

# Corporate Error Reporting

Architecture



Microsoft  
**Software Assurance**  
for Volume Licensing

# Contents

<b>Overview</b>	1
<b>Error Reporting</b>	2
Microsoft Windows Error Reporting Overview	3
The Error Reporting Process	3
Corporate Error Reporting (CER) Overview	5
Error Reporting Policy Overview	6
<b>CER Architecture and Components</b>	7
Architectural Overview	7
CER Shared Directory	7
Mapping Corporate Error Reporting	8
<b>Contoso CER Design</b>	10
Machines To Be Configured For CER	10
CER Server Architecture	10
Requirements Meet	11
Group Policies	12
CER Template	12
CER Group Policy Options	13
Windows Error Reporting (WER)	15
WER Group Policy Options	15
Office 2003 Policies	18
Office Group Policy Options	18
CER Design and Settings	22
<b>Operating CER</b>	23
The Console	23
Responses	23
Submitting Errors	23
Backup and Recovery	23
Monitoring CER	23
<b>Notes</b>	24

# Overview

Corporate Error Reporting (CER) is a Microsoft tool that allows companies to capture information from applications that are Windows Error Reporting (WER) enabled. WER allows applications and the Windows OS to forward crash reports to Microsoft when they occur. Several Microsoft products; including Windows 2003 Server, Windows XP, and Office 2003 have been enabled to forward crash dump information to Microsoft for further analysis when errors occur. This information is critical in helping Microsoft to better understand errors and continuously improve the reliability of its products and 3rd party products.

CER provides companies with several benefits. Many companies do not want their users to automatically forward crash data to Microsoft due to concerns of forwarding company confidential information. CER allows administrators to control crash data before it is forwarded to Microsoft.

**Note:** Microsoft has strict confidentiality restrictions with the crash information it receives. For full details refer to the following web site. <http://oca.microsoft.com/en/Privacy.asp?t=0>

The primary benefit Contoso will receive with implementing CER is the ability to track crash errors within the environment. By having hard data of when Contoso users are experiencing crash events and performing trend analysis Contoso will be able to prioritize which updates to the environment will have the most positive impact to its users. This information will also be a valuable metric for the IT department to measure the effect it has in improving user productivity.

The requirements for implementing and maintaining CER are fairly light. Clients and servers are configured to use CER through Active Directory Group Policies. The CER administration console should be installed on a centrally located file server. It will create the required directory structure and permissions. Once CER is implemented the ongoing maintenance involves reviewing and forwarding crash dumps to Microsoft (this can be automated), and review crash statistics to determine where the most pain is and how to resolve it.

This document will give an overview of how WER works and provide a recommended architecture and configuration settings for Contoso to implement CER.

# Error Reporting

WER is a feature included with Windows XP and the Windows Server 2003 family that helps Microsoft track and address operating system and application interoperability errors. Along with applications such as Office XP and Office 2003 applications, Visio 2002, and Visual Studio .NET, Windows XP and Windows Server 2003 have the ability to send information about errors to Microsoft. This notification allows Microsoft to investigate the cause of the error and provide a solution to the user the next time a report is submitted.

CER includes a console and set of policies that allow administrators to redirect error reports from end-users' computers to a central shared directory on the corporate network, where the data can be reviewed and reported to Microsoft by the administrator through the CER console. Figure 1 shows an overview of CER and WER.

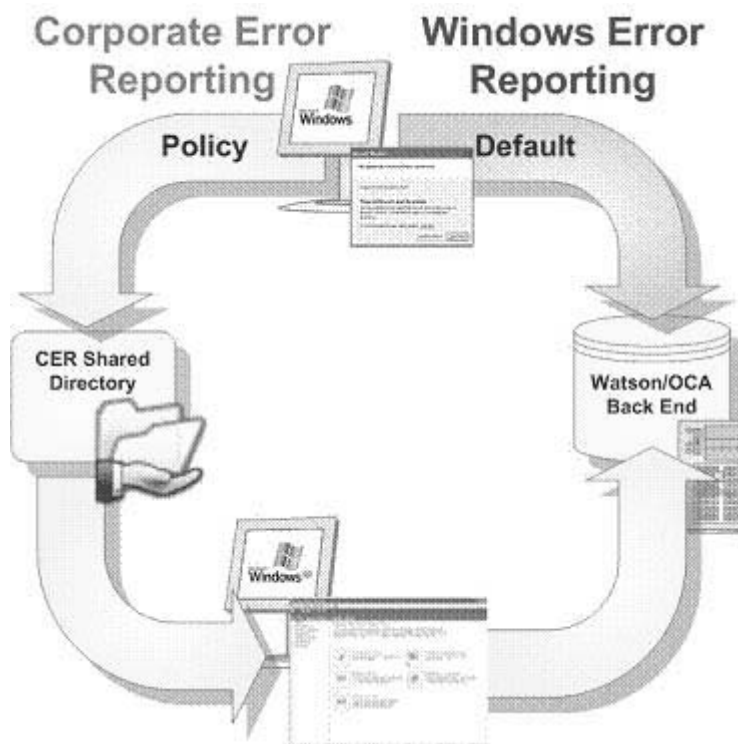


Figure 1 - Corporate Error Reporting and Windows Error Reporting

The CER console (bottom middle of Figure 1) gives the administrator the ability to control the type and amount of data collected and reported to Microsoft, as well as the response provided by Microsoft in the form of a URL (Universal Resource Locator), and to set a custom URL to redirect users to an internal web site for information on how to prevent the issue in the future. CER is designed for organizations of all sizes who do not wish to arbitrarily report error data to Microsoft and track crashes within their environment.

