therefore, you *must* set the Top Level File Names setting to * (an asterisk wildcard).

Important! Do not set the Top Level File Names setting to any value except '*'. For example, if you change the value from * to myreport.doc or *.docx, the Data In Motion trigger is unable to detect any print events!

About document titles

You *can* specify document titles. Although file names are not valid for print events, they do typically contain a document title. For Microsoft Office documents, the document title is often the same as the file name. You can therefore use an XML Attribute data lookup command to test the document title of a print event. Include the lookup command in the Data Lookup Command setting.

Intervention

In each Data In Motion control action, the Intervention setting determines how the trigger handles attempts to print documents. The available options include Inform, Warn and, in particular, Block. If set to Warn, CA DataMinder allows the user to choose whether to continue and send their document to the printer; if set to block, the print operation via the selected printer is denied.

Disable Print Screen Button

Users may attempt use the Print Screen button to circumvent the CPSA. You can configure CA DataMinder to disable the Print Screen button to prevent circumvention.

Note the following:

- No print event is generated when the CPSA blocks a Print Screen operation. Data In Motion triggers do not activate and CA DataMinder does not save details of these blockings in the CMS database.
- You cannot configure the Disable Print Screen feature. That is, you cannot set up the CPSA so that Print Screen is only disabled if it detects specific files, printers or applications.

When the user presses the disabled Print Screen button on their keyboard, CA DataMinder can optionally display a 'Print Screen Denied' warning message.

To disable the Print Screen button

1. Go to the \System Settings folder of the user policy.
2. Set the Disable Print Screen setting to True.

To configure a Print Screen Denied message

If required, you can display a message to alert or inform users that the Print Screen button is disabled.

1. Go to the \Extensions folder of the user policy.
2. Edit the settings in the \Print Screen Denied Message subfolder.
3. Specify the message content.

   Example: "The Print Screen function is blocked. For assistance, contact your network administrator."

4. Specify the display frequency of the message. The available options for the Frequency setting are:

   Never

   The user never sees the message.

   Once per login

   The user sees the message once. This happens the first time they press the Print Screen button in a new Windows login session.

   Always

   The user sees the message every time they press the Print Screen button.

What Data is Captured?

The Capture File Details? setting in each Data In Motion capture action determines what information is captured. You can capture:

File attributes only

CA DataMinder captures print job attributes such as the document title, the application that was used to create the document, the computer that submitted the print job, the name of the printer name, and the print server.

Attributes and file data

For print events, CA DataMinder captures the job attributes described above plus the text content that was sent to the printer.

None

CA DataMinder does not capture any print job details. This option is provided for testing purposes.

