

OpenText™ Endpoint Management

Command Line Utilities Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/en-us/legal>.

© 2008 - 2025 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	5
1 OpenText Endpoint Management Command Line Utilities	7
zac for Windows	8
2 ZENworks Diagnostic Center	17
Collecting ZDC Baseline	17
Downloading and Extracting ZDC	18
Running ZDC	18
3 Troubleshooting ZENworks Diagnostics Center	21
4 Guidelines for Working with Zman	23

About This Guide

This *OpenText Endpoint Management Command Line Utilities Reference* includes information to help you use Endpoint Management utilities.

The information in this guide is organized as follows:

- ♦ [Chapter 1, “OpenText Endpoint Management Command Line Utilities,” on page 7](#)

Audience

This guide is intended for Endpoint Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

OpenText Endpoint Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [Online documentation](#) website.

1 OpenText Endpoint Management Command Line Utilities

The following sections give information on the OpenText Endpoint Management command line utilities:

- ♦ [“zac for Windows\(1\)” on page 8](#)

zac for Windows(1)

Name

zac - The command line management interface for the Endpoint Agent that is installed and running on Windows managed devices.

Syntax

zac command options

Description

The zac utility performs command line management functions on the Endpoint Agent, including installing and removing software bundles, applying policies, and registering and unregistering the device.

Guide to Usage

Most commands have a long form and a short form:

- ♦ Long form: add-reg-key
- ♦ Short form: ark

When both forms are available, the command is listed as follows:

add-reg-key (ark) arguments

When using the command, enter only the long form or the short form:

zac add-reg-key arguments

zac ark arguments

Arguments can be mandatory or optional. Mandatory arguments are included in angle brackets <argument>. Optional arguments are included in square brackets [argument]. If an argument includes a space, enclose it in quotation marks:

zac ark "arg 1"

Help Commands

- ♦ ["/h or --help" on page 8](#)

/h or --help

Displays information about the commands.

List of Commands

- ♦ ["Bundle Commands" on page 9](#)
- ♦ ["File System Commands" on page 11](#)

- ♦ “Inventory Commands” on page 11
- ♦ “Logging Commands” on page 11
- ♦ “Policy Commands” on page 12
- ♦ “Registration Commands” on page 12
- ♦ “Status Commands” on page 14
- ♦ “Agent Update Commands” on page 16
- ♦ “External Message” on page 16

Bundle Commands

- ♦ “`bundle-install (bin) <bundle display name>`” on page 9
- ♦ “`bundle-launch (bln) <bundle display name> [-noSelfHeal]`” on page 9
- ♦ “`bundle-list (bl)`” on page 9
- ♦ “`bundle-props (bp) <bundle display name>`” on page 9
- ♦ “`bundle-refresh (br) <bundle display name or guid>`” on page 10
- ♦ “`bundle-uninstall (bu) <bundle display name>`” on page 10
- ♦ “`bundle-verify (bv) <bundle display name>`” on page 10
- ♦ “`bundle-status-rollup (bsr)`” on page 10

`bundle-install (bin) <bundle display name>`

Installs the specified bundle. Use the `bundle-list` command to get a list of the available bundles and their display names.

Example:

```
zac bin bundle1
```

`bundle-launch (bln) <bundle display name> [-noSelfHeal]`

Launches the specified bundle. Use the `bundle-list` command to get a list of the available bundles and their display names.

Example to launch a bundle based on the display name:

```
zac bln bundle1
```

Example to launch a bundle based on the display name and turn selfhealing off if the launch action fails (by default, selfhealing is turned on):

```
zac bln bundle1 -noSelfHeal
```

`bundle-list (bl)`

Displays the list of bundles assigned to the device and the logged in user.

Example:

```
zac bl
```

`bundle-props (bp) <bundle display name>`

Displays the status, version, GUID, and requirements information for the specified bundle. Use the `bundle-list` command to get a list of the available bundles and their display names.

Example:

```
zac bln bundle1
```

bundle-refresh (br) <bundle display name or guid>

Refreshes information about the specified bundle.

Example:

```
zac br bundle1
```

bundle-uninstall (bu) <bundle display name>

Uninstalls the specified bundle. Use the `bundle-list` command to get a list of installed bundles and their display names.