# Error Reporting

## Microsoft Windows Error Reporting Overview

When you send an error report to Microsoft over the Internet, you provide technical information that product groups at Microsoft use to work with third party software vendors to address the issues being trapped and reported by customers. The data also helps the product groups to enhance future versions of the product. This data is used for quality control purposes only and is not used for tracking individual users or installations for any marketing purpose. If information is available to help you solve the problem, Windows displays an error reporting dialog box with a link to that information. For more information on Microsoft's Data Collection Policy, visit: <http://watson.microsoft.com/dw/dcp.asp>

You can configure error reporting to send Microsoft specific error information as well as reports for operating system errors, Windows component errors or program errors. WER can report kernel mode exceptions, hangs, and user mode exceptions.

By default, any reported errors will be sent directly to Microsoft through the Internet so that development can take a more proactive approach to resolving existing bugs in the code. Errors are dealt with based on the amount of reports on a specific problem. If two users reported the exact same crash, then the reports are filed in the same category. A category with many reports represents a significant problem and is handled first.

## The Error Reporting Process

Error reporting is managed by a client side executable, called DW.exe (DW20.EXE with Office 2003) for applications that ship with error reporting technology, and DWWIN.exe for Windows XP and Windows Server 2003. Although the application client (DW.exe) only handles user mode crash information for the application that shipped with error reporting ability, the operating system client (DWWIN.exe) can report errors in user mode, kernel mode, and unplanned shutdown events.

In the event of a crash or assertion within an error reporting aware application, the application involved in the crash will call out the error reporting executable in a Just-in-Time fashion before the application closes down. The error reporting client saves information such as the application name, application version, and a mini dump of the crash in a local log (such as MSInfo.log). These values make up the parameters of the error report, and their sum is used as the Category ID that Microsoft uses to categorize the report. This information may be useable for identifying the cause of the crash, and will be reported as a base line for the information sent to the Microsoft Error Reporting servers for a user mode crash.

In the error reporting user interface, the user is asked whether to report this crash to Microsoft. The error reporting client will not establish communication with the Microsoft Error Reporting servers without the user's authorization. When the user selects "Yes" to report the crash, the client checks to see if the Internet Connection Wizard has been configured. If not, then the client will fail silently to report the crash to Microsoft without interrupting the user's working experience. The user will not receive an error in this situation, and may believe that the crash data was sent. The crash data will always be written to a local log such as MSInfo.log regardless of whether or not the client machine has Internet access. In any case, the error parameters are always viewable in MSInfo32.exe on Windows XP or Windows Server 2003.

If the user chooses to send the report to Microsoft, a connection is established with Microsoft initially through port 80 (HTTP), and then over port 443 (HTTPS) for the transfer of the report. During the initial call to Microsoft over port 80, the error reporting client determines the action needed based on the parameters in the report. If the error parameters do not equate to an existing category ID, the next available category ID is assigned. In the event that the category ID does exist and additional data was requested by Microsoft to assist in determining the cause of the error to offer a resolution, the error reporting client will submit the additional data over port 443 (HTTPS). All data is sent and received using HTTPS as the transport protocol to ensure secure data transfer to and from the Microsoft Error Reporting server.

When a report is sent to Microsoft, the executable for error reporting will check for any return information response from the Microsoft Error Reporting server. If the error reporting client finds that there is additional information for the user, a link marked as "More Information" will be provided in the reporting dialog box. This link could provide a few different options depending on circumstances:

# Error Reporting

1. If a patch exists, it will point to the URL of an HTML page with information on how to obtain the patch. This likely will point to the Products Update site to request the available patch.
2. If no patch exists and Microsoft Development needs more information to isolate the problem, then the user may be taken to an ASP survey to collect more detailed information to be used to assist in the isolation of the problem.

The process allows a developer to request more detailed data in relation to the crash based on a value set on the Microsoft Error Reporting server. Every time a piece of data is requested users have the option of submitting or not submitting the data being requested.

The error reporting data sent to Microsoft is viewed on a curve, with the categories holding many reports on one end, and the lower hit categories on the other end of the curve. The high end of the curve is reviewed first since creating a resolution for those categories will impact the largest amount of end users.

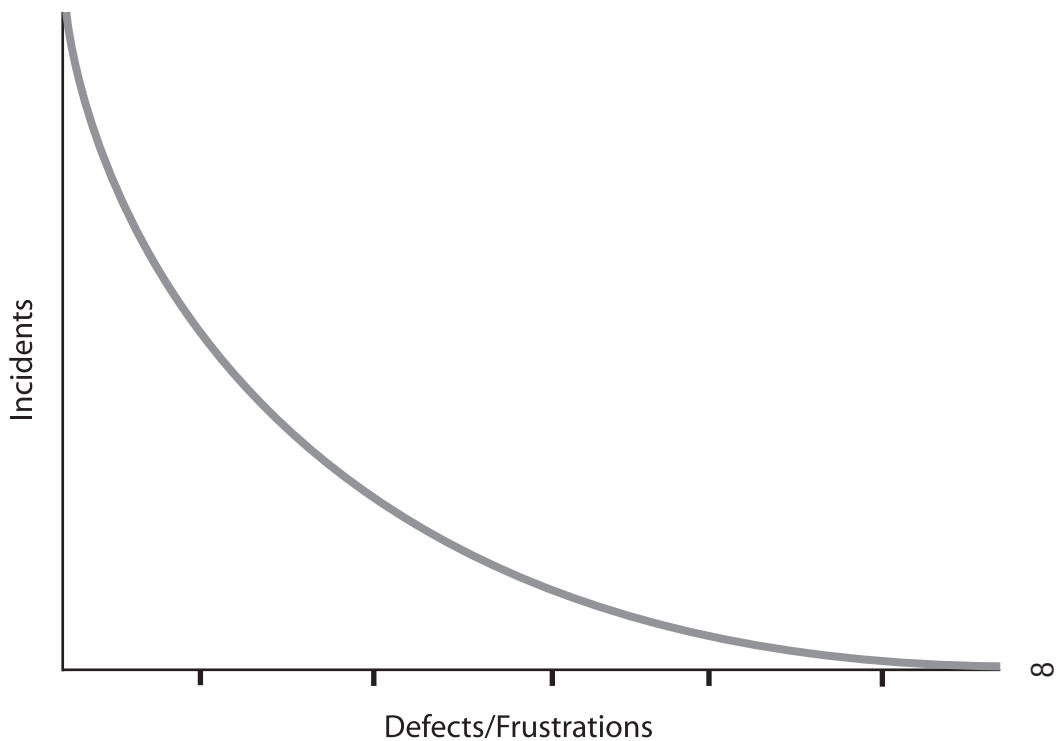


Figure 2 – Incident/Defect curve

The shape of the curve is what makes this whole effort worthwhile. After studying crash related data for several products there is a very clear trend.

