Dell System E-Support Tool (DSET) Version 3.6 User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2014 - 05

Rev. A00

Contents

1 Introduction....................5

What's New In This Release.................... 5

Support Matrix....................5

Supported PowerEdge Systems....................5

Supported PowerEdge Cloud Systems....................7

Supported PowerVault Systems.................... 8

Supported Operating Systems.................... 8

Other Documents You May Need.................... 9

Accessing Documents From Dell Support Site....................10

Contacting Dell.................... 10

2 Using Dell System E-Support Tool (DSET) Application....................11

Generating Basic And Advanced Report....................11

Report Filtering....................12

CLI Options....................12

On Systems Running Windows.................... 12

On Systems Running Linux....................13

List Of CLI Options.................... 13

Usage Examples....................17

Viewing DSET Report....................18

3 Error Codes....................19

DSET Application Error Codes.................... 19

1

Introduction

Dell System E-Support Tool (DSET) is a utility that collects configuration and log data for various chassis hardware, storage, software, and operating system components of a Dell PowerEdge server and consolidates the data into a **.zip** file.

What's New In This Release

- Support for Dell PowerEdge Express Flash PCIe SSDs on the following operating systems:
  - Microsoft Windows Server 2012. Processor: x64/EM64T
  - Microsoft Windows Server 2008 R2 or later, including Hyper-V virtualization. Processor: x64/EM64T
  - Red Hat Enterprise Linux 6.1 64 bit or later. Processor: x64/EM64T
  - SUSE Linux Enterprise Server 11 SP2 64 bit or later. Processor: x64/EM64T
  - VMware ESXi 5.1 or later
- Support for the following new hardware platforms: PowerEdge R220 and R920
- Support for the following new operating systems:
  - Microsoft Windows 2012 R2
  - Windows 2012 R2 Hyper-V
  - RHEL 6.5
  - SLES 11 SP3
  - Cent OS 6.3
  - Citrix Xen Server 6.2
  - Oracle Enterprise Linux 6.4
  - Oracle Virtual Machine 3.2
  - ESXi 5.0 U3
  - ESXi 5.1 U2
  - ESXi 5.5
- Support for 9th generation PowerEdge RAID H730P controller
- Support for iDRAC firmware version 1.55.55
- Support for checking the communication between the target server and provider

Support Matrix

Supported PowerEdge Systems

This section lists the supported PowerEdge Systems.

Table 1. Supported PowerEdge Systems

Model	Generation	Description	Supported
6950	9G	Rack	Yes
2970	9G	Rack	Yes
2950	9G	Rack	Yes
2900	9G	Rack	Yes
1950	9G	Rack	Yes
1900	9G	Rack	Yes
1955	9G	Modular	Yes
R905	10G	Rack	Yes
R900	10G	Rack	Yes
R805	10G	Rack	Yes
T605	10G	Tower	Yes
T300	10G	Tower	Yes
R300	10G	Rack	Yes
R200	10G	Rack	Yes
T105	10G	Tower	Yes
T100	10G	Tower	Yes
M600	10G	Modular	Yes
M605	10G	Modular	Yes
M805	10G	Modular	Yes
M905	10G	Modular	Yes
R915	11G	Rack	Yes
R910	11G	Rack	Yes
R815	11G	Rack	Yes
R810	11G	Rack	Yes
R715	11G	Rack	Yes
T710	11G	Tower	Yes
R710	11G	Rack	Yes
T610	11G	Tower	Yes
R610	11G	Rack	Yes
R515	11G	Rack	Yes
R510	11G	Rack	Yes
R415	11G	Rack	Yes

Model	Generation	Description	Supported
T410	11G	Tower	Yes
R410	11G	Rack	Yes
T310	11G	Tower	Yes
R310	11G	Rack	Yes
R210 II	11G	Rack	Yes
R210	11G	Rack	Yes
T110 II	11G	Tower	Yes
T110	11G	Tower	Yes
M610	11G	Modular	Yes
M610x	11G	Modular	Yes
M710	11G	Modular	Yes
M710HD	11G	Modular	Yes
M910	11G	Modular	Yes
R720	12G	Rack	Yes
R720xd	12G	Rack	Yes
R620	12G	Rack	Yes
T620	12G	Tower	Yes
M620	12G	Blade	Yes
R820	12G	Rack	Yes
R420	12G	Rack	Yes
R520	12G	Rack	Yes
R320	12G	Rack	Yes
M520	12G	Blade	Yes
M420	12G	Blade	Yes
M820	12G	Blade	Yes
T420	12G	Tower	Yes
T320	12G	Tower	Yes
VRTX	12G	Chassis	Yes
R220	12G	Rack	Yes
R920	12G	Rack	Yes

Supported PowerEdge Cloud Systems

This section lists the supported PowerEdge Systems.