CPSA Optional Registry Changes

To configure the CPSA, you can edit the following automatic registry values on each host machine. You can define a list of applications you want the agent to ignore (if required) and set the log level. To do this, you modify values in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA DataMinder
    \CurrentVersion\ClientPrintAgent
```

Within this registry key, the registry values you can edit are:

IgnoredApplicationList

Type: REG_SZ

Data: Specifies a semicolon-separated list of applications that are exempted from CPSA control. Users are permitted to print documents using these applications. For example, you may not want to monitor the printing of documents from graphics packages.

Default: Empty list

Note: For changes to this registry setting to take effect, you must restart any relevant application.

LogLevel

Type: REG_DWORD

Data: Determines the level of logging for the Client File Print System Agent. Log entries are written to the Activity log (viewable in the Administration console). For example, you can configure the agent to only log errors or important system messages.

Default: 2

The supported logging levels are:

1

Errors only

2

Errors and warnings

3

Errors and warnings, plus informational and status messages. For example, it shows storage and retrieval on every resource item.

Note: Setting LogLevel=3 will cause the log file to grow rapidly. This level of logging is provided for short-term testing and diagnostic purposes.

Chapter 6: Client Network Agent

Note: The Client Network Agent and CA DataMinder Network are separate features. The Client Network Agent runs on endpoint computers. CA DataMinder Network (formerly known as the NBA) operates at the network boundary and runs on dedicated Bivio appliances or Linux servers.

About the Client Network Agent

You can use the Client Network Agent (or 'network agent') to control web activity on endpoint computers. Specifically, the network agent can monitor HTTP requests. This activity includes attempts to post files and comments to web sites or to submit form data. It can also monitor attempts to check in files to SharePoint libraries.

Which browsers and applications are monitored by default?

By default, the network agent is configured to monitor web activity for most common browsers and Microsoft Office applications:

- Microsoft Internet Explorer
- Mozilla Firefox
- Opera
- Google Chrome
- SeaMonkey
- Safari
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

These browsers and applications are specified in the machine policy settings for the Client Network Agent.

How does the network agent differ from the Internet Explorer agent?

In previous versions of CA DataMinder, the Internet Explorer agent could only apply policy to web activity in Internet Explorer browsers. It applied Web triggers and could apply the full range of control actions, including Warn actions.

The network agent can apply policy to network activity in any browser and applies Data In Motion triggers. It does not support Warn control actions. Also, Data In Motion triggers offer greater file detection capabilities and also support Data Lookup commands.

Note: Unlike the Internet Explorer agent, the network agent cannot apply policy to file downloads.

How does the network agent differ from the CA DataMinder Network?

The CA DataMinder Network (NBA) operates at the network boundary and monitors outbound and inbound traffic. It runs on a dedicated Bivio hardware device or a dedicated Linux server. The NBA can also monitor traffic sent using multiple protocols, including SMTP and FTP. In particular, the NBA is able to differentiate webmails and apply Outgoing Email triggers.

The client network agent runs on users' workstations and monitors outbound network activity. Also, in the current release it can only monitor HTTP traffic.

How Does the Client Network Agent Control Web Activity?

The network agent can detect when a user submits data (files, comments, forms) to a web site. In technical terms, the agent monitors HTTP requests to web servers and web services.

First, the network agent applies machine policy to determine whether the application or browser is under policy control. Then it applies Data In Motion triggers to analyze the data submission. The process is summarized below.

1. **Network agent applies machine policy.**

   First, the network agent checks whether the user is using an *excluded* application or browser.

   The CNA ignores network activity in excluded applications and browsers. For example, you may have excluded Microsoft Word from policy control when it is used to check in or check out documents from a SharePoint site.

   If the user is using an *included* application or browser, the CNA monitors the network activity and applies Data In Motion triggers.

2. **Network agent applies Data In Motion triggers.**

   Data In Motion triggers activate when the network agent detects activity on the endpoint computer that breaches user policy. Such activity can include comments, files, and forms posted to web sites.

   When the network agent applies Data In Motion triggers, it always applies the policy for the CA DataMinder user currently logged onto the computer hosting the network agent.

   Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can also use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author.

   If a trigger fires, you can configure a control action to block the data submission. If no control trigger fires, the user is allowed to submit the data to the web site.

Deploy the Client Network Agent

This section summarizes how to install and configure the network agent.

To install the CNA

1. Find setup.exe in the root of your CA DataMinder distribution image. Run setup.exe to launch the CA DataMinder installation wizard.

   The Installation Type screen opens.

2. Click Advanced Installation.
3. In the Advanced Install Options screen, choose Endpoint Agents and then click Install.

   This launches the CA DataMinder client installation wizard in a separate window.

4. In the client installation wizard, navigate to the Customer Setup screen.
5. In the Custom Setup screen, choose Network Agent.
6. In the final wizard screen, click Install to start the file transfer.

To configure the CNA

See the following sections for full details. Briefly, you need to:

1. (Optional) Edit the machine policy for the host computer to exclude specific applications or browsers from policy control.

   We recommend that you edit the Common Client Policy.

2. Set up Data In Motion triggers and control actions in your user policies.

More information:

Configure the Local Machine Policy (see page 99)
Configure the User Policy (see page 100)

Configure the Local Machine Policy

(Optional)

If required, you can configure the network agent to ignore network activity in specific applications or browsers. You specify the applications and browsers in the machine policy. We recommend that you edit the Common Client Policy. The key settings are in the following folder:

Client Network Agent folder

This folder contains the Applications settings. If required, you can edit these settings to set which applications are exempt from or included in policy control. (By default, the network agent monitors common web browsers and Microsoft Office applications.)

Important! Be aware that the network agent is not suitable for monitoring Office Communicator traffic! See the note below.

Which Application List?

This setting specifies whether the network agent uses an Included or Excluded list of applications. By default, the network agent uses the Included list which contains a predefined set of default applications.

Included Applications

If you specify the Included list, the network agent only monitors the included applications for network activity. By default, this list includes most common browsers and Microsoft Office applications (see page 95).

Note: Before making any changes, review the applications that the network agent will monitor. For example, applications such as Windows Update Agent do not permit their network traffic to be intercepted and may be adversely affected.

Excluded Applications

If you specify the Excluded list, the network agent monitors all applications except those on the Excluded list. The network agent ignores network activity in excluded applications and browsers. Such activity is exempt from policy control.

For example, you may want to exempt Microsoft Word when it is used to check in or check out documents from a SharePoint site.

Note: By default, the following applications and services are *excluded* from policy control. You cannot override these defaults.

- Microsoft Office Communicator
- Windows services
- CA DataMinder

Configure the User Policy

To complete the network agent deployment, you must edit Data In Motion triggers and control actions in the user policy.

These triggers include settings that let you specify which types of document or data submission you want the network agent to detect. This section focuses on the key Data In Motion settings for the network agent.

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents. Verify that the following agent is selected:

- Client Network Agent for File

  You *must* select this agent if you want to analyze data submitted to web sites, including files being uploaded to file sync websites such as DropBox.com.

Which Targets?

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

Use the Targets settings to define URLs that you want to monitor or exempt. You can specify lists of included or excluded URLs.

Type the URLs that you want to include or exclude. Use ? and * wildcards if required. If you set up the trigger to use:

- Included URLs**,** the trigger only fires if a user tries to submit data to a URL on the Included list. For example, add www.facebook.com to the Included list.
- Excluded URLs**,** these URLs are exempted from control by the network agent. But attempts to submit data to any other (unlisted) URL *will* fire the trigger.

Top Level File Lists

All Data In Motion triggers include Top Level File Lists. Use these lists to detect normal files or zip files, or files in network locations.

Edit these lists to identify the names of files that you want to apply policy to. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, choose whether to use an Included, Excluded or Ignored file list.

Individual/Embedded File List

If required, Data In Motion triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Intervention