- Worst 1% of the defects = 50% of the failures!
- Worst 20% of the defects = 80% of the failures

# Error Reporting

## Corporate Error Reporting Overview

In a corporate environment, it may be important to provide a way to control what data is sent to Microsoft based on the contents of the report. It is possible that the request for more extensive data will return a document, or other bits of personal user information that may contain sensitive material that the corporation would want filtered. Although all data is viewable to the end user before the report is delivered to Microsoft, the end user may not understand all the internal corporate security policies. Error reporting in these corporate environments can be controlled by the implementation of CER.

CER is a set of tools and policies designed for administrators to manage error reports created by the WER client, as well as error reporting clients shipped with applications. CER provides redirection of the error report to an internal shared directory within the company where the report can be stored until reviewed by an administrator. In addition, the CER console provides administrators a way to view the collected data and synchronize the data with Microsoft as appropriate. With this solution implemented, the administrator would be able to collect explicit data on problems with the products that are capable of reporting crash and error events to Microsoft, and evaluate the solutions reported back by Microsoft in a form or a URL before they reach the error reporting clients. This solution also affords the administrator a reference of quantified data collected.

CER is extremely useful in identifying issues based on true metrics within the organization. For example, it is possible to quantify an issue in Microsoft Word running a third party add-in even before the corporate helpdesk is contacted by a user who is tired of seeing Word crash. This allows the administrator to take a more proactive stance in finding solutions for the end users, which ultimately reduces the total cost of ownership for all error reporting aware applications.

If the error reporting clients are configured for CER, the error reports are redirected to a network shared directory available through a Universal Naming Convention (UNC). As a result, administrators in the information technology (IT) department can use the CER console to review the redirected error reports and filter the reports that are sent to Microsoft based on your corporate policies and the data contained within the error report.

CER requires configuration of each desktop that has an error reporting client through policies that set the appropriate registry keys and values for error redirection. The error reporting clients look for these policy keys prior to sending any reports to Microsoft if the send option was elected by the user. Many details of the error reporting process are configurable, such as which data gets sent and where to send the data. Some applications, such as Office 2003, ship with their own administrative templates for configuring error reporting policy through Active Directory. CER 2.0 has its own administrative template and a logon script, either of which can be used to set global policies for some or all error reporting aware applications or operating systems in the network. The CER 2.0 template and script allow administrators to use Group Policy and Active Directory to deploy and manage CER policies in a centralized manner.

# Error Reporting

## Error Reporting Policy Overview

Error reporting clients in Microsoft products enable developers to proactively review and fix crashes in their respective products. The default behavior of an error reporting client is to collect information on the crash and send this data to Microsoft over HTTPS. This behavior can be modified via policy, so that, for example, all information could be sent to an internal location to be analyzed locally. Then, data for individual applications could be sent on to the relevant software vendor or developer, which could work to address issues.

The data collection instructions defined for the error reporting client can be superseded by policy keys in the registry on the client machine. These policy keys are checked each time a report is to be prepared from a crash, and their instructions are followed if found. This policy checking behavior allows corporate administrators to manage error reporting data by using a combination of policy keys on the client machines and the CER console. The Reporting and Collection Options in the CER console allows the administrator to configure the CER shared directory to further modify the clients' behavior.

There are currently three major versions of error reporting clients that may be found with Microsoft products: the Error Reporting (ER) 1.0 client, ER 1.5 client, and ER 2.0 client. The ER 1.0 client can only report faults to Microsoft and cannot be controlled via policy to an alternate reporting location; however this client may be disabled via policy. With the ER 1.5 and ER 2.0 clients, the error reporting behavior can be controlled via policies set by the administrator to control reporting location, company name used in the user interface at the time of the crash, and the amount of data to collect. With the ER 1.0 and ER 1.5 clients, the location of the policy in the registry is set by a flag in the code of the application calling the error reporting client. With the ER 2.0 client the path is hard-coded, and can only be controlled by flags set to indicate per machine or per user policy.

# CER Architecture & Components

The three primary elements of CER 2.0 are the CER 2.0 console, the CER shared directory, and the error reporting clients. These elements work together to create and manage error reports.

## Architectural Overview

Figure 3 shows the architecture of the CER console and command line utility.

