Application Reporting Tool

© 2017 PTC Inc. All Rights Reserved.

Table of Contents

Application Reporting Tool **1**
Table of Contents **2**
Application Reporting Tool 3
Overview 3
Accessing the Application Reporting Tool 4
Collecting Event Logs **5**
Creating On-Demand Process Memory Dumps 6
Enabling Process Memory Dumps on Crash 7
Excluding Server Application Data Content 8
Information in an Application Report 9
Generating an Application Report **11**
Index **17**

Application Reporting Tool

Help version 1.008

CONTENTS

Overview
What is the Application Reporting Tool?

Accessing the Application Reporting Tool
Where can I find the Application Reporting Tool on a system?

Collecting Event Logs
What are event logs and which ones do I need to collect?

Creating On-Demand Process Memory Dumps
How to choose processes and why memory dumps may be necessary?

Enabling Process Memory Dumps on Crash
How to automatically capture memory dumps when a product crashes?

Excluding Server Application Data Content
Can I exclude non-relevant historical data from the archive?

Information Included in an Application Report
What is sent to Technical Support with an Application Report archive?

Generating an Application Report
How do I create a report using the Application Reporting Tool?

Overview

The Application Reporting Tool is a technical support utility that automates the process of gathering and archiving data for troubleshooting or identifying system issues. With the exception of identifying hardware and gathering general operating system information, the Application Reporting Tool only collects file and registry information that directly pertains to related applications. After report generation, the entire report archive is stored in a user-specified location and may be reviewed before sending to technical support.

*For more information regarding what data is collected as part of an Application Report archive, see **Information Included in an Application Report**.*

See Also:
Generating an Application Report
Accessing the Application Report

Accessing the Application Reporting Tool

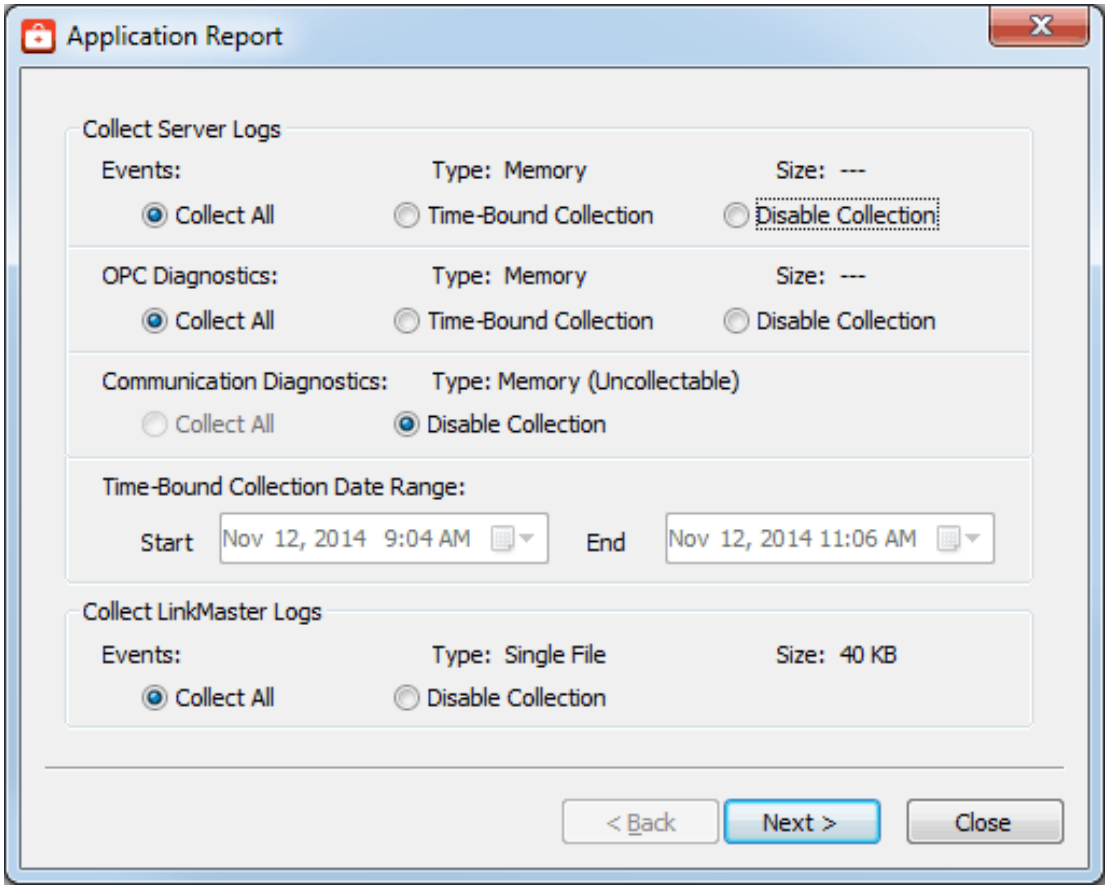
To run the Application Reporting Tool:

1. To start, click **Start** | **All Programs**.
2. Select **<Vendor>** | **<Product>** | **Utilities.**
3. Select **Application Report**.

See Also:
Generating an Application Report

Collecting Event Logs

An application-specific, user-configurable event logging service is included in most products. The technical support team may request the logs generated by the service to better understand the error and any relevant diagnostic information provided by the product.



The Event Log collection interface is divided into two sections, allowing collection of server logs and LinkMaster logs. If either product is not installed, the section is disabled.

