

# Agentless Exception Monitoring in Operations Manager 2007

---

## Functionality Overview and Installation Walkthrough

**Version 1.0**

**Authors:**

Anders Bengtsson, MCSE(Security) | <http://www.contoso.se>  
Pete Zerger, MCSE(Messaging) | MCTS(SQL 2005) | MVP-MOM

**Some Rights Reserved:** You are free to reference this document, so long as you properly credit the author and provide a link back to the published source.

# Table of Contents

Introduction .....	3
Agentless Exception Monitoring (AEM) .....	3
Customer Experience Improvement Program (CEIP) .....	4
AEM Installation and Configuration .....	4
Configure a Management Server for AEM .....	4
Configure a Group Policy Object for AEM .....	6
Configuring Error Transmission .....	6
Test AEM .....	7
Customize client monitoring data collection and the solution response URL .....	7
Viewing Collected Data .....	8
Accessing AEM Views and Reports .....	8
Scalability and Grooming .....	9
FAQ about AEM .....	9
Additional Resources .....	10
Feedback .....	10

## Introduction

Monitoring desktop client hardware, operating system and application faults can be of great value in terms of reducing total cost of ownership (TCO) through identification of widespread faults in the monitored environment. In Operations Manager 2007, there are actually three components for monitoring the client experience:

- Agentless Exception Monitoring (AEM)
- Customer Experience Improvement Program (CEIP)
- Management Packs for Windows-based workstation operating systems and applications

In this document, we'll focus specifically on configuration Agent Exception Monitoring feature. Perhaps it is appropriate here to define what AEM entails in a bit more detail.

### Agentless Exception Monitoring (AEM)

AEM enables monitoring operating systems for crashes and applications for errors. Error reporting clients are configured via group policy to redirect error reports to an Operations Manager 2007 Management Server, instead of sending these reports directly to Microsoft. Operations Manager 2007 provides detailed views and reports into the error data collected throughout your organization. This facilitates determination of how often a given operating system or application experiences an error and the number of affected computers and users. This determination enables support teams to direct efforts to the areas where they will have the most benefit to the organization.

It is actually not necessary to have an Ops Mgr agent deployed to a client machine in order for it to participate in Agent Exception Monitoring. However, these machines will appear in the Monitoring pane as "Not monitored" and will not appear in the Administration pane at all.

The Windows Error Reporting (WER) client is included in the Windows XP and Windows Server 2003 operating system. For Windows 2000, error reporting is not part of the operating system but comes in Microsoft programs, such as Microsoft Office XP and Microsoft Office 2003 applications, Microsoft Visio 2002, and Microsoft Visual Studio .NET., and which report errors in this application. When the error reports are anonymously synchronized with Microsoft, solution responses that are available for the respective errors are provided back to the client. You can also use AEM to provide solutions for issues experienced with your in-house applications.

There are two local security groups created on the management server where AEM – AEMUsers and AEMAgent. By default, AEMUsers should contain authenticated users. This group represents all credentials that will have access to the AEM data. Typically these are the credentials Watson or the Windows Error reporting client runs under to send Error reports. AEMAgent is the group that represents the group that has full access to the AEM files, folders and resources. This group contains Built-in Administrators by default. During creation of the file share created by the 'Configure Client monitoring' wizard, the above groups are used to ACL various directories and files.

In this release, when error data is transmitted cannot be controlled. On demand transmission or scheduled time configurable transmission will be possible in the next release.

## Customer Experience Improvement Program (CEIP)

When you choose to participate, Windows automatically sends information to Microsoft about how you use certain products. Information from your computer is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. In the Client Monitoring Configuration Wizard, you will actually be presented a single screen for configuring Customer Experience Improvement Program (CEIP) settings. This will you to determine whether customer error data if first forwarded to a management server before being forwarded to Microsoft, or if the data will be forwarded to Microsoft directly.

## AEM Installation and Configuration

### Configure a Management Server for AEM

In this chapter we will enable AEM on a management server and also create the ADM file that we will use to control client error reporting.