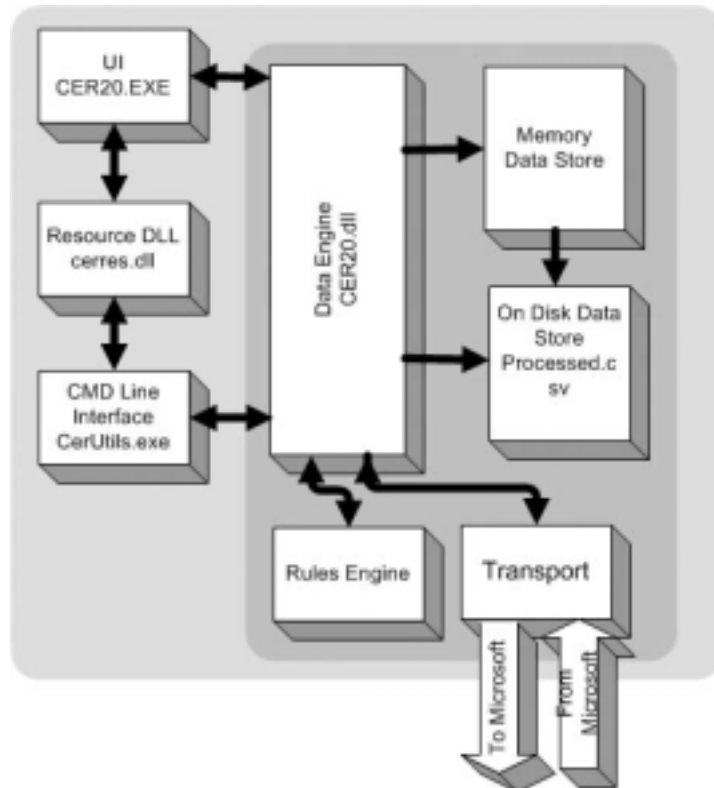


Figure 3 – CER Console and Command Line Utility Architecture

## CER Shared Directory

The CER shared directory is no more than a shared folder structure on an NTFS partition. The error reporting client will access the root of the CER shared directory through the UNC path specified in the local machine's policy for error reporting. The root folder of the CER shared directory can have any name desired, and can be hidden with the \$ variable if desired. The CER console is used to create the entire shared directory automatically with specific permissions to secure the data. An administrator can create the CER shared directory manually and also set specific folder permissions, but this is not recommended.

# CER Architecture & Components

The CER shared directory is used to collect redirected error reports. Within this shared directory are three folders with specific NTFS permissions applied. These folders are Cabs, Counts, and Status. When an error reporting client is redirected to a CER shared directory, the client looks for these folders, and uses them to contain parts of the error report. Collectively, the three folders hold the complete error report which can be viewed and managed with the CER console. The console then writes the overall reported data to a CSV file in a folder called Processed at the root of the CER shared directory.

A CER shared directory can be local to the reporting machine, as long as the policy of the local machine uses a valid UNC or mapped drive to the local location. The error reporting client will successfully report to the CER shared directory.

If the error reporting client finds a policy key to redirect the report to a CER shared directory, its reporting behavior changes and will no longer use HTTP and HTTPS. Instead, the error reporting client will use RPC to create a folder structure based on the report parameters under the expected shared directory the error reporting client was redirected to through a UNC path. This means that the error report cannot pass through a traditional firewall unless a Virtual Network Channel (VNC) is used to create a network conduit between firewall routers. If the UNC path is unavailable, the error reporting client will fail silently to send the report.

## Mapping Corporate Error Reporting

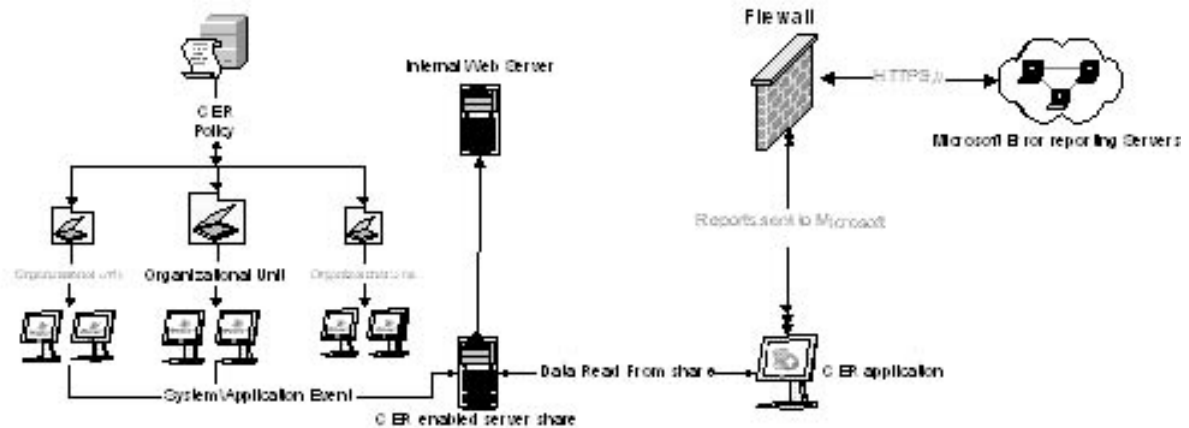
To effectively deploy and administrate CER, creating a map of the CER client "world" is helpful.

Since error reports cannot be redirected through a firewall, there may be a need to set up multiple CER servers. One server will be needed for each network segmented by a firewall. If deployment is based on geographic region, each region could be a unique zone as long as all the users in an identified zone have access to the CER server through UNC or drive mapping.

The drawing below identifies a single zone controlled by policies to enable CER: multiple machines with error reporting clients, a web server for the hosting of the redirected URLs, a single CER server, and an administrative machine running the CER console. Here the workflow of the report can be visualized.

As the network becomes more complex with firewall segmentation, the workflow shown in Figure 4 becomes duplicated for each zone.

## Escalation Workflow



- **Redirect individual Reports to an internal Web Page**
  - Redirect individual reports to an internal web site
  - Useful for Internal Development collection of additional information
  - Supports "Steps to Reproduce" for Premier escalation
    - Used in conjunction with Export feature of CER

Figure 4 – Corporate Error Reporting Data Flow

In this example we have users in a single zone configured to redirect error event data through the error reporting client to a CER shared directory. The CER shared directory has been configured to capture user feedback by redirecting the "thank you" dialog box of the error reporting client to an internal web server when the report is completed. The managed response will load in a web browser when the user reporting the crash clicks on the "More Information" link in the "thank you" dialog box. An administrator can then review the crash data collected in the CER shared directory using the CER console and report the appropriate selections of unreported errors to Microsoft after reviewing the error report information and the survey created to capture user input.