Table 2. Supported PowerEdge Cloud Systems

Model	Type	Name	Supported
C1100	Server	Scooby	Yes
C2100	Server	Scooby-Fish	Yes
C6100	Sled	Plutonium	Yes
C6105	Sled	Cesium	Yes
C6145	Sled	Platinum	Yes

Supported PowerVault Systems

This section lists the supported PowerVault Systems.

Table 3. Supported PowerVault Systems

Model	Supported
NX200	Yes
NX300	Yes
NX1950	Yes
NX3000	Yes
MD1000	Yes
MD1120	Yes
MD1200	Yes
MD1220	Yes

Supported Operating Systems

This section lists the supported operating systems.

Table 4. Supported Operating Systems

Operating System	x86 or x64	Supported on Client and Host
Microsoft		
Windows XP	x86	Supported only in Client
Windows Vista	x86	Supported only in Client
Windows Vists SP1	x86	Supported only in Client
Windows 7	x86	Supported only in Client
Windows Server 2003	x86 and x64	Yes
Windows Server 2003 R2	x86 and x64	Yes
Windows Server 2008	x86 and x64	Yes
Windows Server 2008 R2	x64	Yes
Small Business Server 2011	x64	Yes

Operating System	x86 or x64	Supported on Client and Host
Windows Server 2012	x64	Yes
Windows Server 2012 R2	x64	Yes
Linux		
Red Hat Enterprise Linux 5	x86 and x64	Yes
Red Hat Enterprise Linux 6	x64	Yes
RHEV 3.0	x64	Yes
Cent 6.2	x64	Yes
Cent 6.4	x64	Yes
Cent 6.3	x64	Yes
Suse Linux Enterprise Server 10	x64	Yes
Suse Linux Enterprise Server 11	x64	Yes
Oracle Enterprise Linux 6.4	x64	Yes
Virtualization		
Microsoft Hyper-V Server 2008 R2	x64	Yes
Microsoft Hyper-V Server 2012 R2	x64	Yes
VMWare ESX 4.0	x64	Yes
VMWare ESX 4.1	x64	Yes
VMWare ESXi 4.0	x64	OpenManage Server Administrator Provider
VMWare ESXi 4.1	x64	OpenManage Server Administrator Provider
VMWare ESXi 5.0	x64	OpenManage Server Administrator Provider
VMWare ESXi 5.1	x64	OpenManage Server Administrator Provider
VMWare ESXi 5.5	x64	OpenManage Server Administrator Provider
Citrix Xenserver 6.2	x86	Yes
Oracle Virtual Machine 3.2	x64	Yes

Other Documents You May Need

In addition to this guide, you can view the *Release Notes*:

- During installation:
  - On systems running Linux, run the **./dell-dset-lx(bit)-(Version Number).bin** file and select option 1.

- After permanently installing the application:
  - On systems running Windows, in the **Start** menu, navigate to **DSET 3.6** → **View ReleaseNotes**. The *Release Notes* is displayed.
  - On systems running Linux, **the ReleaseNotes.txt** is available at **/opt/dell/advdiags/ dset/** folder.
- For information on installing the DSET application, see *Dell System E-Support Tool (DSET) Version 3.x Installation Guide* available at **dell.com/serviceabilitytools**.