Server Logs

Three types of server logs are collectable:

- **Event Logs** record noteworthy occurrences at the server level.
- **OPC Diagnostic Logs** record OPC events occurring between an OPC client and the server.
- **Communication Diagnostic Logs** record messages and events occurring between a driver and a device.

As part of each log, the following details are provided:

- **Type**: One of three values (file, directory, memory) represents the server's configured Persistence Mode for each of the available log types.
- **Size**: The estimated size of the logs being saved.

Each log may be collected using one of the following methods:

- **Collect All:** Collects every log record for the selected log type. If the log is configured as a File or Directory, this information is copied directly to the output archive. If the log is configured as Memory, a file is generated based on the stored records.

  Note: The Collect All option does not copy communication diagnostic logs from memory.
- **Time-Bound Collection:** Using the provided Start and End date pickers, a subset of records may be specified for collection to the archive. This feature is available for all log Types and updates the Size field based on the number of records selected.

  Note: The Time-Bound function is only available for Event and OPC Diagnostic logs.
- **Disable Collection:** Log records of this type will not be collected as part of the archive.

LinkMaster Logs

- **Event Logs** record noteworthy occurrences at the server level.

As part of each log, the following details are provided:

- **Type**: One of three values (file, directory, memory) represents the server's configured Persistence Mode for each of the available log types.
- **Size**: The estimated size of the logs being saved.

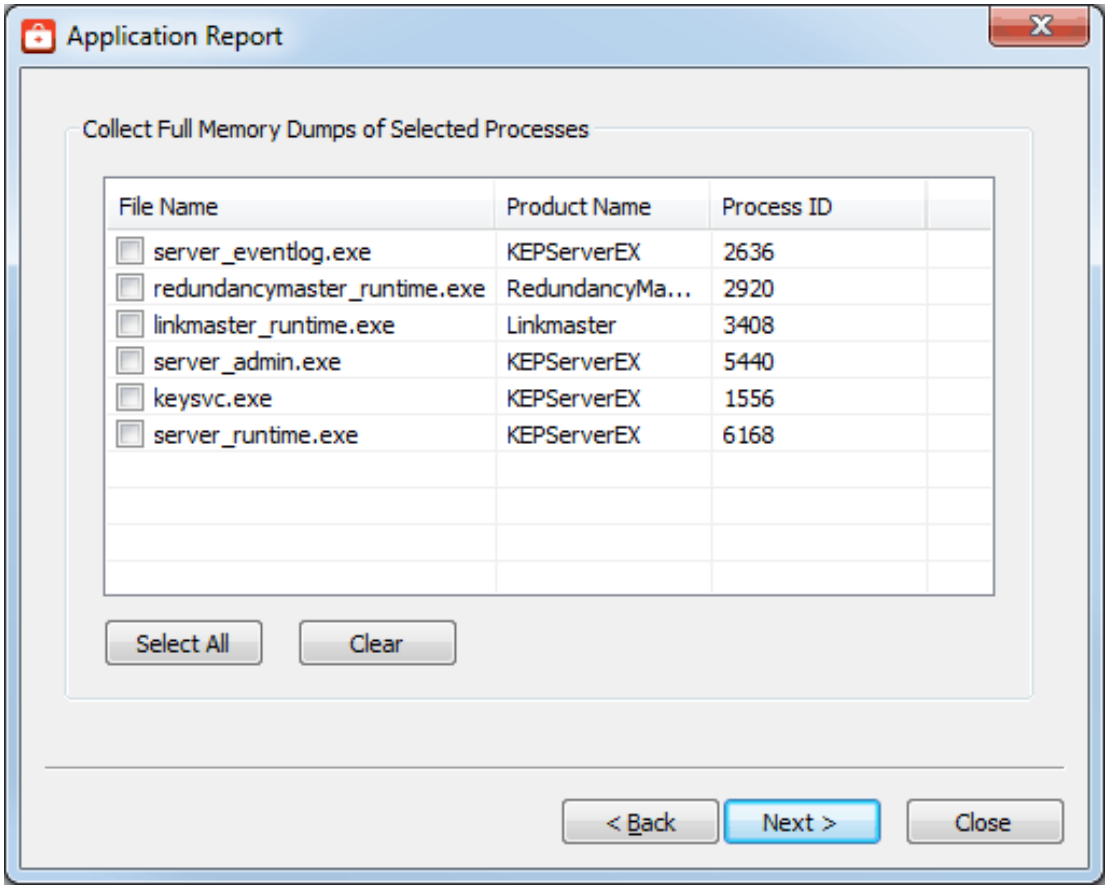
Each log may be collected using one of the following methods:

- **Collect All**: Collects every log record for the LinkMaster log. If the log is configured as a File or Directory, this information is copied directly to the output archive. If the log is configured as Memory, this option is disabled.
- **Disable Collection**: Log records of this type will not be collected as part of the archive.

Creating On-Demand Process Memory Dumps

A process memory dump creates a virtual snapshot of any running processes. These snapshots allow technical support to examine the state of a running process and identify the cause of issues. To generate a process dump for a running processes, check the corresponding box.

In general, process memory dumps are most useful when specific programs are entering an unresponsive or excessively slow state. In this situation, a process memory dump provides the support team with a "snapshot" representing the current state of the process.