There are several components in designing CER:

- Determine which desktops and servers that will be targeted for collecting error reports.
- Ensure those servers will be able to use a Universal Naming Convention (UNC) path to reach the CER server.
- Determine how group policies will be applied to enable CER.

## Machines to be Configured for CER

CER is a new technology for Contoso that will allow them to track issues within the environment. Ideally all systems will be configured to use CER but this would not be practical to do immediately. Instead, Contoso should use a phased approach with deploying CER to ensure Contoso is realizing the value of the technology before deploying it to every system in the enterprise.

At this time Microsoft recommends the following phases for CER deployment:

- Phase I – Have CER configured and scaled to be deployed to all servers and desktops within the US and ADRoot domains before the rollout begins. This will give Contoso a large number of machines to sample from to determine if the information collected from CER is valuable while still being verily simple implementation because all machines would be able to reach a single CER server. All devices in these domains will have Operating Systems that will support CER and this will allow Contoso to baseline its environment. It will also provide Contoso with solid data points on the reliability of the new environment being deployed.
- Phase II – If Phase I is achieving the business value Contoso requires then Contoso should look to expand CER to the reset of the enterprise. This would include the DMZ (which would probably require a separate CER server because of the fire wall) and any other machines that are not part of the US or ADRoot domains.

The remainder of this document will focus on the design of CER for Phase I. The design for Phase II should be a separate task once it has been determined necessary by Contoso.

## CER Server Architecture

When designing the CER environment we must take into account the availability and scalability requirements to determine the proper server architecture. Listed below are the Contoso requirements:

- Since reporting errors is not a very common operation and machines only connect when an error occurs the server does not need to be scaled for 1,000s of concurrent connections.
- Contoso may want to keep a record of error reports for historical tracking purposes. Hence, the server should be sized to keep error reports for at least 2 years.
- If the service is not available clients will not notice any difference (to the end user it will appear they have sent the error report even though the service is down). If Contoso misses a few error reports the loss to Contoso will be minimal and CER is not a mission critical service for Contoso hence, the design does not call for a highly available solution.
- The CER design should be able to support approximately 20,000 CER enabled machines. This will account for all of the current machines Contoso has that would be involved with Phase I and allow for significant growth of the environment.
- Minimal overhead and maintenance.

# Contoso CER Design

Taking into account the requirements above Microsoft recommends Contoso implement a single server for CER of the US and ADRoot domains. The server should be located within the 982 datacenter to be in a central location for the enterprise.

A single CER server is only an option if all machines within the ADRoot and US Domains can map a UNC path to this server. This requires all the machines to use a common DNS environment and not have any firewalls to traverse in the network to get to the CER server. At this time it is believed both of these requires will be meet for all the machines to be monitored in Phase I.

The sizing of the server should be about the same for a department size file & print server. Most likely the CER service would not require a dedicated server provided the server it is installed on is not overloaded. Another option would be to use a server class machine near the end of its life cycle.

There are two components for CER, there is the shared directory and the CER console. Table 1 lists the recommendations for a dedicated central server containing the CER share and also running the CER console. The console can also be installed on desktop class machines but it will be easier for Contoso to just remotely connect to the CER for administration

Table 1 – CER Dedicated Server Sizing Recommendations

Type	Configuration
Server Name	TBD (for this document it is assumed the server name is CERSERVER)
OS	Windows 2003 Standard Edition
CPU	700 MHz or higher Pentium compatible CPU
Memory	1GB (mostly for the console)
Disk	104 GB available (RAID 5 Optional)
File System	NTFS
Network	100Mb minimum Internet Access

## Requirements Meet

- **Scalability** – The single server will be able to meet the anticipated error reports generated by 20,000 machines. If Contoso experiences a higher rate of error reports than anticipated (1 per week per machine) then additional CER servers or disk space on the single CER server may be required.
- **Historical Tracking** – Estimating that the average error report size is 50 KB and a user will generate 1 error report each week and Contoso wants to have 2 years worth of data the following calculation (50 Kb \* 104 \* 20,000 = 104,000,000,000 KB or 104 GB). The average report size of 50KB is a bit of guess and is based on the default report setting of medium-low and user information collected.

Optionally, Contoso could export the information collected from CER to a SQL database for more advanced and quicker query results. Since Contoso is just starting with CER it does not appear to be a requirement at this time but is an option in the future. This design does not address enabling this functionality.

Also, Contoso could elect to configure CER to delete the error information collected from the machines and only keep the error counts and any responses from Microsoft. This would significantly reduce the disk space requirements for CER.

- **Availability** – While the single CER server is a single point of failure, the non-critical role of CER within Contoso and the high reliability built into Windows 2003 server will meet the necessary availability requirements for CER at Contoso.
- **Maintenance** – With only a single server for CER the maintenance of the environment will be minimized and the administrative tasks for CER can be automated if desired.

## Group Policies

Group Policies for Error Reporting are very confusing at best. They are used to centrally manage the configuration for CER within the enterprise. There are several Group Policy templates for configuring CER and Error Reporting overall, for the OS, and Office. Since the goal of Phase 1 is to configure error reporting for all machines within the US and ADRoot domains the group policy changes should be implemented for Computers in the default domain group policy object for both domains.

To further confuse the situation the CER council can be used to over ride the policy settings. In general the GPO policy settings are for configuring error reporting when sending reports directly to Microsoft. While the settings in the CER are used when CER is enabled.

The next 3 sections detail the current CER group policy settings from three different template files and recommend policy settings. Included is the registry path so redundant settings can be identified. The recommended policy settings are based on the premise of only enabling CER and allowing users to have as much freedom for configuration as possible. If more policies are enforced it is possible exceptions will occur that would require additional policy settings to over ride the domain settings making the environment even more complicated. The main objective here is to only enable CER so it can be used when errors occur. Windows XP and Windows 2003 servers default configurations enable error reporting. Hence, most systems will report errors by default and will not need to be forced to by policy. If it is determined that a significant percentage of the population is not reporting errors Contoso can look to enforce it by policy.