Accessing Documents From Dell Support Site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Systems Management documents — **dell.com/softwaresecuritymanuals**
  - For Remote Enterprise Systems Management documents — **dell.com/esmmanuals**
  - For Enterprise Systems Management documents — **dell.com/openmanagemanuals**
  - For Client Systems Management documents — **dell.com/OMConnectionsClient**
  - For Serviceability Tools documents — **dell.com/serviceabilitytools**
  - For OpenManage Connections Enterprise Systems Management documents — **dell.com/ OMConnectionsEnterpriseSystemsManagement**
  - For OpenManage Connections Client Systems Management documents — **dell.com/OMConnectionsClient**
- From the Dell Support site:
  a. Go to **dell.com/support/manuals**.
  b. Under **General support** section, click **Software & Security**.
  c. In the **Software & Security** group box, click the required link from the following:
     - **Serviceability Tools**
     - **Enterprise System Management**
     - **Client System Management**
     - **Remote Enterprise System Management**
  d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the **Search** box.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **dell.com/support**
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down menu at the top of page.
4. Select the appropriate service or support link based on your need.

2

Using Dell System E-Support Tool (DSET) Application

Using the DSET application, you can generate reports on local and remote systems. The reports can be generated on:

- Local systems using GUI or CLI
- Remote systems using CLI

The data collection is allowed for the following operating systems on client and server:

- On a client system running Microsoft Windows to a server running Windows
- On a client system running Windows to a server running Linux
- On a client system running Linux to a server running Linux

NOTE: Data collection is not allowed from a client system running Linux to a server running Windows.

Event viewer and application logs are generated that can be used for troubleshooting purpose.

Generating Basic And Advanced Report

Before generating the report, make sure that Remote Provider is installed on the system.

On a system running Windows, while collecting a report from a system running Linux using non-root user credentials, make sure:

- To add the user to the root group on the system running Linux.
- To add the user to the **sudoers** file as follows:
  - `%root ALL=(ALL) NOPASSWD: ALL` — provides permission to all the users in the root group.
  - `<User> ALL=(ALL) NOPASSWD: ALL` — provides permission only to the specified user.

NOTE: For a non-root user, the hardware and storage data is collected using OpenManage Server Administrator namespace only.

On systems running Windows:

- To generate a basic report using the GUI, in the **Start** menu, navigate to **DSET 3.6** → **Create Basic DSET Report.**
- To generate an advanced report using the GUI, in the **Start** menu, navigate to **DSET 3.6** → **Create Advanced DSET Report.**

  A command window is displayed indicating the status. The generated report is saved as a **.zip** file on the user's desktop. For example, **DSET Report for [WIN-BPJ3P19JC4T SvcTag-7654321-PE R720xd] on 02-28- 2012 at 01.26 AM.zip.**

NOTE: On certain systems running Windows Server 2003 R2, Windows Server 2008, Windows SBS 2008, Windows SBS 2011, Windows Server 2012, and Windows Server 2012 R2 Hyper-V you must run the DSET application using the elevated privilege mode, where User Access Control (UAC) is enabled. To do this, right-click the **Create Basic DSET Report** or **Create Advanced DSET Report**, select **Run As Administrator**, and provide the administrator password.

For information about report filtering, see Report Filtering.

Report Filtering

During Dell System E–Support Tool (DSET) report collection, you can use this option to filter the critical information from the report such as:

- Host name
- IP address
- Subnet mask
- Default gateway
- MAC address
- DHCP server
- DNS server
- Processes
- Environment variables
- Registry
- Logs
- iSCSI data
- Fibre Channel data (host WWN and port WWN)

NOTE: If report filtering option is enabled for one-time report collection (Zero Footprint report), all of the above data is filtered. In permanent installation, you can specify the data to be filtered.

To enable the data filtering, select the **Enable Report Filtering** option during report collection.

To enable the data filtering using CLI, at the command prompt, run `dellsysteminfo –v`. Type `yes` to enable this option. For more information on report filtering, see List of CLI Options.

To include any of the data to the report, specify ’**no**’ in the following file:

- On systems running Windows — **<system drive>:\Program Files (x86)\Dell\AdvDiags\DSET\config\privacy_presetlist.cfg** (in 64-bit systems) or **<system drive>:\Program Files\Dell\AdvDiags\DSET\config\privacy_presetlist.cfg** (in 32- bit systems).
- On systems running Linux — **/opt/dell/advdiags/dset/config/privacy_presetlist.cfg**

NOTE: The logs may contain data such as IP or MAC address and so on. If logs are set to "no", then the data is not filtered in the report.

CLI Options

This section provides the CLI options for systems running Windows and Linux.