Example:

```
zac bu bundle1
```

bundle-verify (bv) <bundle display name>

Verifies an installed bundle (specified by `bundle display name`) to ensure that no files have been removed or corrupted. Use the `bundle-list` command to get a list of the installed bundles and their display names.

Example:

```
zac bv bundle1
```

bundle-status-rollup (bsr)

Rolls up the status information of a given bundle to the server, based on the display name or GUID of the bundle.

Options:

-a Rolls up the status information of the available bundles.

-s Rolls up the status information of a bundle to the specified server. The server name can be a DNS name of the server. Specify the new port number in addition to the server name.

-n Rolls up the status information of specific bundles, based on the display name or the GUID of the bundle.

Examples:

To roll up the status information of available bundles:

```
zac bundle-status-rollup -a
```

To roll up the status information of a given bundle, based on the display name or GUID of the bundle:

```
zac bsr -n
```

To roll up the status information of available bundles to the specified Primary Server:

```
zac bsr -a -s <server name>
```

For example, `zac bsr -a -s 164.99.137.50`

To roll up the status information of a given bundle to the specified Primary Server, based on the display name or GUID of the bundle:

```
zac bsr -n "Bun1 display name" "Bun2 display name" -s <server name>
```

NOTE: To run the `zac bsr` command, you need to be a Windows administrator.

File System Commands

- ♦ “`file-system-guid (fsg) [-d] [-r]`” on page 11

file-system-guid (fsg) [-d] [-r]

Displays, removes, or restores the workstation GUID in the file system in preparation for taking an image.

For example:

To display the GUID value:

```
zac fsg
```

To remove the GUID and also `conninfo.dat` from the file system:

```
zac file-system-guid -d
```

To restore the GUID to the file system:

```
zac file-system-guid -r
```

To display the GUID value:

```
zac fsg
```

Inventory Commands

- ♦ “`inventory [scannow | cdf | -f scannow]`” on page 11

inventory [scannow | cdf | -f scannow]

Runs an inventory scan or opens the Collection Data Form.

Example to run an inventory scan:

```
zac inv scannow
```

Example to open the Collection Data Form:

```
zac inv cdf
```

Example to run a full scan:

```
zac inv -f scannow
```

Logging Commands

- ♦ “`logger (log) [resetlog | level [MANAGED|ERROR|WARN|INFO|DEBUG] | managedlevel]`” on page 11

logger (log) [resetlog | level [MANAGED|ERROR|WARN|INFO|DEBUG] | managedlevel]

Changes or displays the logger configuration for the Endpoint Agent.

You can use the following options:

`resetlog` - Resets the log.

level - If this option is used without a level, it displays the current managed logging level. If it is used with one of the levels, changes the logging level to the specified level.

managedlevel - Displays the Global Log level of the zone.

Example to reset the log file:

```
zac logger resetlog
```

Example to show the current log level:

```
zac logger level
```

Example to set the log level to DEBUG and above:

```
zac logger level DEBUG
```

Policy Commands

- ♦ `"policy-list (pl)"` on page 12
- ♦ `"policy-refresh (pr)"` on page 12
- ♦ `"policy-refresh (pr) [/force] [/nologoff]"` on page 12

policy-list (pl)

Lists the policies that are currently being enforced on the device (effective policies). To list all policies (effective and non-effective), use the `--all` option.

Examples:

```
zac pl
```

```
zac pl --all
```

policy-refresh (pr)

Applies all of the policies assigned to the device and user.

Example:

```
zac pr
```

policy-refresh (pr) [/force] [/nologoff]

Applies all of the policies assigned to the device and user forcefully and without logging off.

Example:

To apply forcefully all of the policies assigned to the device and user:

```
zac pr /force
```

To forcefully apply all of the policies assigned to the device and user without logging off:

```
zac pr /force /nologoff
```

Registration Commands

- ♦ `"add-reg-key (ark) <registration key>"` on page 13
- ♦ `"register (reg) [-g] [-k <key>] <Cloud Server URL>"` on page 13
- ♦ `"unregister (unr) [-f]"` on page 13

add-reg-key (ark) <registration key>

Registers the device by using the specified key. Registration with keys are additive. If the device has previously been registered with a key and you register it with a new key, the device receives all group assignments associated with both keys.