# CER Group Policy Options

## CER Template

The CER template is called CER20.ADM and can be downloaded from [www.microsoft.com/resources/satech/cer/ToolboxMNU.asp](http://www.microsoft.com/resources/satech/cer/ToolboxMNU.asp). The CER template is located in the GPO tree at Administrative Templates/Corporate Error Reporting 2.0 and contains the following settings.

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Windows XP and higher Operating system including 'Group 1' Applications	Enable/Disable	Enable allows you to enter data for the other Options. Enabling this setting will configure CER reporting for the OS and Office 2003 because they use the same settings.	NA	Set to Enable
	Local error reporting file path (UNC or drive letter)	Sets path the CER Share	Software\Policies\Microsoft\PCHealth>Error Reporting\DW\DWFileTreeRoot	\\CERServer\CERFiles\$
	Name to replace 'Microsoft' with during reporting	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\PCHealth>Error Reporting\DW\DWReporteeName	Contoso  By setting to Contoso users will feel Contoso is requesting the data and will be more likely to submit.
Office XP and 'Group 2' Applications	Enable/Disable	Enable allows you to enter data for the other Options. This setting configures CER for the Office XP set of applications.		Set to Enable
	Local error reporting file path (UNC or drive letter)	Sets path the CER Share	Software\Policies\Microsoft\Office\10.0\Common\DWFileTreeRoot	\\CERServer\CERFiles\$
	Name to replace 'Microsoft' with during reporting	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\Office\10.0\Common\DWReporteeName	Contoso  By setting to Contoso users will feel Contoso is requesting the data and will be more likely to submit.

Table 2 – CER Group Policy Options

# CER Group Policy Options

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Group 3 Applications	Enable/Disable	Enable allows you to enter data for the other Options. This setting configures CER for the Windows Media Player. Sets path the CER Share		Set to Enable
	Local error reporting file path (UNC or drive letter)	Sets path the CER Share	Software\Policies\Microsoft\Media Player\Player\Exception Handling\DWFileTreeRoot	\\CERServer\CERFiles\$
	Name to replace 'Microsoft' with during reporting	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\Media Player\Player\ExceptionHandling\DWReporteeName	Contoso  By setting to Contoso users will feel Contoso is requesting the data and will be more likely to submit.
Group 4 Applications	Enable/Disable	Enable allows you to enter data for the other Options. This setting configures CER for misc applications. Could be for future use.		Set to Enable
	Local error reporting file path (UNC or drive letter)	Sets path the CER Share	Software\Policies\Microsoft\ErrorReporting\DW\DWFile TreeRoot	\\CERServer\CERFiles\$
	Name to replace 'Microsoft' with during reporting	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\ErrorReporting\DW\DWReportee Name	Contoso  By setting to Contoso users will feel Contoso is requesting the data and will be more likely to submit.

By setting to Contoso users will feel Contoso is requesting the data and will be more likely to submit.

# Windows Error Reporting

## Windows Error Reporting

Windows Error reporting settings determine how the user will be notified of errors and controls the options made available to the user. Windows Error Reporting settings are found in the system.adm template that comes with Windows 2003 servers. In the GPO tree they are located in the Administrative Template/System/Error Reporting folder.

The following options exist for configuring error reporting:

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Display Error Notification	Enable/Disable	Controls if the user is notified that an error has occurred. By default this is enabled for desktops and disabled for servers.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWAllowHeadless	Since we are trying to set a single domain policy and the default settings is what Contoso will want it is recommended to not configure this setting.
Report Errors	Enable/Disable	When this is enabled users are forced to report errors. They cannot change the setting in control panel.	Software\Policies\Microsoft\Media Player\Player\Exception Handling\DW\FileTreeRoot	Leave this setting as not configured. If it were enabled all machines would be forced to report errors and there maybe exceptions.
	Do not display links to any Microsoft provided 'more information' web sites.	If the error is a known issue, after the error is reported to Microsoft a web link maybe returned to the client for more information on resolving the error.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWNoExternalURL	Do not configure. Will be controlled by the CER Console. From testing it appears that this setting has no effect when CER is being used. The setting for CER will always be used. Go to the Microsoft response web site or go to the internal response website.
	Do not collect additional files.	After reporting the error, Microsoft may request additional information to diagnose the problem. This setting can block those requests	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWNoFileCollection	Do not set. Will be controlled by the CER Console.

Table 3 – Windows Error Reporting Group Policy Options

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
	Do not collect additional machine data.	After reporting the error, Microsoft may request additional information, such as registry settings, to diagnose the problem. This setting can block those requests.	Software\Policies\Microsoft\PCHealth\Error Reporting\DW\DWNoSecondLevelCollection	Do not set. Will be controlled by the CER Console.
	Force queue mode for application errors.	If the 'Force queue mode for application errors' checkbox is checked, then the user will not be offered the chance to report when an error occurs. Instead, the error will be placed in a queue directory, and the next admin to log onto the machine will be given the chance to report the error.	Software\Policies\Microsoft\PCHealth\Error Reporting\ForceQueueMode	This is a setting that can not be set by the CER console. The default setting on the machines are fine hence this should not be set.
	Corporate Upload file path:	Set the UNC path to the CER share	Software\Policies\Microsoft\PCHealth\Error Reporting\DW\DWFileTreeRoot	This is the same setting as the one set in the CER template for Group 1 applications. It will be set by that template and does not need to be set here. Leave not configured.
	Replace instances of the word 'Microsoft' with	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\PCHealth\Error Reporting\DW\DWReporteeName	This is the same setting as the one set in the CER template for Group 1 applications. It will be set by that template and does not need to be set here.