On Systems Running Windows

To start the CLI mode, in the **Start** menu, navigate to **DSET 3.6** → **DSET CLI.** The CLI command window opens and displays the location of the installed support files as:

<InstallDirectory>\AdvDiags\DSET\bin

At the command prompt, run the following command:

```
DellSystemInfo.exe [Options]
```

On Systems Running Linux

At the command prompt, run any of the following commands:

```
dellsysteminfo [Options]
```

Or

Change directory to **/opt/dell/advdiags/dset/bin** and run the command

```
dellsysteminfo.sh [Options]
```

List Of CLI Options

The `-h` option displays the list of available CLI options. To view the options, run the following command:

- On systems running Windows: `DellSystemInfo.exe -h`
- On systems running Linux: `dellsysteminfo -h`

Table 5. Command and Description

Command	Description
`-h`, --help	Displays the help text and exit.
`-s`, --server	Provide the details of the server to connect to. Use '.' to specify the local server details. For local report collection, the default setting is used and this parameter is not required. For remote report collection, the IP address of the remote server must be provided. For collection from an iDRAC7 source, provide the iDRAC IP address.
`-u`, --username	On systems running Windows, the current user name is used by default. On systems running Linux, you must provide the user name. For local report collection, this parameter is optional. For remote report collection, the user name for the remote server must be provided and the user must have administrator privileges on the remote server. For collection from an iDRAC7 source, provide the iDRAC login user name.
`-p`, --password	On systems running Windows, the current user password is used by default. On systems running Linux, specify the password. For local report collection, this parameter is optional for system running Windows but required for system running Linux. For collection from an iDRAC7 source, provide the iDRAC login password.

Command	Description
	NOTE: If `-p` is not included in the command, then you will receive a prompt to type in the password.
`-d`, --collect	Specify the type of data to be collected (one or more of the following) separated by a comma without any space: • `hw`— Server • `st`— Storage • `sw`— Software • `lg`— Logs • `ad`— Advanced logs **NOTE:** • If not specified, the default value for `-d` is `hw`, `st`, `sw`, and `lg`. • If `ad` is specified, by default, all the logs are collected and this may result in large size reports. • For iDRAC namespace only hardware and storage information is collected.
`-n`, --namespace	Specify the namespace to connect. If left blank, the program selects the best available namespace or specify one of the following options: • `root/dsetcim` for DSET — This is the default namespace that is installed with the Remote Provider component. Remote DSET receives information from this namespace even if Server Administrator is installed on the system. • `omsa` for OpenManage Server Administrator — Use this namespace instead of using the default namespace. In this case, install Server Administrator before running this command. • `root/cimv2` for ESX or ESXi default providers— Use this namespace on systems running ESX or ESXi. • `root/dcim/sysman` for OpenManage Server Administrator on ESXi — Use this namespace for connecting to the Server Administrator installed on the target ESXi system. • `root/dcim` — Use this name space for collecting data from an iDRAC7 system. **NOTE:** The collection is supported for systems only with an iDRAC7 system with express or enterprise license.
`-c`, --className	Provide the class name to retrieve the data for a specific component. If class name is provided, specify the namespace. For example, to retrieve data for CPU: On systems running Windows: `DellSystemInfo.exe -n root/dsetcim -c DCIM_CPUViewExt` On systems running Linux:

Command	Description
	`dellsysteminfo -n root/dsetcim -c DCIM_CPUViewExt`
`-r`, --reportname	Specify the default location for the generated report (**.zip**) file. The default location is desktop for Windows and **/root** for Linux. The default file name is DSET appended with the host name, service tag, and time stamp. Either report name or report name with full path is required to access it later and to upload to Dell Technical Support.
`-v`, --privacy	Use this option to filter the critical information mentioned in the Report Filtering section. Type `yes` to enable this option. Default option is `no`.
`-a`, --upload	Upload the report to the Dell Technical Support. Type `-a auto` to upload the generated report automatically to the Dell Technical Support. Type `-a manual` and include the (`-r`) filename to manually upload the report to the Dell Technical Support.
`-x`, --proxyhost	Upload the report to Dell Technical Support specifying proxy details. Type `-x` proxy IP or type host name to use the proxy server to upload the report to Dell Technical Support.
`-y`, --proxyusername	Type `-y` user name of the proxy server used to upload the report.
`-z`, --proxypassword	Type `-z` password for the user name of the proxy server used to upload the report. **NOTE:** If `-z` is not included in the command, then you will receive a prompt to type the password.