Example:

```
zac ark key12
```

register (reg) [-g] [-k <key>] <Cloud Server URL>

Registers the device in a Management Zone.

You can use the following options:

g - Lets you create a new device object with a new GUID and password for the device if you have multiple devices with the same GUID. When you register a device by using this switch, all the associations (policies and bundles) assigned to the original device object are removed. You cannot use this option to create a new GUID for a Primary Server or a Satellite device. The local user must have Local Administrator rights to use this option.

You can use the following options:

k - Lets you register the device using the specified registration key.

sn - Lets you register the device using subscription name.

a - Lets you register the device using the Enrollment token.

g - Lets you create a new device object with a new GUID and password for the device if you have multiple devices with the same GUID. When you register a device by using this switch, all the associations (policies and bundles) assigned to the original device object are removed.

Examples:

To register a device using the enrollment token and subscription name, run the following command:

```
zac register -a <EnrollmentToken> -sn <subscriptionname> https://abcd.opentext.com
```

If you run the command without specifying the parameters, then you will be prompted to provide enrollment token and subscription name.

To register using a key, run the following command:

```
zac register -k mykey https://abcd.opentext.com
```

To generate a new device GUID and then register, run the following command:

```
zac register -g https://abcd.opentext.com
```

NOTE: When you modify or update the GUID using the -g option, then audit and messages generated with the old GUID will be lost.

unregister (unr) [-f]

Removes the device's registration from the current Zone.

Example:

To force a device to unregister locally when a server cannot be contacted:

```
zac unr -f
```

Status Commands

- ♦ “`cache-clear (cc)`” on page 14
- ♦ “`dump-prop-pages (dpp) <target directory>`” on page 14
- ♦ “`refresh (ref)[general | partial bundle <Bundle Display Name> [bypasscache]`” on page 14
- ♦ “`set-proxy (sp) [options] <IP address/Hostname:port>`” on page 15
- ♦ “`zone-config (zc) [-l]`” on page 15
- ♦ “`statussender (sts)`” on page 15

cache-clear (cc)

Clears the Endpoint Management cache on the device. This removes all entries in the cache database and deletes any cache files associated with those entries.

Example:

```
zac cc
```

NOTE: If your administrator has enabled the self defense feature for the Endpoint Agent, you must supply an override password before running the `zac cc` command. Otherwise, you receive the following message:

```
You do not have permission to clear the cache. Please contact your
Endpoint Management administrator.
```

You must request the override password from your Endpoint Management administrator. If he has not set an override password, he must do so before you can use the command. After you receive the password:

1. Double-click the Agent tray icon in the system tray, click **Agent** (under **Status**), then click the **Policy Override** link in the **Agent Security Settings** section to display the About box.
 2. Click **Override Policy**, enter the override password, then click **Override**.
 3. Go to a command line prompt and run the `zac cc` command.
 4. After the cache is successfully cleared, return to the About box and click **Load Policy** to disable the password override.
-

dump-prop-pages (dpp) <target directory>

Outputs the HTML pages displayed in the Endpoint Management icon’s property pages to files in the specified target directory.

Example:

```
zac dpp c:\temp
```

refresh (ref)[general | partial bundle <Bundle Display Name> [bypasscache]

Initiates a general refresh to refresh all bundles, policies, registration, and configuration settings; initiates a partial refresh to refresh all policies, registration, and configuration settings.

Use `bypasscache` to avoid using data from the server cache during the refresh. This option is useful for testing or troubleshooting.

Examples:

```
zac ref general bypasscache
zac ref partial bypasscache
```

set-proxy (sp) [options] <IP address/Hostname:port>

Specifies a proxy to contact rather than contacting a Cloud Server directly.

The options are:

- default - Sets a proxy that can be overridden by proxy settings from the Management Zone.
- clear - Clears the current proxy, but will use proxy settings from the Management Zone.
- ipv6 - sets an IPv6 proxy.

Examples:

IPv4:

```
zac sp 123.456.78.90:2349 administrator novell
zac sp /default 123.456.78.90:2349
zac sp /clear
```

IPv6:

```
zac sp /ipv6 [2001:db8:0:1:1:1:1:1]:2349 administrator novell
zac sp /default /ipv6 [2001:db8:0:1:1:1:1:1]:2349
zac sp /clear /ipv6
```

If a username and password is not specified, then you will be prompted to enter them.

zone-config (zc) [-l]

Displays information about the Cloud Server that the device is accessing for configuration information (the Configuration server) or lists the information for the Configuration server.