In each Data In Motion control action, the Intervention setting determines how the network agent handles data submissions to web sites. The key supported options are Block and Categorize. The Block option prevents the user from submitting data or uploading a file.

Note: The network agent also supports None and No Further Actions intervention options.

Chapter 7: Endpoint Hardening

This section describes measures to control the risk of end users circumventing, disabling, or otherwise avoiding the attentions of the CA DataMinder endpoint agent.

This section contains the following topics:

Why Endpoint Hardening?

There can be motivation for end users to circumvent, disable, or otherwise avoid the attentions of the CA DataMinder endpoint agent. Endpoint agents include various email, browser, and application plug-ins and other CA DataMinder components, including the collection manager (WgnCM) and the CA DataMinder infrastructure service (WgnInfra).

Important: We recommend one single measure above all others to reduce or eliminate the risk of users tampering with your CA DataMinder endpoint agent installation: Ensure that users are not given local administrator privileges over their workstations, and that they do not have access to an account with such privileges.
Read this guide before installing CA DataMinder, because some security decisions have an impact on your choice of deployment options.

Most customers already employ methods to limit the ability of users to reconfigure their clients. To ensure maximum compatibility with such methods, the CA DataMinder endpoint agent does not automatically enable the techniques suggested in this document. However, you can add an extension to the installation process to invoke these techniques automatically.

Contact CA Technologies to discuss your requirements.

The following sections describe further measures that you can use to control the risk.

Hardening Email Endpoints

More information:

Re-enable Outlook Endpoint Agent Automatically

The CA DataMinder Outlook agent is an Outlook COM add-in. Typically, if users have the necessary permissions, they can disable Outlook add-ins.

To prevent users from disabling the CA DataMinder Outlook agent, CA DataMinder automatically and silently re-enables the agent if a user disables it. After deploying the CA DataMinder Outlook agent, create the following DWORD registry values to control the re-enabling behavior.

Follow these steps:

1. Log on to the machine hosting the Outlook agent.
2. Edit the following registry key:

   `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA DataMinder\CurrentVersion\EMail`

   Or for a 32-bit Outlook client running on a 64-bit OS:

   `HKEY_LOCAL_MACHINE\Software\WOW6432Node\ComputerAssociates\CA DataMinder\CurrentVersion\EMail`

3. Add the following registry values:

OutlookMonitorIntervalInSeconds

Type: REG_DWORD

Data: Specifies how often CA DataMinder verifies whether the Outlook client agent is disabled in the current session. (A security feature in Outlook can automatically disable certain add-ins). Set this option to 0 to disable monitoring. Specifically, it checks the registry for the wgnemol.dll name and path.

Default: 5 seconds

OutlookRepairDisabledExtension

Type: REG_DWORD

Data: Specifies whether CA DataMinder should re-enable the Outlook client agent if it is found to be disabled. If this registry value is set to a non-zero value and the Outlook client agent is found to be disabled, CA DataMinder re-enables the client agent and writes a Windows application log entry to that effect.

Default: 0 (do not re-enable)

Note: For more information about how to configure the Outlook Agent using EmailClientOptions.mst, see the 'Technical Information, Installation Transforms' section in the *Platform Deployment Guide*.

Working Offline

Microsoft Outlook and Notes both offer users the ability to work offline. This can create potential loopholes within CA DataMinder.

Prevent Emails From Being Deleted

This problem can only occur with client integration when outgoing e-mail triggers are configured to forward e-mails to other recipients, for example, compliance officers.

CA DataMinder policy triggers can be configured to forward e-mails to another recipient automatically, for example, a compliance officer. If an e-mail causes such a trigger to fire, both the original e-mail and the forwarded message remain in the outbox of the sender's local mailbox until the sender goes back online. The sender has opportunity to delete the e-mail intended for the compliance officer before going back online. Although the policy breach is recorded in the CMS, the original e-mail reaches its recipients, but the forwarded message is not sent to the compliance officer because the sender deleted it from their local Outbox.

To help ensure that e-mails are correctly forwarded to compliance officers, we strongly recommend installing a hybrid client and server agent deployment (see previous section).

- Explicitly configure the Exchange or Domino server agent to reprocess e-mails already processed by an Outlook or Notes client agent.
- If you do install both client and server agents, edit the ReprocessClientEmails registry value on the Exchange or Domino server. For details, see the *Message Server Integration Guide*.

Ensure That Emails Are Captured