The process list contains the following fields for every detected process currently running:

- **File Name**: This refers to the executable name of a process. Although a single product, many applications are actually comprised of multiple executables, each of which is individually selectable.
- **Product Name**: The product name allows a user to distinguish between two identically named executables. For example, several products may include a program named "runtime.exe", but a dump may only be required for single product's "runtime.exe".
- **Process ID**: A unique identifier used by the operating system to identify a process.

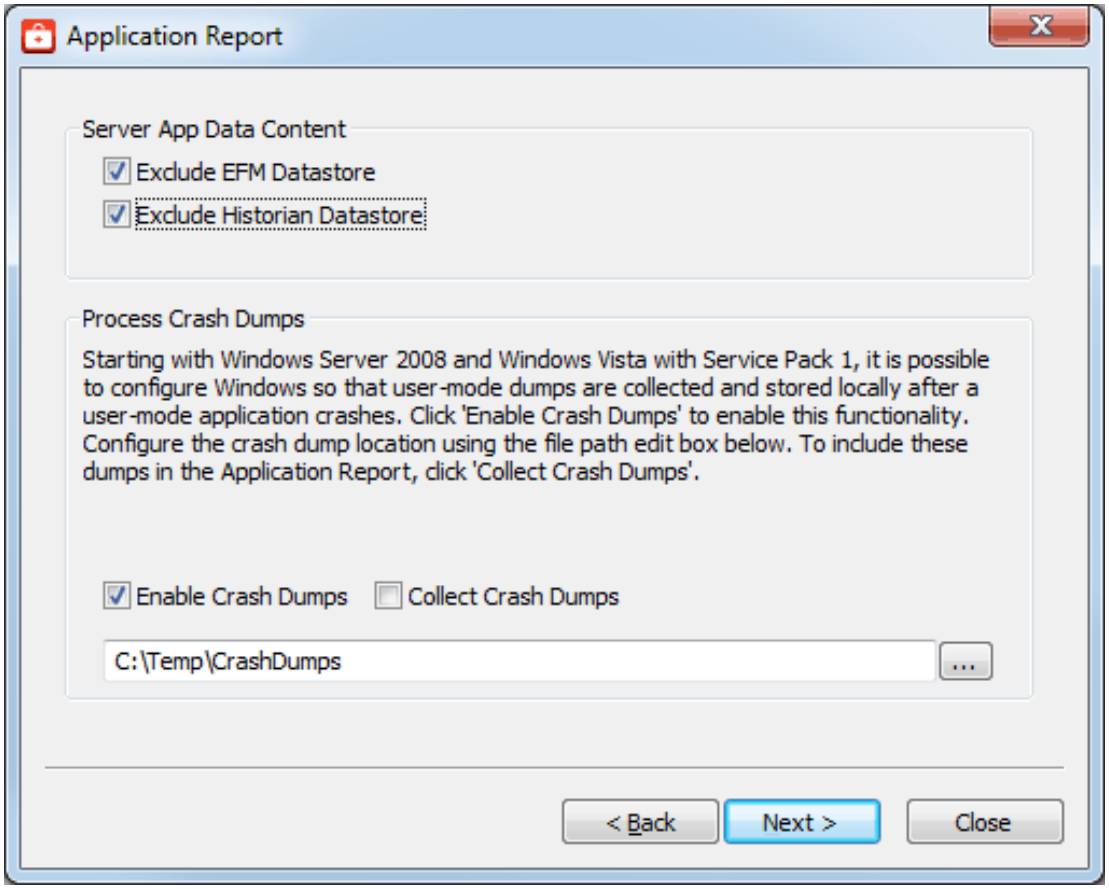
Warning:
Process memory dumps should only be generated if necessary for technical support. Each process memory dump increases the size of the final Application Report archive and lengthens the output generation time.

Note:
Process memory dumps require administrative privileges. If the system or authorized user does not have adequate privileges, the utility requests temporary elevation of rights to administrator level.

Enabling Process Memory Dumps on Crash

Windows Vista SP1/Server 2008 releases and higher provide the ability to generate process memory dumps automatically when a process crashes, providing valuable insight into the conditions leading to the crash. The Application Reporting Tool configures the system to collect ONLY those dumps related to this particular vendor software.

In general, process memory dumps are most useful when specific programs are entering an unresponsive or excessively slow state. In this situation, a process memory dump provides the support team with a "snapshot" representing the current state of the process.