Examples:

```
zac zc
zac zc -l
```

statussender (sts)

This command rolls up status information to the Primary Server. You can either roll up information that was updated since the last time the status was rolled-up or you can roll up the complete status information.

Examples:

To roll up status information that was updated since the last successful status roll up:

```
zac sts rollup
```

To roll up status information on the same thread

```
zac sts rollup syn
```

To roll up complete status information:

```
zac sts rollup full
```

Agent Update Commands

- ♦ “`zac agent-update-report-status / aurs`” on page 16

`zac agent-update-report-status / aurs`

Enables administrators to resend the agent update status to the cloud server immediately.

External Message

`zac ExtMessageProc / emp`

Executes external message processor command.

2 ZENworks Diagnostic Center

ZENworks provides a tool called as ZENworks Diagnostic Center (ZDC) that helps you to verify the health of the Primary Servers and the Management Zone before deploying a system update.

ZENworks Diagnostic Center (ZDC) performs a series of diagnostic tests on Primary Servers, and determines the state of the Primary Servers and the Management zone. ZDC comprises of the following verifiers:

- ♦ **ZENworks System Files Verifier:** Verifies the existence and consistency of critical system files that are required by ZENworks.
- ♦ **ZENworks Database Schema Verifier:** Validates the correctness of the schema (tables, indexes, database procedures, etc) of the databases used by ZENworks.
- ♦ **ZENworks Content Verifier:** Validates the existence and consistency of the contents hosted on the Primary Server that has ZDC installed and running.

To verify the database schema before upgrading ZENworks, you must use the ZENworks Diagnostic Center tool available in the ZENworks Installation media. To verify the health of the Primary Servers and the Management Zone after upgrading ZENworks, download and use the ZENworks Diagnostic Center from ZENworks Control Center. For more information, go through the following sections:

- ♦ [“Collecting ZDC Baseline” on page 17](#)
- ♦ [“Downloading and Extracting ZDC” on page 18](#)
- ♦ [“Running ZDC” on page 18](#)

Collecting ZDC Baseline

When you perform some database maintenance activities, the database objects such as indexes might be missing, as a result, issues such as performance degradation, might be observed. Hence, before performing any database maintenance activities, it is recommended that you to run ZDC and collect a baseline from the database. After completing the maintenance activity, run ZDC again to identify and re-create the missing schema objects. The steps to be performed are as follows:

1. Download the relevant version of ZDC from the Micro Focus Customer Center.

For example, if you are using ZENworks 2017 Update 4, then ensure that you download and use the ZDC for ZENworks 2017 Update 4.

2. Run the following commands on a Primary Server to collect the baseline schema:

- ♦ **ZENworks Database:** `./zdc collect -v zendatabase -b mybaseline.zdc`
- ♦ **Audit Database:** `./zdc collect -v auditdatabase -b mybaseline.zdc`
- ♦ **Antimalware Database:** `./zdc collect -v amdatabse -b mybaseline.zdc`

The baseline file (mybaseline.zdc) is saved in the same location.

3. Perform the required database maintenance activity.

After performing the required maintenance activity, run the following commands to verify the schema of the database:

- ♦ **ZENworks Database:** `./zdc verify -v zendatabase -b mybaseline.zdc`
- ♦ **Audit Database:** `./zdc verify -v auditdatabase -b mybaseline.zdc`
- ♦ **Antimalware Database:** `./zdc verify -v amdatabse -b mybaseline.zdc`

Downloading and Extracting ZDC

You need to download and extract ZENworks Diagnostic Center on the Primary Server on which you want to run the tool.

- 1 Open a Web browser to the following address:

[Micro Focus Download](#) site.

- 2 From the ZCM <version> ZENworks Diagnostic Center - executable and pattern file page, download the `ZENworksDiagnosticCenter.zip` file to a temporary location and extract the ZIP file contents.

ZENworks system files and the ZENworks database schema require baseline data collected from known good deployments to compare with and assess the health of the current deployment data.