1. From the **Start Menu**, select the **SCOM Operations Console**
2. In the Navigation pane (left), Click **Administration**
3. In the Administration pane, click **Management Servers**
4. In the Action pane, right click a **management server** and select **Configure Client Monitoring** from the context menu

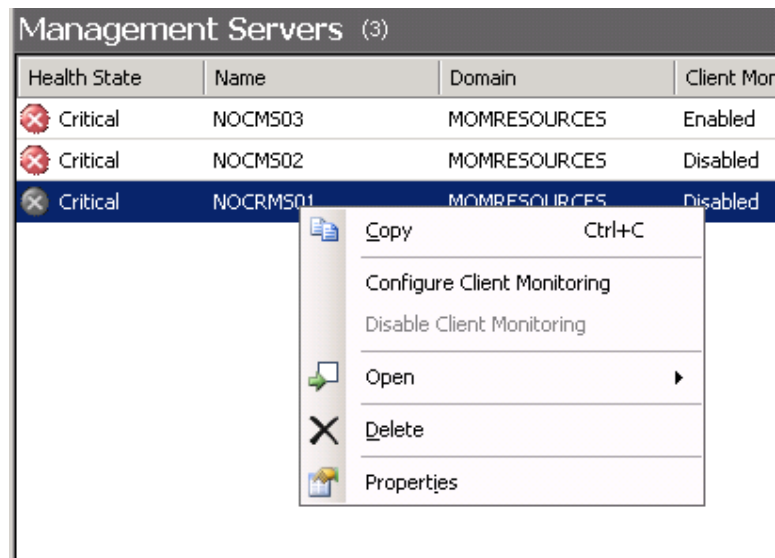


Figure 1 - Launch Client Monitoring Configuration Wizard

5. In the Client Monitoring Configuration Wizard - Introduction window, click **Next**

- In the Client Monitoring Configuration Wizard - Customer Experience Improvement Program window, select **"Yes, use the selected Management Server to collect and forward CEIP data to Microsoft"**. **Uncheck "Use Secure Socket (SSL) protocol"**, the only time you should use SSL is when you have a certificate installed on your management server. Leave default **port 51907** and leave **Use Windows Authentication** checked. Click **Next**

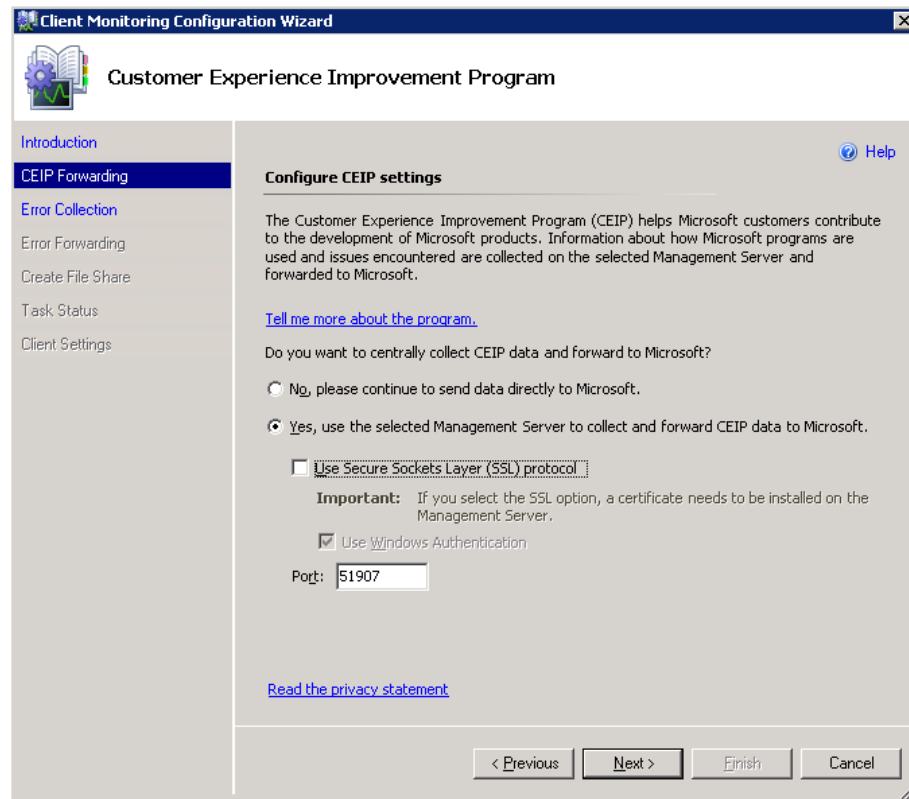


Figure 2 - CEIP Settings in Client Monitoring Configuration Wizard

- In the Client Monitoring Configuration Wizard - Specify error collection settings window, input a file share path where to collect error reports, for example C:\ErrorData. Check **"Collect error reports from Windows Vista-based or later clients"** and **uncheck "Use Secure Sockets Layer (SSL) protocol"**. Leave default **port 51906**. Input an **organization name**, this name will be displayed in error messages at client computers. Click **Next**



The file share for error reports must be on a LOCAL NTFS drive with at least 2GB of free space. Do not input a UNC path or a mapped drive letter or configuration will fail.