Table 3 – Windows Error Reporting Group Policy Options - *continued*

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Advanced Error Reporting Settings\Default application reporting settings	Enable/Disable	Used to configure which application errors are reported, MS apps, Windows, non-MS apps.		The defaults are to report errors for all applications. That is what is recommended hence this will not be set.
	Report all application errors or not	Choose to report errors from all applications or not	Software\Policies\Microsoft\PCHealth\ErrorReporting\AllOrNone	Report all application errors (default)
	Report all MS application errors	Choose to report all MS application errors or not.	Software\Policies\Microsoft\PCHealth\ErrorReporting\IncludeMicrosoftApps	Report all MS application errors (default)
	Report all Windows application errors	Choose to report all Windows errors or not	Software\Policies\Microsoft\PCHealth\ErrorReporting\IncludeWindowsApps	Report all Windows errors (default)
Advanced Error Reporting Settings>List of applications to always report errors for	Enter executable names of applications whose errors should always be reported	This policy is used to override the more broad one of not reporting for any applications	Software\Policies\Microsoft\PCHealth\ErrorReporting\InclusionList	Not required at this time. Leave not configured.
Advanced Error Reporting Settings>List of applications to never report errors for	Enter executable names of applications whose errors should never be reported	This policy is used to override the more broad one of reporting errors for any application	Software\Policies\Microsoft\PCHealth\ErrorReporting\ExclusionList	Not required at this time. Leave not configured.
Advanced Error Reporting Settings\Report Operating System errors	Enable/Disable	Used to force operating system errors to be reported. If not configured the setting in the control panel 'upload operating system errors' will be used.	Software\Policies\Microsoft\PCHealth\ErrorReporting\IncludeKernelFaults	Default settings are fine (enabled). Leave not configured.

Table 3 – Windows Error Reporting Group Policy Options - *continued*

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Advanced Error Reporting Settings\ Report unplanned shutdown events	Enable/Disable	This setting controls whether or not unplanned shutdown events can be reported when error reporting is enabled.	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\ IncludeShutdownErrs	Default settings are fine (enabled). Leave not configured.

Table 3 – Windows Error Reporting Group Policy Options - *continued*

The system error reporting template had one fault in that it would be nice to be able to force users to send error reports but not keep that hidden from them. Unfortunately, this is not possible because if the error report dialog is exposed to the user they can choose not to send the error report. Also, in order to set several of the settings error reporting must be enabled which we don't necessarily want to do. Fortunately, the CER template allows for setting the proper policies (UNC path and name replacement) that this is not an issue.

**Note:** Since the CER and Window templates set policies to the same keys the Group Policy Management Console Resultant Set of Policies does not accurately represent which templates are making the policy settings.

## Office 2003 Policies

Office 2003 has its own ADM file called AER\_1033.ADM and is located on the Office 2003 CD. When imported its settings are located at Administrative Templates/Application Error Reporting in the Group Policy editor. The settings configured by these policies are stored in the same place in the registry that the Windows ones are. Hence, confusion can occur if these are not set in sync with each other. There are several more options for Office error reporting because it uses a different application for error reporting (DW20.EXE) than Windows (DWWIN.EXE). The following lists the settings for office error reporting.

Group Policy Name	Options	Description	Registry Path	Recommended Setting
General Reporting\ Disable Error Reporting	Enable/Disable	Enable so the user will not send any error reports. Otherwise the user will be prompted to send an error report.	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\DW\ DWNeverUpload	Leave default of not configured.
General Reporting\ Do not Upload user documents	Enable/Disable	After reporting the error, Microsoft may request additional information, in the case with office documents, to diagnose the problem. This setting can block those	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\DW\ DWNOfFileCollection	Do not set. Will be controlled by the CER Console

Table 4 – Office Group Policy Options

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
General Reporting\ Do not upload any additional data	Enable/Disable	After reporting the error, Microsoft may request additional information, such as registry settings, to diagnose the problem. This setting can block those request	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\DW\ DWNNoSecondLevel Collection	Do not set. Will be controlled by the CER Console.
General Reporting\ Do not display Microsoft web page	Enable/Disable	If the error is a known issue, after the error is reported to Microsoft a web link maybe returned to the client for more information on resolving the error.	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\DW\ DWNNoExternalURL	Do not configure. Will be controlled by the CER Console. From testing it appears that this setting has no effect when CER is being used. The setting for CER will always be used. Go to the Microsoft response web site or go to the internal response website.
Corporate Error Reporting\ Local Error reporting file path	Enable/Local error reporting file path (UNC or drive letter)	Set the UNC path to the CER share	Software\Policies\ Microsoft\PCHealth\ ErrorReporting\DW\ DWFileTreeRoot	This is the same setting as the one set in the CER template for Group 1 applications. It will be set by that template and does not need to be set here. Leave not configured.
Corporate Error Reporting\ Log error report details	Enable/Disable	If you ENABLE this policy, error details including username and machine name are written to the crash.log file at the root of your corporate error reporting file path.	Software\Policies\ Microsoft\PCHealth\ Error Reporting\DW\ DWTracking	Do not set. Will be controlled by the CER Console.

Table 4 – Office Group Policy Options - continued

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Corporate Error Reporting\Hide Don't Send button	Enable/Disable	If you ENABLE this policy the user sees only one button on the error reporting dialog: Send Error Report. Otherwise they will have a Do Not send button as well.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWAlwaysReport	Set to Enabled. This is a new option that Windows error reporting does not have yet. At this time we recommend to enable it so users will always report errors. If this becomes an issue it can be disabled.
Corporate Error Reporting\Replace Microsoft with your company name	Replace instances of the word 'Microsoft' with	Replace the Microsoft name with another in the error report. It is used in the sentence to describe who is requesting the report.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWReporteeName	This is the same setting as the one set in the CER template for Group 1 applications. It will be set by that template and does not need to be set here.
Corporate Error Reporting\URL to launch after reporting	Enter URL path	If you ENABLE this policy, each user who sends a report will see a final dialog with a link to the URL you specify. If you DISABLE or DO NOT CONFIGURE this policy the user may be sent to a Microsoft web page after reporting.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWURLLaunch	Do not configure. Not required for this environment.