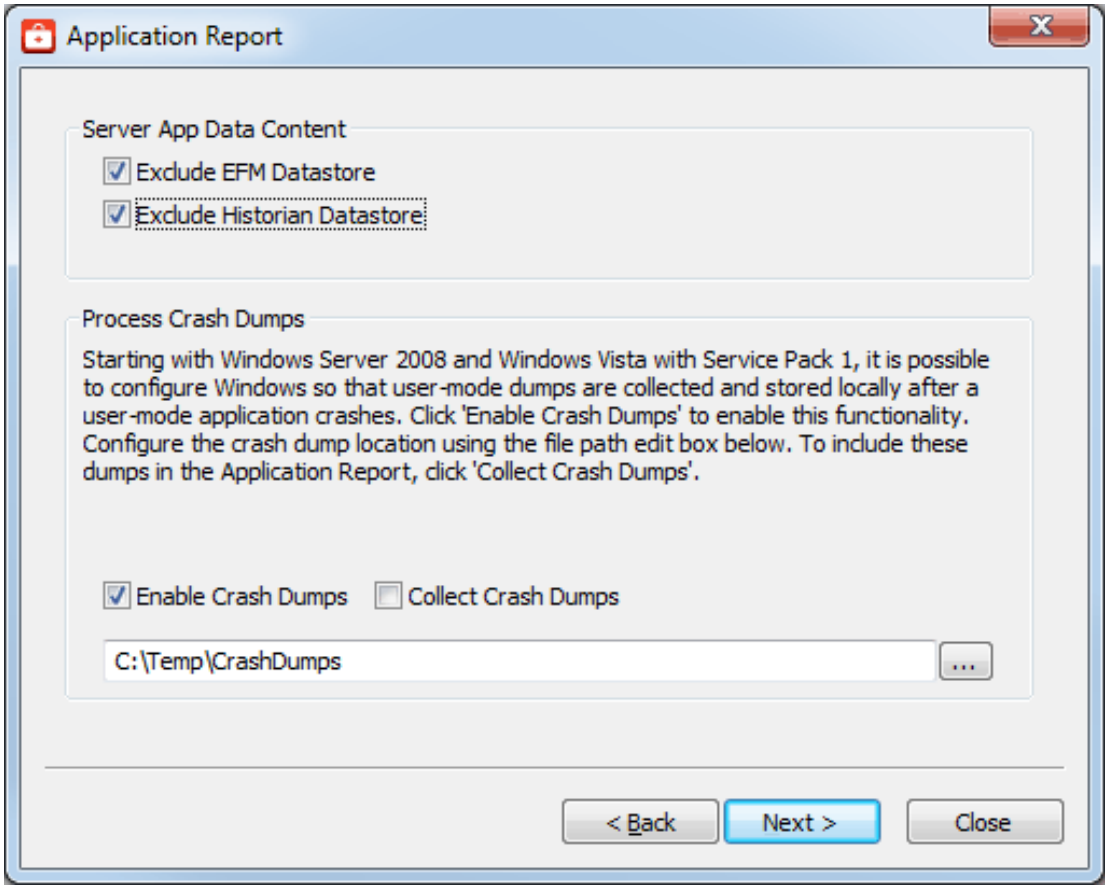
Within the Crash Dump Collection section, the following options are provided:

- **Enable Crash Dumps**: Sets / disables a system-wide registry key, notifying Windows to generate a process memory dump any time a process crashes. Within the text field, a default path of C:\Temp\CrashDumps is provided and may be changed to any location at any time.
- **Collect Crash Dumps**: Process memory dumps related to vendor products that are stored in the selected path are collected as part of the Application Report archive. Within the archive, process memory dumps appear in the /CrashDumps folder of related products.

Note:
Collecting process memory dumps require administrative privileges and Windows Vista SP1/Server 2008 or newer operating system. If the system or authorized user does not have adequate privileges, the utility requests temporary elevation of rights to administrator level.

Excluding Server Application Data Content

Many Windows applications leverage the Application Data directory as an area for storage of temporary or long-term files that do not require direct user interaction. The Application Reporting Tool collects this directory to provide technical support staff with a better understanding of the state of applications on the system. Plug-ins installed as part of the server product also use this space for storage. This information is not always needed by technical support and can be excluded to reduce size and time when unnecessary.



Within the Exclude Server App Data Content section, the following options are provided:

- **EFM Datastore**: Server's EFM Suite stores its historical EFM (Electronic Flow Measurement) data within the Application Data directory. Selecting this option prevents collection of EFM content when collecting the Application Data directory. If no EFM content exists within Application Data, this selection has no effect.
- **Historian Datastore**: The server's local "historian" plug-in may store its database in any location, including the Application Data directory. Selecting this option prevents collection of historian datastore files when collecting the Application Data directory. If no historian datastore exists within Application Data, this selection has no effect.

Information in an Application Report

As part of the Application Reporting Tool, many different pieces of information are included. Below is a comprehensive list of information and files collected as part of archive generation.

System

- Information Compiled:
  - Hardware Details
  - Operating System Details
  - Active and Disconnected Network Interfaces
  - Installed .NET Frameworks
  - DCOM State and Permissions

        - OPC Enum Service Details
        - Registered OPC Servers (as seen by OPC Enum)
- Files Copied:
    - bootstrap.log
        - Error log generated during the failure of any Windows installer application
    - <AppData>\Vendor\Common
        - Vendor Hardware Keys
    - <AppData>\FLEXnet
        - Vendor Licensing
    - Windows System Event Log File
    - Windows Application Event Log File

General Product

- Information Compiled:
    - Installed Components
        - A list of .exe and .dll files stored in the install directory of each product
    - Xi Wrapper (Server Only)
    - Product Registry Entries
        - HKEY_CURRENT_USER\SOFTWARE\<Vendor>\<Product>\V5
        - HKEY_LOCAL_MACHINE\SOFTWARE\<Vendor>\<Product>\V5
        - HKEY_CLASSES_ROOT\AppID\<Product_CLSID>
        - HKEY_CLASSES_ROOT\CLSID\<Product_CLSID>
    - Product DCOM Configuration and Permissions
- Files Copied:
    - Trusted Storage Diagnostics
        - License details file generated by a product's "activation_client.exe"
    - Install Log
        - The log file generated by each product during installation and modification
    - (Optional) Event Log Files
        - Includes Event, OPC Diagnostics, and Communication Diagnostics logs. *See "Collecting Event Logs" on page 5*
    - Application Data
        - Temporary and long-term storage for application specific files
        - Log files from the Program Files directory (RedundancyMaster Only)
    - Xi Wrapper (Server Only)
        - Install information and executable configuration files (only if .NET framework version 3.5 is installed)