- In the Client Monitoring Configuration Wizard - Configure Error Forwarding to Microsoft, select **"Forward all collected error to Microsoft (Recommended)"** and also select **"Detailed (the error signature and requested additional data)"**. Click **Next**

9. In the Client Monitoring Configuration Wizard - Task Credentials, input an account with enough permissions or use a existing user account. Click **Next**
10. In the Client Monitoring Configuration Wizard - Task Status, verify that you get "**A file share has been successfully created**", click **Next**
11. In the Client Monitoring Configuration Wizard - Create Group Policy Administrative Template; Select where to store the ADM file that you will use to control clients error reporting. Note that the location must end with .adm, for example input C:\AEM.adm. Click **Finish**.

## Configure a Group Policy Object for AEM

Next, we will import the ADM file into a group policy object and also associate the policy with a organization unit (OU) including clients that you want to monitor. In this guide I will use Group Policy Management Console (GPMC). GPMC is a free tool from Microsoft used to administrate group policies.

1. From the **Start Menu**, select Group Policy Management
2. In Group Policy Management, in the left pane, expand your forest and your domains, right-click Group Policy Objects and choose **New**
3. In the New GPO box, input a suitable name, for example AEM and click **OK**
4. Right-click the new group policy object and choose **Edit**
5. In Group Policy Object Editor, expand **Computer Configuration** and **right-click Administrative Templates** and choose **Add/Remove Templates...**
6. In the Add/Remove Templates window, click **Add...** and select your AEM.adm file that you created during management server configuration. Click **Close**
7. In the Group Policy Object Editor, there is now a new folder under Administrative Templates named System Center Operations Manager (SCOM). Expand the folder and **enable all policies in it and in all subfolders**. Note that some policies will be set to disable automatically, even if you enable them. Then **close Group Policy Object Editor**.
8. In Group Policy Management, right click a OU where you store computer objects for machines you want to monitor, and choose **Link a Existing GPO...**
9. In the Select GPO, select the AEM group policy object and **click OK**
10. Close the Group Policy Management

## Configuring Error Transmission

With error transmission settings you can control which error reports are sent to Microsoft and what diagnostic data is included.

1. From the **Start Menu**, select the SCOM **Operations Console**

2. In the Navigation pane (left), Click **Administration**
3. In the Administration pane, click **Settings**
4. In the Action pane, right click **Privacy** and select **Properties** from the context menu
5. In the Global Management Group Settings - Privacy window, click **Error Transmission**
6. On the Error Transmission tab, if you click **Filter** you can specify the criteria for errors that you want send to Microsoft. On this tab you can also specify which additional files you want to send to Microsoft, for example memory dumps. You can also specify if you want to show Microsoft solution on the error on error reporting computer, or if you want to show a internal webpage.

Make sure that these settings are in line with your organization security and privacy policy.

7. On the Error Transmission tab, click **OK**

## Test AEM

You can add a registry key to any client computer to add the feature to generate a crash.

1. From the **Start Menu** choose **Run** and input **regedit**, then click **OK**
2. In Registry Editor, browse to  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters
3. In Registry Editor, right-click and choose **New DWORD Value**. Name the new key **CrashOnCtrlScroll**, and set **value 1**
4. **Quit Registry Editor** and **restart the computer**

When you computer is up and running again, you should be able to generate a blue screen by holding down the right Ctrl key and click Scroll Lock twice.

## Customize client monitoring data collection and the solution response URL

These settings can help you control which data to collect when an error occurs. These settings also control which link to show users when a error occurs.

1. From the **Start Menu**, select the **SCOM Operations Console**
2. In the Navigation pane (left), Click **Monitoring**
3. In the Monitoring pane, expand **Agentless Exception Monitoring** and click **Application Error Group View**
4. In the Action pane, click **Show or Edit Error Group Properties**

5. In the Error Bucket Responses window, you can click **Custom Collection** and then click **Edit** to create a collection configuration on what diagnostic data to collect when a error occurs. Note that you can use variables like %WINDIR% for file paths.
6. In the Error Bucket Responses window, in the lower part of the window you can choose which link to be shown for a user when a error occurs. For example a link to your organization self service portal or knowledgebase portal. Click **OK**

## Viewing Collected Data

### Accessing AEM Views and Reports

There are several views into AEM data accessible in the Monitoring space. To access these views, expand the Agentless Exception Monitoring

1. Log on to the computer with an account that is a member of the Operations Manager Operators role for the Operations Manager 2007 Management Group.
2. In the Operations Console, select the **Monitoring** workspace.