This problem can only occur with client integration when outgoing e-mail triggers are configured to perform recipient lookup operations.

CA DataMinder policy triggers can be configured to look up recipient details on an Exchange or Domino server to process outgoing e-mails. If an e-mail is sent to a distribution list, CA DataMinder extracts details for each member of the list. But if a user sends an e-mail while disconnected from their organization's e-mail server, CA DataMinder cannot connect to Exchange or Domino and so cannot extract details for members of distribution lists saved in the local address book. As a result, e-mail triggers set up to detect specific recipients do not fire and the e-mail is not captured or controlled.

This problem applies to users working offline in Microsoft Outlook and running Lotus Notes in 'island mode'. In Outlook, you cannot expand distribution lists when working offline. In Lotus Notes, you can expand distribution lists when working in island mode, but only if the local address books have been synchronized with the ones on the Domino server.

To help ensure that any policy triggers dependent on recipient details are applied correctly to e-mails sent under these conditions, we strongly recommend installing a hybrid client and server agent deployment.

- Explicitly configure the Exchange or Domino server agent to reprocess e-mails already processed by an Outlook or Notes client agent.
- If you do install both client and server agents, edit the ReprocessClientEmails registry value on the Exchange or Domino server. For detals, see the *Message Server Integration Guide*.

Deploy Server-Side Email Enforcement

If client-side techniques do not provide sufficient protection (for example, you cannot control Local Administrator rights), you need server-side enforcement. We recommend that you deploy CA DataMinder email server agents to monitor and control email transiting through your Microsoft Exchange or Lotus Domino servers.

The CA DataMinder Exchange and Domino server agents can apply policy at the email server regardless of whether the Outlook or Notes client agent has already applied policy, and do so by default if policy has not been applied. Specifically, a server agent can detect whether the CA DataMinder endpoint agent has already processed a message. If the message has not already been processed, the server agent infers that the CA DataMinder endpoint agent is either not present on the sender's client, or has been disabled.

Contact CA Technologies to discuss your requirements.

General Hardening Recommendations

Block Unauthorized Browsers and Email Applications

'Circumvention' means that the user runs an email or browser application for which CA DataMinder does not offer an endpoint agent (for example, the Mozilla Thunderbird and Zimbra email applications).

To prevent circumvention, configure Application Monitor control actions in the user policy to block users from running these applications.

Follow these steps:

1. Launch the Administration console and open User Administration or Machine Administration.
2. Select a User, Group and click Edit policy.
3. Browse to the following policy path:
   `Control\Application Monitor\Control Triggers\Application n\`
4. Specify the application included in the ban, for example thunderbird.exe or zdesktop.exe.
5. Browse to the following policy path:
   `Control\Application Monitor\Control Actions\Control Action n\`
6. Set the Intervention option for the control action to Block.

   Starting the application now triggers a block action.

Prevent Unauthorized Uninstallation of CA DataMinder

By default, CA DataMinder is installed in such a way that users can view, modify, or remove the endpoint using the standard Windows utility 'Add or Remove Programs'. However, CA DataMinder ships with a sample Microsoft Installer transform script that prevents the user from invoking 'Add or Remove Programs' to modify or uninstall the endpoint.

For command line, Group Policy or SMS installations, you can use a transform to prevent users from uninstalling CA DataMinder with the Add/Remove Programs utility. The ClientLockDown.mst transform disables the Change and Remove buttons when a user selects CA DataMinder in the Add/Remove Programs dialog.

Follow these steps:

1. Find the ClientLockDown.vbs script in the \Support folder of your CA DataMinder distribution media.
2. Run the script.

   It creates the ClientLockDown_Client.mst (or ClientLockDown_Client_x64.mst) transform.
3. Copy the transform into the folder containing your administrative installation source image.
4. When you install the client, also deploy the ClientLockDown_Client.mst transform.

   `msiexec /i path\client.msi ARPSYSTEMCOMPONENT=1 TRANSFORMS=path\ClientLockDown_Client.mst`

Use File Permissions to Protect Event Data and Document Fingerprints

We recommend to limit user access to event data held in the local endpoint agent database, and to email or web page content in blob files held below the CA DataMinder data folder. You also want to prevent unauthorized users from tampering with, for example, the document fingerprints stored in content index files in the "C:\ProgramData\CA\CA DataMinder\data\PRC\IndexCache" folder.

By default, the CA DataMinder software and data are in some of the following folders, depending on your operating system:

```
C:\Program Files\CA\CA DataMinder\
C:\Program Files (x86)\CA\CA DataMinder\
C:\ProgramData\CA\CA DataMinder\data\
C:\Documents and Settings\All Users\Application Data\CA\CA DataMinder\
```

Note: On an NTFS volume, the "CA" folders typically inherit attributes and permissions from their parent folders. The default file system privileges provide basic protection because users require administrator privileges to modify files in these folders.

Follow these steps:

1. Change the folder attributes of all "CA" folders to System Hidden where necessary.

   This attribute prevents users from seeing the CA DataMinder software and data files.

2. Reduce user permissions to the "C:\ProgramData\CA\CA DataMinder\data" folder.

3. Reduce user permissions to the "C:\Documents and Settings\All Users\Application Data\CA\CA DataMinder\" folder.

Important: Ensure that the account under which the CA DataMinder infrastructure service runs (typically LocalSystem) retains full access to all CA DataMinder folders!

Preventing Man-in-the-Middle Attacks

CA DataMinder endpoints rely on network communication between the CA DataMinder Infrastructure Services to exchange data (such as events, or policies) with their parent server. This network communication makes the endpoint server subject to a possible 'man-in-the-middle' attack: In such an attack, the endpoint is not communicating with its real parent, but with a rogue server.

CA DataMinder uses various combinations of proprietary UDP, and encrypted Java RMI TCP-based protocols for its communications.

1. Before a communication session exchanges data, the protocols verify the identity of the server and client. If the identity is incorrect, the protocol terminates the session and logs the termination.

2. In sessions where important policy data is synchronized, the installation code of the CA DataMinder system is also verified. The verification helps ensure that the sessions contact the same CA DataMinder network of clients and servers.

What do realistic and likely attacks look like?

- It is possible (but, due to the proprietary nature of the communications, unlikely) that attackers develop custom software to spoof the behavior of a parent server. The most realistic form of 'attack' would come from a real CA DataMinder server which is configured to be a rogue server.

- The most likely attack is the reconfiguration of the endpoints 'hosts' or 'lmhosts' files: Attackers attempt to map the parent server to a rogue server, or to an invalid IP address, to stop communications with a parent server.

  By default, Administrator rights are required to edit these files. Depending upon the actual communications being performed, this reconfiguration can be sufficient to fool an endpoint into certain communications with a 'rogue' server.

If this level of protection is insufficient, configure CA DataMinder to run in Advanced Encryption Mode (FIPS 140-2). This mode uses TLS and certificates to provide the ultimate protection for communications between the endpoint and its parent. Manufacturing a 'man-in-the-middle' attack is near-impossible without having first compromised the security of either the endpoint or parent server.

Important: You have to deploy CA DataMinder in Advanced Encryption Mode from the start. You cannot convert an existing CA DataMinder deployment to Advanced Encryption Mode.

For CA DataMinder to be compatible with FIPS 140-2, you deploy it in Advanced Encryption Mode. This section describes the deployment procedure.

Follow these steps:

1. Designate a secure server that is separate from your intended CA DataMinder enterprise.
2. Generate the self-signed root certificate.
3. Generate the Key Store and Revocation List.
4. Deploy your CA DataMinder servers and client machines.
    a. Create new administrative installation source images.
    b. Customize the new source images.
    c. Install the servers and client machines from the appropriate source image.
5. Confirm that encryption is correctly configured in the machine policy for all your CA DataMinder servers and client machines.
6. Secure the critical Advanced Encryption files on your CA DataMinder servers and client machines so that they can only be accessed by the CA DataMinder infrastructure.

Note: See the 'Advanced Encryption Mode' chapter in the *Platform Deployment Guide* for further details as part of the CA DataMinder deployment procedure.

Apply Registry Permissions

On CA DataMinder endpoints, you can make the following registry changes:

HKEY_LOCAL_MACHINE\Software\CA DataMinder

This registry key contains machine-wide settings written only by the installer and the CA DataMinder infrastructure service.

You can apply permissions to this key using Regedt32 to prevent access by unauthorized users. The SYSTEM (Local System) account requires full access.

HKEY_CURRENT_USER\Software\CA DataMinder

This registry key contains housekeeping information, written by the runtime integration components and the consoles.

HKEY_CLASSES_ROOT

The install process registers COM servers and file extensions under the HKEY_CLASSES_ROOT registry hive and other integration settings under HKEY_LOCAL_MACHINE\Software\Microsoft registry key.

Important: Tampering with these registry values can jeopardize the integrity of the installation. We do not recommend restrictive permissions here. We strongly recommend that this registry key retains Read access for all user types.

Registry Changes for Endpoint Agents

When you install a CA DataMinder browser and email endpoint agent, the installer makes changes to the following registry keys:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
  \Explorer\Browser Helper Objects

HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\Client\Extensions\Wgn
```