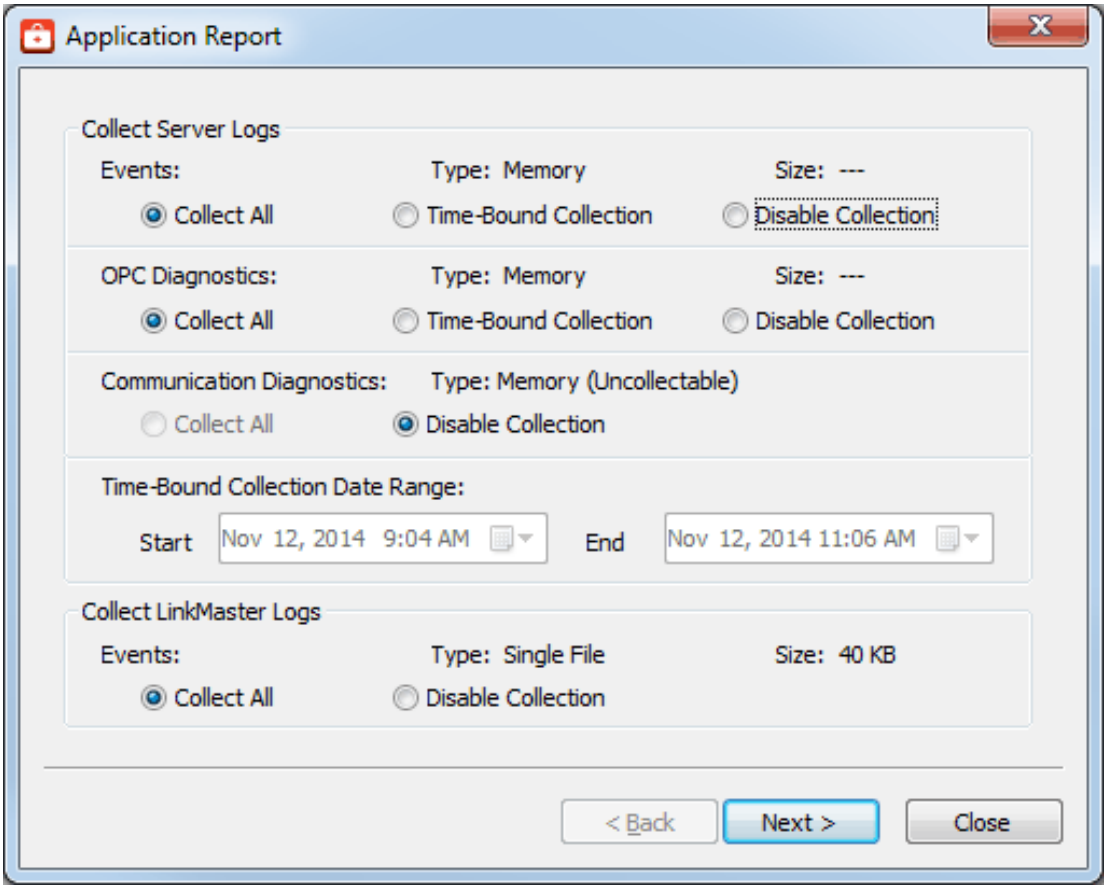
Other

- (Optional) On-Demand Process Memory Dumps
    - *See **Creating On-Demand Process Memory Dumps***
- (Optional) Process Memory Crash Dumps
    - *See **Enabling Process Memory Dumps on Crash***