`-m`, --validate	Option to validate whether the report can be collected or not.
	When this option is used with `DellSystemInfo.exe`, `-a` , `-x`, `-y`, and `-z` are not included.
	If the validation is successful, then
	`Connection authentication test to device is successful.`
	message is displayed.
	If the validation is not successful, then
	`Dell System E-Support Tool is unable to connect to the system using any of the supported protocols.`
	message is displayed.

NOTE:

- Using authenticated proxy (-x, -y, and -z) option to upload the report are supported only for systems running the Windows operating system.
- The data collected from iDRAC7 namespace is limited compared to the data collected from systems running the Windows operating system or Linux operating systems with the Remote Provider installed.

Order Of Connection For Data Source

DSET uses the following data sources based on the namespace to collect hardware and storage information:

1. Remote Provider (Linux or Windows)
2. OpenManage Server Administrator Native (Linux or Windows)
3. ESX with SMASH profile
4. ESXi with Open Manage Server Administrator installed
5. iDRAC7 (out-of-band)

The following table provides the data source supported for DSET on Windows and Linux-based system.

Table 6. Data Source and DSET on Windows and Linux-based systems

Data Source	DSET on Windows-based System	DSET on Linux-based System
Remote Provider (Windows)	Yes	No
iDRAC7 (out-of-band)	Yes (only remote systems)	Yes (only remote systems)
Remote Provider (Linux)	Yes	Yes
OpenManage Server Administrator Native (Windows)	Yes	No
OpenManage Server Administrator Native (Linux)	Yes	Yes (only local systems)
ESX with SMASH profile	Yes	Yes
ESXi with OpenManage Server Administrator installed	Yes	Yes (only remote systems)

The following table provides information on the data collection supported by DSET for the data source:

Table 7. Data Collection Supported by DSET Application and Data Source

Data Source	Hardware Components	Storage Components	Operating System	Logs
Remote Provider	Full	Full	Full	Full
iDRAC7	Limited	Limited	No	No
OpenManage Server Administrator	Full	Full	Full	Full
ESX with SMASH profile	Limited	No	Full	Full
ESXi with OpenManage Server	Full	Full	Limited	Limited

Data Source	Hardware Components	Storage Components	Operating System	Logs
Administrator installed				

Usage Examples

This section provides examples to generate Zero FootPrint report and also reports on your local and remote systems.

On Local System

Example 1: To collect software information and save it in the specified location, run the following command:

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe -d sw -r C:\temp
  \software.zip
  ```

- On systems running Linux

  ```
  dellsysteminfo -d sw -r /opt/dell/myreports/software.zip
  ```

Example 2: To collect information from DSETCIM namespace and save it in the specified location, run the following command:

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe -n root/dsetcim -
  r C:\temp\all.zip
  ```

- On systems running Linux

  ```
  dellsysteminfo -n root/dsetcim -r /opt/dell/myreports/all.zip
  ```

Example 3: To collect report information with report filtering option enabled, auto upload to Dell Technical Support, and save it in the specified folder, run the following command:

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe -v yes -a auto -r
  C:\temp\dsetreport.zip
  ```

- On systems running Linux

  ```
  dellsysteminfo -v yes -a auto -r /opt/dell/myreports/dsetreport.zip
  ```

NOTE: If `-d` option is not specified, then hw, st, sw, and lg data categories are collected by default.

For more information on report filtering, see Report Filtering.

Example 4: To collect report information and upload to Dell Technical Support using authenticated proxy, run the command:

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe –a manual –r C:
  \temp\dset_report.zip –x <IP_ADDRESS> –y lab\test
  ```

  or

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe –upload=manual –r
  C:\temp\dset_report.zip —proxyhost= <IP_ADDRESS> —proxyusername=lab\test
  ```

On Remote System

Example 1: To run the report on a remote system, provide the Fully Qualified Domain Name (FQDN) or IP address of the remote system and administrator credentials.

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe -s <IP_ADDRESS> -
  u <USERNAME> -p <PASSWORD> -d hw,sw -r C:\temp\dset.zip
  ```

- On systems running Linux

  ```
  dellsysteminfo -s <IP_ADDRESS> -u <USERNAME> -p <PASSWORD> -d hw,sw -r /opt/
  dell/myreports/dset.zip
  ```

NOTE: The data collected from ESX/ESXi namespace is lesser compared to the data collected from Windows or Linux systems on which Remote Provider is installed.