Automated Endpoint Protection

Most customers already employ methods to limit the ability of users to reconfigure their clients. To ensure maximum compatibility with such methods, the CA DataMinder endpoint agent does not automatically enable the techniques suggested in this document. However, you can add an extension to the installation process to invoke these techniques automatically.

Contact CA Technologies to discuss your requirements.

Chapter 8: Known Issues

This section contains the following topics:

Firewall Configuration on Endpoints

The CA DataMinder installation wizard automatically registers the CA DataMinder infrastructure as a firewall exception. This enables data, including policy updates, to replicate unhindered through the firewall between CA DataMinder endpoints and servers. However, you must *disable* the 'exception blocking' feature in the Windows firewall to allow the CA DataMinder exceptions.

Endpoints on Windows XP and Windows 2003

Clear the ‘Don’t allow exceptions’ check box. Find this setting on the General tab of the Windows Firewall applet.

Endpoints on Windows Vista, Windows 7, and Windows 8

Clear the 'Block all incoming connections' option. Find this option in the 'Domain network settings' section of the Windows Firewall applet.

Endpoints on Windows Server 2008 and Windows Server 2012

Clear the 'Block all incoming connections' option. Find this option in the 'Domain network settings' section of the Windows Firewall applet.

Note: CA DataMinder endpoint agents support 'centralized applications' running on Windows Server. For these deployments, users access applications such as Outlook on a central server using, for example, Citrix or Remote Desktop Connection.

Important! If you do not clear the checkbox or options described above, these firewall settings remain *enabled*. Consequently, the Windows Firewall allows no firewall exceptions. It therefore blocks the CA DataMinder infrastructure, which prevents the CA DataMinder endpoint computers from contacting its parent server. In particular, endpoint agents cannot receive any user or machine policies. The endpoint agents are therefore paralyzed and cannot capture or control user activity.

CFSA Can Prevent BitLocker From Encrypting USB Devices

The Client File System Agent (CFSA) can affect the operation of the BitLocker To Go encryption feature on endpoint computers.

If the CFSA is installed on an endpoint computer and configured to apply policy to files being copied to removable devices (such as USB drives or SD cards), BitLocker cannot initialize removable devices for encryption. That is, it cannot give these devices the "lockdown treatment". This is because the BitLocker initialization process is denied write access to the device by the CFSA.

Note: This problem only occurs if the CFSA is explicitly configured to apply policy to removable devices. Also, if a removable device has been initialized by BitLocker running on a different computer, the device can used on any endpoint computer hosting the CFSA, even if the CFSA is configured to apply policy to removable devices.

Internet Explorer 9 Can Hang After Displaying Intervention Dialog

Under certain circumstances, typically, when the browser has submitted data using AJAX (for example, when uploading files to web mail sites), the CA DataMinder intervention dialog can cause Internet Explorer v9 to hang. This issue has been found with update versions 9.0.3 and 9.0.6, and can be assumed to exist on others. The issue has been reported to Microsoft.

As a workaround, add the following setting to the registry for each user who may be affected:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows]

"DetourDialogs"="no"
```