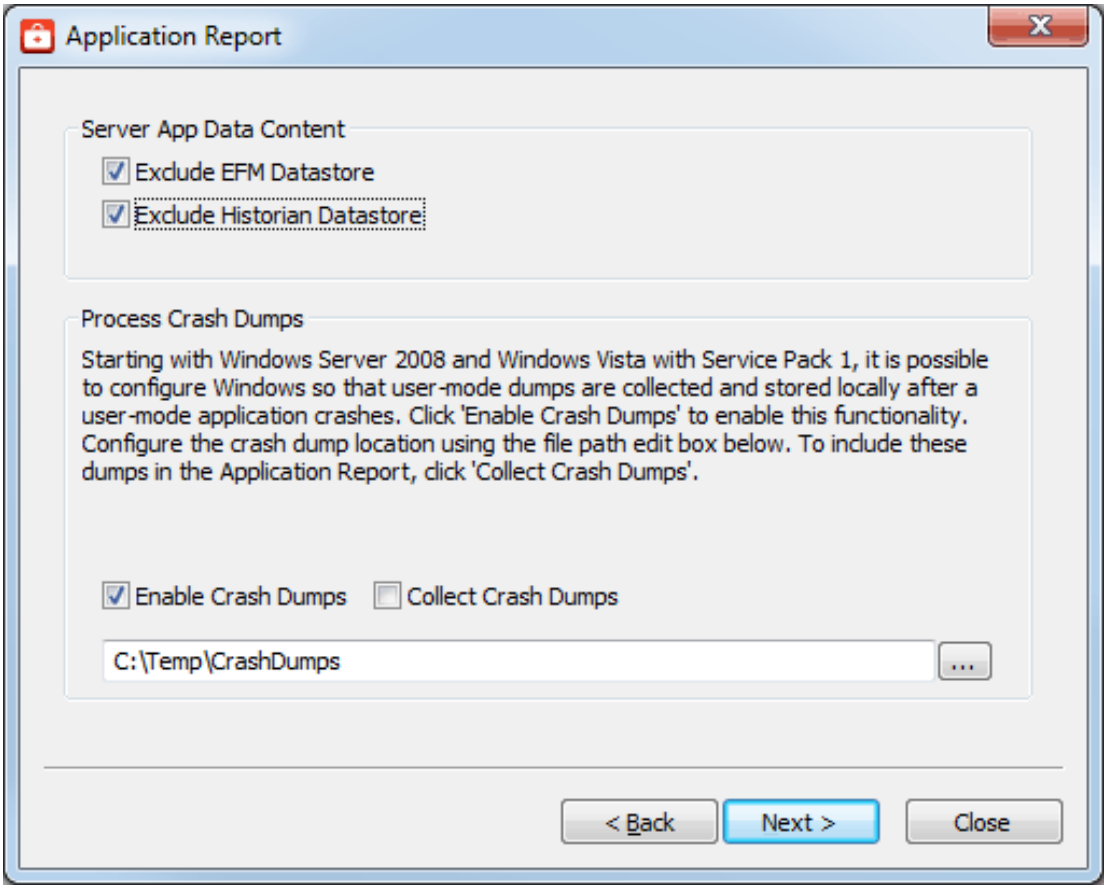
Generating an Application Report

To run the Application Reporting Tool:

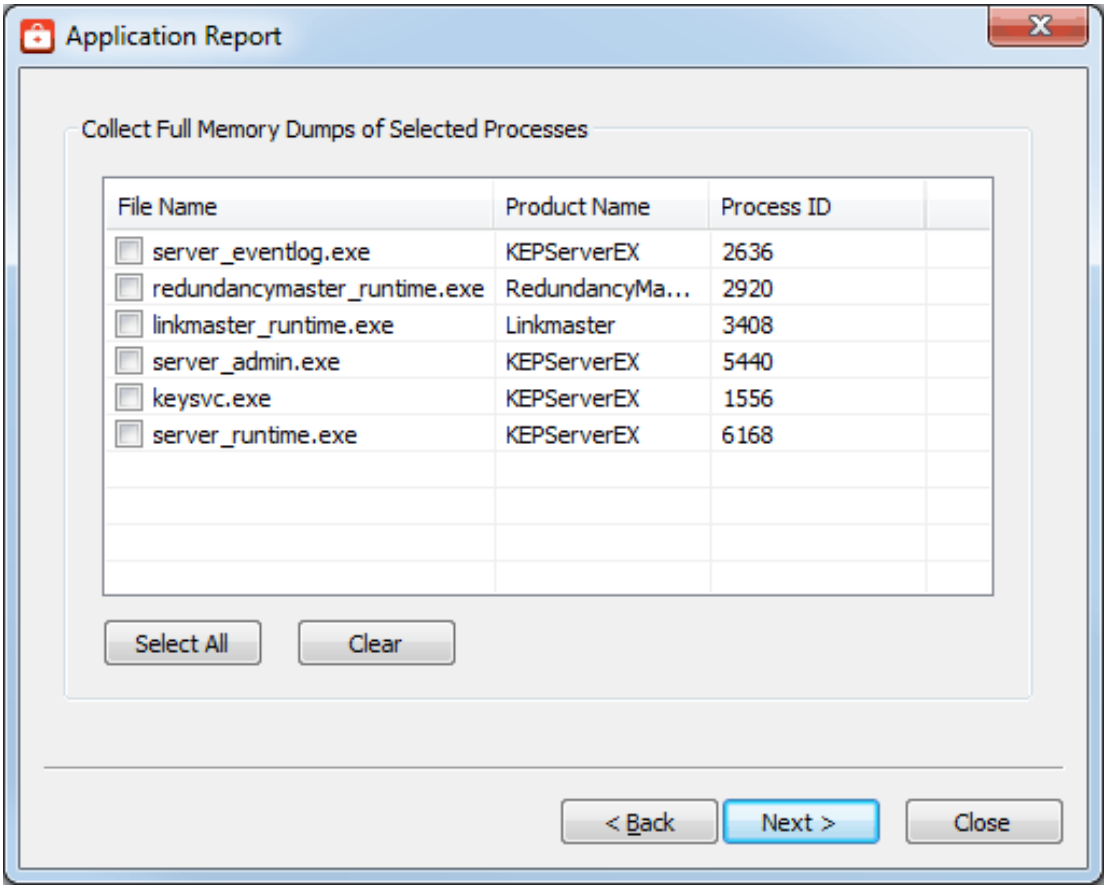
1. To start, click **Start** | **All Programs**.
2. Select **<Vendor>** | **<Product>** | **Utilities.**
3. Select **Application Report**.
4. Choose any event logs for collection, as described in **Collecting Event Logs**.