Example 2: To collect report information and auto upload to Dell Technical Support using authenticated proxy, run the command:

- On systems running Windows

  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe –a auto –r C:
  \temp\dset_report.zip –x <IP_ADDRESS> –y lab\test –s <IP_ADDRESS> –u
  <USERNAME> –p <PASSWORD>
  ```

Example 3: To collect report information from an iDRAC7 source.

-
  ```
  C:\Program Files\Dell\AdvDiags\DSET\bin> DellSystemInfo.exe -s<iDRAC
  IP_Address> -u <username> -p<password> -r C:\temp\dset_report.zip
  ```

  NOTE: Limited data is collected from the iDRAC7 source.

Zero FootPrint Report Collection

Example 1: To collect software and hardware information silently and save it in the specified location, run the following command:

- On systems running Windows: `Dell_DSET_3.6.x.exe REPORTNAME=<NAME> COLLECT=<hw,sw> /qn`
- On systems running Linux: `dell-dset-lx(bit)-(Version_Number).bin –qn -d <hw,sw> -r<reportname>`

Viewing DSET Report

You can view the hardware, storage, and software data in the generated report using the GUI. The logs and advanced log information are available in the log files located in the logs folder (part of the **.zip** file).

To view the report:

- On systems running Windows, unzip the **.zip** file using the password 'dell'.
- On systems running Linux, copy the **.zip** file to Windows system and unzip the file using the password 'dell'.

After you unzip, read the **ReadmeFirst.txt** file for instructions to view the report.

3

Error Codes

This appendix provides the list of Dell System E-Support Tool (DSET) application error codes.

DSET Application Error Codes

DSET application returns custom error codes on collection of reports.

To view the error code returned after the collection of report:

- For systems running on Windows type, `echo %errorlevel%`.
- For systems running on Linux type, `echo $?`.

The list of error codes returned by `dellsysteminfo` are:

Table 8. DSET Error Codes and Description

Error Code	Description	Solution
0	Success	-
1	Any error that is not part of the list provided in this table.	-
2	Incorrect option provided in the command line.	Check the command line options and provide the valid option.
3	The device is not reachable through the supported protocol.	-
4	iDRAC has Basic Management With IPMI license.	Upgrade the license to iDRAC7 Express or Enterprise.
5	The user name and password is not correct.	Provide the correct user name and password.
6	Unable to collect due to hardware connection error.	-
7	Sudo prerequisite is missing.	For more details on prerequisites, see the *Release Notes* available at **dell.com/serviceabilitytools**.
8	Hardware data source is not found.	-
9	Storage data source is not found.	-
10	Software data source is not found.	-
11	Logs data is not collected.	-
12	Error occurred while creating index in the report for SCSI or SAS storage devices.	-
13	Final report conversion to zip file format failed.	-

Error Code	Description	Solution
14	Failed to convert files from text to xml format.	-
15	Data of a few hardware classes are not collected.	-
16	Data of a few software classes are not collected.	-
17	Data of a few storage classes are not collected.	-
18	Invalid file name is provided or the path to save the report does not exist.	-
19	Invalid class name is provided for data collection.	Check for available class name.
21	Incorrect option for uploading the file is provided in the command line.	Check for available option for the file upload in the help menu.
22	Report file size exceeds the maximum size allowed for upload.	-
23	Server SSL certificate is invalid or expired.	-
24	Failed to divide the report file into chunks for upload.	-
25	Error occurred while uploading file to the server due to server issues.	Try to upload the file again later.
26	The report file to upload is invalid or corrupted.	Make sure that the file to upload is valid.
27	Upload time for report file exceeds the maximum allowed time.	Server may be busy or slow. Try to upload again later.
28	Initialization of the upload module failed.	-
29	Failed to set the provided authenticated proxy credentials.	-
30	Proxy authentication method is not supported.	Only Basic, Negotiate, and NTLM Authentication methods are supported.
31	Invalid proxy credentials are provided to upload the report.	Provide valid proxy credentials.
40	The admin user privileges are not available.	DSET must be run as an administrator.
41	Any exception error.	-
42	Unable to collect due to software connection error.	-