**NOTE:** When you run the Operations Console on a computer that is not a Management Server, the Connect To Server dialog box displays. In the Server name text box, type the name of the Operations Manager 2007 Management Server that you want the Operations Console to connect to.

3. Expand the **Monitoring** pane, then **Agentless Exception Monitoring**, and then click on a view.

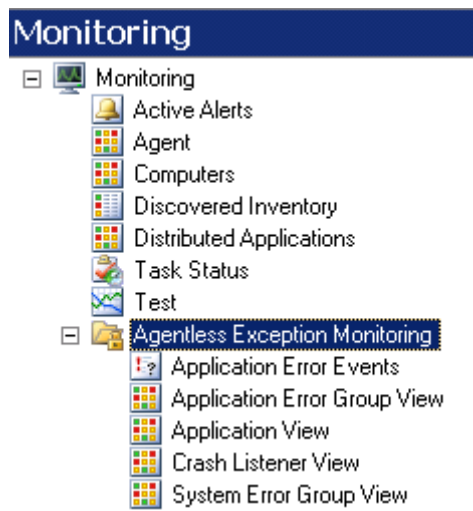


Figure 3 - AEM views in the Monitoring space

There are also 4 reports in the Reporting space to display information on aggregated AEM data. These can be accessed in the Operations Console in the Reporting space:

- Top Applications
- Top Application Growth and Resolution
- Top Error Groups
- Top Error Growth and Resolution

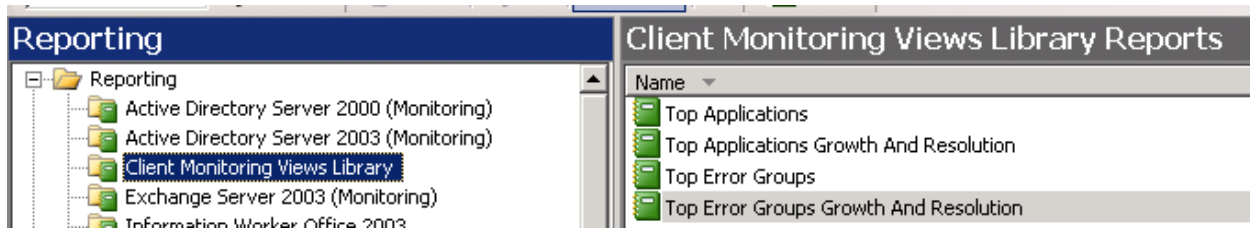


Figure 4 - AEM reports in the Reporting space.

## Scalability and Grooming

A management server playing host to the AEM roles typically experiences high disk I/O, which means the special considerations should be given to the disk subsystem in planning for AEM in your environment. Since the file share must be local, this can mean using DAS, NAS or SAN storage, and precludes the use of DFS as a means to replicate this data to multiple locations. Care should be taken to provide dedicated disk I/O separate from any system and database volumes. The Operations Manager 2007 Performance and Scalability Guide provides hardware sizing guidance for up to 100,000 clients, and should be consulting in the course of your deployment planning efforts.

By default, crash dumps older than 45 days are groomed from the file share.

## FAQ about AEM

### Q: Will AEM work with old versions of Windows?

A: AEM will work with Windows XP, Windows 2003 and later. For old versions like Windows 2000 there is no support in the OS, instead the support can be in applications. For example Office 2000 and Windows Media Player support forward of error reports.

### Q: Why are my AEM machines without a agent under "not monitored" machines in the console?

A: When an error report is received from a computer AEM registry the machine in the operations database. If the machine don't have a agent installed it will be shown as not monitored.

## **Additional Resources**

### **Performance and Scalability Whitepaper**

[http://download.microsoft.com/download/d/3/6/d3633fa3-ce15-4071-be51-5e036a36f965/OM2007\\_PerfScal.doc](http://download.microsoft.com/download/d/3/6/d3633fa3-ce15-4071-be51-5e036a36f965/OM2007_PerfScal.doc)

### **Operations Manager 2007 training video, Configure Client Monitoring**

[http://www.microsoft.com/winme/0703/28666/AEM\\_Edited.aspx](http://www.microsoft.com/winme/0703/28666/AEM_Edited.aspx)

### **System Center Operations Manager 2007 Product Documentation**

<http://www.microsoft.com/technet/opsmgr/2007/library/proddocs.mspix>

### **Group Policy Management Console with Service Pack 1**

<http://www.microsoft.com/downloads/details.aspx?familyid=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=en>

## **Feedback**

I hope you find this article helpful. Your feedback is always welcome and appreciated at [anders@contoso.se](mailto:anders@contoso.se) or [administrator@systemcenterforum.org](mailto:administrator@systemcenterforum.org)