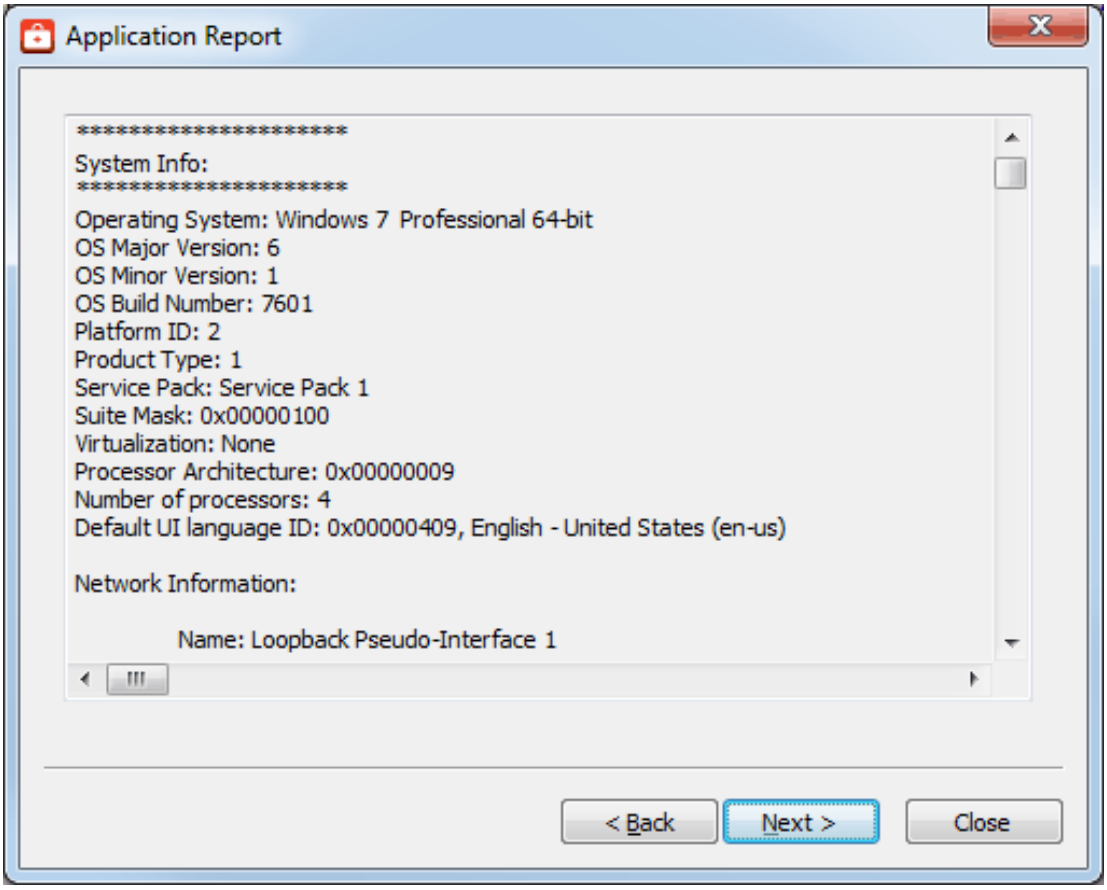
5. Click **Next**.
6. Select content to exclude content from collection, as described in **Excluding Server Application Data**.
7. Select process crash dump settings, as described in **Enabling Process Memory Dumps on Crash**.



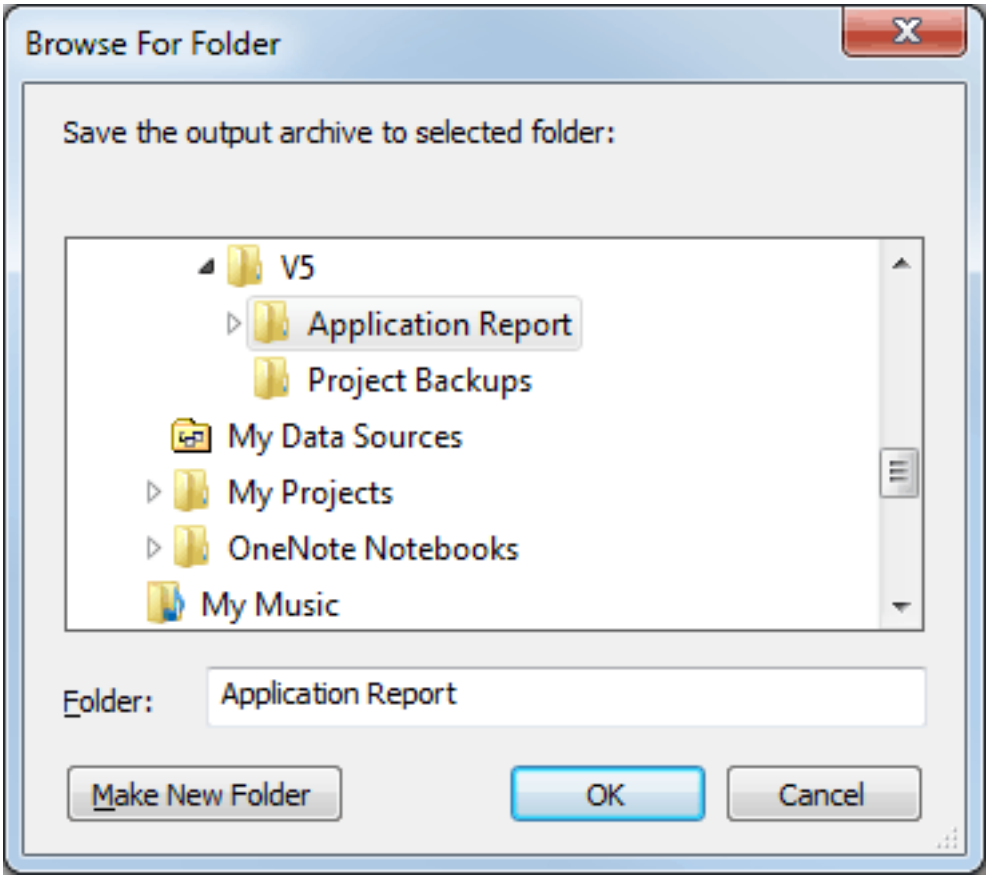
8. Select the processes for which to generate on-demand process memory dumps. *For more information on process memory dumping, including when a memory dump is necessary, refer to* ***Creating On Demand Process Memory Dumps***.