Table 4 – Office Group Policy Options - *continued*

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Corporate Error Reporting\URL to explain why user should report	Enter URL path	If you ENABLE this policy a link is displayed on the error reporting dialog with the text 'Why should I report?' Clicking the link launches the URL you specify in the policy. This policy allows you to create your own web page which explains why users should send error reports.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWExplainerURL	Do not configure. Not required for this environment.
Queued Reporting\Bypass queue and send all reports	Enable/Disable	This policy disables error report queuing. If you ENABLE this policy no reports are queued. Error reports are always sent at the time the error occurs. If the machine is offline and the report cannot be sent, the report is deleted.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWBypassQueue	Leave not configured. The default is to queue reports.
Queued Reporting\Send all queued reports silently	Enable/Disable	This policy allows you to send all queued reports without prompting the user. If you ENABLE this policy the queued dialog is not displayed. When a user logs on all queued reports are silently uploaded. If you DISABLE or DO NOT CONFIGURE this policy the user is prompted to either send or not send the reports.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWAllQueuesHeadless	Leave this setting Not configured. We want the user to know they are sending the errors, just we want them to always send them.

Table 4 – Office Group Policy Options - *continued*

# Windows Error Reporting

Group Policy Name	Options	Description	Registry Path	Recommended Setting
Queued Reporting\Maximum number of queued reports	Number of reports to queue 0 -1000 Default 50	This policy sets the maximum number of error reports stored in each queue. If you DISABLE or DO NOT CONFIGURE this policy the default maximum of 50 is used.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWMaxQueueSize	Leave this setting Not configured. 50 should be plenty since Contoso does not have users disconnected for long periods of time.
Queued Reporting\Time between queued reporting requests	Number of minutes before reminded to send in reports 20 – 100,000 Default 3 days	This policy controls how often the user may be prompted to send queued reports. If you DISABLE or DO NOT CONFIGURE this policy the default of 4320 minutes (3 days) is used.	Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\DWQueuePesterInterval	Recommend to leave this setting not configured. It maybe a bit confusing to users but 3 days should not be that annoying to them. Hopefully the Contoso name in the dialog will encourage them to send in the reports.

Table 4 – Office Group Policy Options - *continued*

The Office template has some new settings and functionality that will be useful above what windows error reporting can do now. It will be able to queue errors while the users are offline and it allows Contoso to force users to send in error reports while they are still notified it is happening.

## CER Design and Settings

Several error reporting settings can be configured by the CER console. There are four levels that can be used to configure what information can be collect from errors that will be reported back to Microsoft. The recommended setting is the default of only sending program and system reports (Medium-Low). Files, registry settings, and system information will not be sent to Microsoft. If Contoso is running into a problem that requires this information it can be enabled to collect that information but it will not be collected by default. User name, Computer, and date of error should be collected to help Contoso classify were the errors are being reported from.

After reports have been submitted by the client it is up to the CER operator to submit them to Microsoft. The operator can review the reports before submitting them or automatically have all reports submitted. It is recommended to have them automatically submitted. This can be accomplished by configuring a scheduled process to run a CER command line utility called CERUTILS.EXE.

By default CER will continue to collect the error reports generated by the clients in .cab files until 5 have been collected of the same error. This is a configurable setting in the CER console. At this time it would be recommended to leave the default until Contoso sees how many reports are being generated in their environment. Once 5 errors of the same type have occurred .cab files will not be collected and CER will only send the number of times the error has occurred to Microsoft. The CER console can also be configured to delete the .cab files after Microsoft has a resolution for the error. It would be recommended to implement this configuration.

## The Console

The console reads the CER share into memory and then is able to perform operations on the data. If there is a lot of data collected the console may take a long time to open while it reads in all the data. There are a couple of options to get around this. If the operator only wants to view the data the CER console can be opened in read only mode. The second option is to export the information it has collected into an XML file and then use a separate tool to work with the data.

## Responses

When an error is submitted to Microsoft, if there are any responses to the issue, a URL will be sent to CER to link to the information. Every time the error is submitted CER will look for an updated response. For errors that have not been resolved but the operator would like to check if a response has been issued the operator can go into the CER console and for each individual error check if there are any updated responses.

Optionally, CER responses can be redirected to a different internal URL. At this time this functionality is not required.

## Submitting Errors

Submitting errors to Microsoft can be done through the console or automated through a command line application called CERUTILS.EXE. It is recommended to create a daily automated task that will run the utility using the following command line:

```
"C:\Program Files\Corporate Error Reporting 2.0\cerutils.exe" c:\CERFiles$ /r /v /l:"C:\Program Files\Corporate Error Reporting 2.0\cerlog.txt"
```

**Note:** This command will fail with an Error: Access Denied if it is run while the CER Console is open in write mode.  
Backup and Recovery

CER stores its information in the CER share directory and any custom view settings that are created in the CER console are stored in the registry. Hence, a full backup of the CER server consists of a file backup of the CER share directory, the system drive, and the servers system state should be backed up. Recovery of the information would be to reinstall the CER console, copy back the share and recover the system state information which would include the registry settings. The server name should stay the same in a disaster recovery situation.

## Monitoring CER

At this time the only way to monitor CER is through the console or the log file that is generated by the CERUTILS program. Hence it is recommend to open up and review the console and the log file at least once a week to ensure CER is functioning properly. Optionally, a monitoring script could be run to review the log file for any errors and generate and event in the event log to be picked up by MOM.

© 2003 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft is a registered trademark of Microsoft in the United States and/or other countries.  
Fictitious Disclaimer:

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, places, or events is intended or should be inferred.