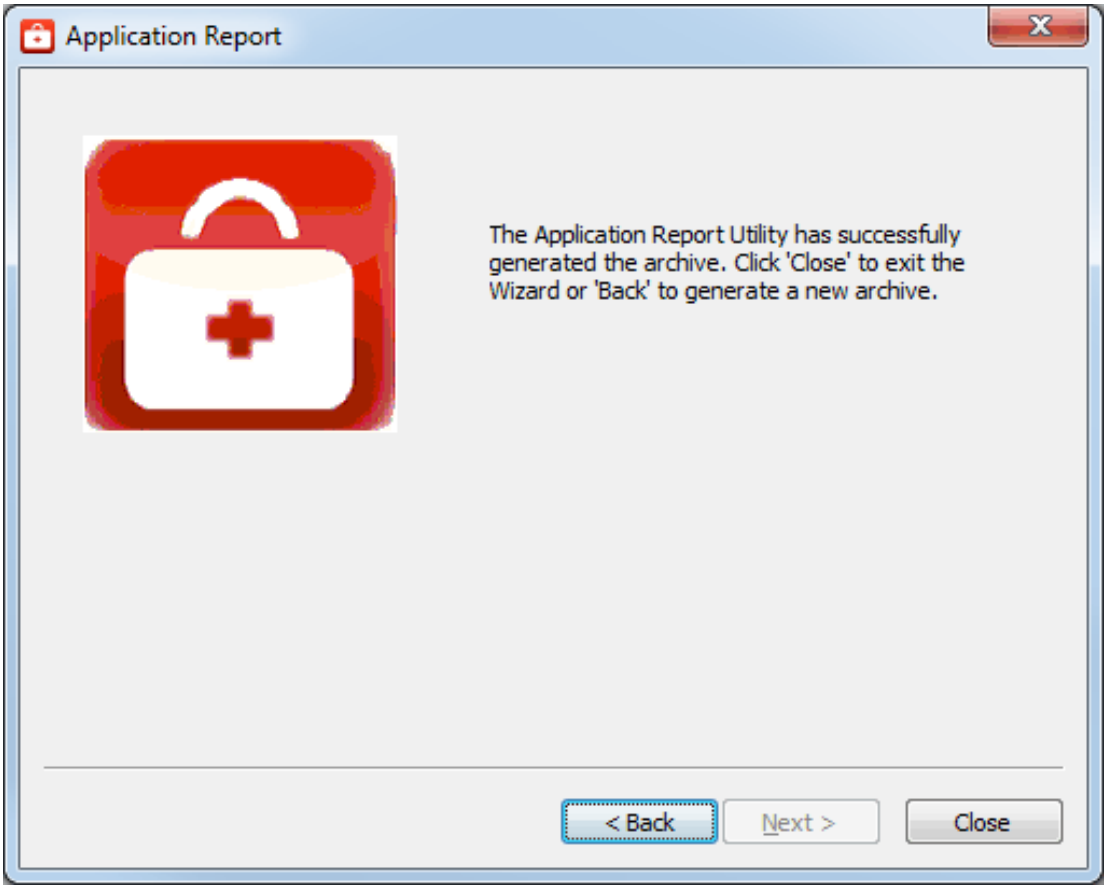
9. Click **Next**.
10. The Application Reporting Tool generates a preview of the collected data for review. For details regarding the information collected, see **Information Included in an Application Report**. Verify the settings and click **Next** (or click **Back** to make changes before generating).



11. Browse to and select the folder in which to save the report archive.



12. Click **OK**.
13. The Application Reporting Tool collects the files, generates the archive, and displays a notification message on completion.



14. Click **Close**.
15. Browse to the archive in the output folder. Output archives are compressed using the ZIP format and follow the naming convention (UTC Time):

    ARU_YEAR-MONTH-DAY_HOUR-MIN-SEC.zip
16. Send the file to Technical Support or extract the archive and browse the directory for the files of interest.

See Also:
Accessing the Application Report

Index

A

Accessing the Application Report 4
Application Data 8

B

bootstrap.log 10

C

Collect Crash Dumps 8
Collecting Event Logs 5
Collection 6
Communication Diagnostic Log 5
Creating On-Demand Process Memory Dumps 6

D

DCOM State 9
Diagnostics 10

E

EFM Datastore 9
Electronic Flow Measurement 9
Enable Crash Dumps 8
Enabling Process Memory Dumps on Crash 7
Event Log 5
Excluding Server Application Data Content 8

G

Generating an Application Report 11

H

Help Contents 3
Historian Datastore 9

I

Information in an Application Report 9

L

LinkMaster 6
Log records 6

N

Network Interfaces 9

O

OPC Diagnostic Logs 5
OPC Enum 10
Output archives 16
Overview 3

P

Process ID 7
Process memory dump 7
Product Name 7

S

Server Log 5
Snapshot 7

T

Time-Bound Collection 6

X

Xi Wrapper 10

Z

ZIP format 16