The ZIP file contains the baseline data file, `zdc_<version>.zdc`, which is available in the `data` directory. This file contains the baseline data collected from the known good deployments of ZENworks Configuration Management.

ZDC executable and configuration files are required to run ZDC. The directory that contains the ZENworks Diagnostic Center is referred to as `$ZDC_Home`.

Running ZDC

- 1 At Primary Server's console prompt, go to the `$ZDC_Home` directory.
- 2 Run the appropriate command.

- ♦ To verify the complete ZENworks content:

On Windows: `zdc.bat verify -b
<complete_path_of_the_ZDC_baseline_data_file>`

On Linux: `./zdc verify -b
<complete_path_of_the_ZDC_baseline_data_file>`

- ♦ To verify the specific ZENworks system files, the ZENworks database schema, or the ZENworks content:

On Windows: `zdc.bat verify -v systemfiles,zendatabase,zencontent -b
<complete_path_of_the_ZDC_baseline_data_file>`

On Linux: `./zdc verify -v systemfiles,zendatabase,zencontent -b
<complete_path_of_the_ZDC_baseline_data_file>`

- ♦ To verify only for the ZENworks system files:

On Windows: `zdc.bat verify -v systemfiles -b
<complete_path_of_the_ZDC_baseline_data_file>`

On Linux: `./zdc verify -v systemfiles -b
<complete_path_of_the_ZDC_baseline_data_file>`

- ♦ To verify only for the ZENworks database schema:

On Windows: `zdc.bat verify -v zendatabase -b
<complete_path_of_the_ZDC_baseline_data_file>`

On Linux: `./zdc verify -v zendatabase -b
<complete_path_of_the_ZDC_baseline_data_file>`

- ♦ To verify only for the ZENworks content:

On Windows: `zdc.bat verify -v zencontent`

On Linux: `./zdc verify -v zencontent`

You can also specify the following command options while running ZDC.

-s: session name

-l: complete path of the ZDC log filename

-r: complete path of the ZDC reports directory

ZDC runs the diagnostic tests and generates the reports in the HTML format. The reports are stored in the `$ZDC_Home/reports/timestamp` directory on a Linux Primary Server. To view the reports, open `index.html` that is located in the `report` directory.

The complete log of the diagnostic tests is stored in `$ZDC_HOME/logs/timestamp.log` on a Linux Primary Server.

Verifying Audit Database

To verify the Audit Database schema in ZENworks by using the ZDC tool:

- ♦ **On Windows:** Run the `zdc.bat verify auditdatabase -b
<complete_path_of_the_ZDC_baseline_data_file>` command.
- ♦ **On Linux:** Run the `./zdc verify auditdatabase -b
<complete_path_of_the_ZDC_baseline_data_file>` command.

Audit and ZENworks databases cannot be verified by running the command in one instance. They need to be verified separately.

The ZDC reports for Audit are present in the `reports\timestamp` directory. You can view reports from the `index.html` file.

Verifying Antimalware Database

To verify the Antimalware Database schema in ZENworks by using the ZDC tool:

- ♦ **On Windows:** Run the `zdc.bat verify -v amdatabse -b
<complete_path_of_the_ZDC_baseline_data_file>` command.
- ♦ **On Linux:** Run the `./zdc verify -v amdatabse -b
<complete_path_of_the_ZDC_baseline_data_file>` command.

Antimalware, Audit and ZENworks databases cannot be verified by running the command in one instance. They need to be verified separately.

The ZDC reports for Audit are present in the `reports\timestamp` directory. You can view reports from the `index.html` file.

3 Troubleshooting ZENworks Diagnostics Center

The following sections provide solutions to the problems you might encounter while working with Micro Focus ZENworks Diagnostics Center:

ZENworks Diagnostics Center Report displays Inconsistencies for Patch Management

Source: ZENworks 2020 Update 3

Explanation: While running ZENworks Diagnostics on the database, the following inconsistencies will be displayed in the ZDC report:

```
ERROR Missing object in table 'patchsignature'
Object type: [Index] , Object name:
[uniq_patchsignature_type]
Detail: [Name: uniq_patchsignature_type, Table:
patchsignature, ColumnMap: {type=1}, isConstraint: false]
```

```
IndexERROR Missing object in table 'patchsignature'
Object type: [Constraint] , Object name:
[uniq_patchsignature_type]
Detail: [Name: uniq_patchsignature_type, Type: UNIQUE,
Table: patchsignature, ColumnOrder {Position: 1
[ColumnName: type, DeleteCascade: false}]}
```

```
ConstraintERROR Missing object in table 'patchsuperseded'
Object type: [Index] , Object name: [uniq_patchsuperseded]
Detail: [Name: uniq_patchsuperseded, Table:
patchsuperseded, ColumnMap: {newpatchid=1, oldpatchid=2},
isConstraint: false]
```

```
IndexERROR Missing object in table 'patchsuperseded'
Object type: [Constraint] , Object name:
[fk_patchsuperseded_newpatchid]
Detail: [Name: fk_patchsuperseded_newpatchid, Type: FOREIGN
KEY, Table: patchsuperseded, ColumnOrder {Position: 1
[ColumnName: newpatchid, DeleteCascade: true]}]
```

```
ConstraintERROR Missing object in table 'patchsuperseded'
Object type: [Constraint] , Object name:
[fk_patchsuperseded_oldpatchid]
Detail: [Name: fk_patchsuperseded_oldpatchid, Type: FOREIGN
KEY, Table: patchsuperseded, ColumnOrder {Position: 1
[ColumnName: oldpatchid, DeleteCascade: true]}]
```

```
ConstraintERROR Missing object in table 'patchsuperseded'
Object type: [Constraint] , Object name:
[uniq_patchsuperseded]
Detail: [Name: uniq_patchsuperseded, Type: UNIQUE, Table:
patchsuperseded, ColumnOrder {Position: 1 [ColumnName:
newpatchid, DeleteCascade: false]} {Position: 2
[ColumnName: oldpatchid, DeleteCascade: false]}]
```

```
ConstraintERROR Missing object in table 'patchdevicestatus'
Object type: [Index] , Object name:
[uniq_patchdevicestatus]
Detail: [Name: uniq_patchdevicestatus, Table:
patchdevicestatus, ColumnMap: {deviceid=1, signature_id=2},
isConstraint: false]
```

```
IndexERROR Missing object in table 'patchdevicestatus'
Object type: [Constraint] , Object name:
[uniq_patchdevicestatus]
Detail: [Name: uniq_patchdevicestatus, Type: UNIQUE, Table:
patchdevicestatus, ColumnOrder {Position: 1 [ColumnName:
deviceid, DeleteCascade: false]} {Position: 2 [ColumnName:
signature_id, DeleteCascade: false]}]
```

Action: These inconsistencies can be ignored. If you are using ZENworks Patch Management with legacy feed even after updating to ZENworks 2020 Update 3, then you will observe these inconsistencies. In ZENworks 2020 Update 3, after migrating to the Advanced Patch feed, all inconsistencies would be automatically addressed.

4 Guidelines for Working with Zman

Follow these guidelines as you work with the zman command line utility of Micro Focus ZENworks:

- ♦ If an XML file that is exported by using the zman commands such as `bundle-create` or `policy-create` contains diacritic or extended ASCII characters such as ñ, ë, and Ä, you must open the file in an editor using the UTF-8 encoding. If you make any changes to the file, you must save it the UTF-8 format.
- ♦ If you want to redirect the output of a command containing extended ASCII characters to a file on Windows, you must not use the command line redirection operator (>), because the code page of an MS-DOS prompt is different from the code page used to write to files on most locales.

For example, in case of Western European languages like English, French, German, and Spanish, the code page of the DOS prompt is cp437 or cp850, but the rest of the Windows operating system uses cp1252.

To redirect the output to a file and correctly retain the extended ASCII characters, use the `-R | -Redirect` global option.

- ♦ While connecting to Linux Servers from a Windows machine by using clients like PuTTY, set the character set used for translation to UTF-8. This ensures proper translation of characters other than standard ASCII characters.

To set the character set for translation to UTF-8 in PuTTY:

1. Open the PuTTY client.
2. In the PuTTY Configuration window, click **Windows > Translation**.
3. In the **Received Data Assumed to be in Which Character Set** drop-down list, select **UTF-8**.

NOTE: You do not need to do this if the input to the command or its output contains only the a-z or A-Z characters.

- ♦ By default, zman uses the default locale of the server. You can have zman use a specific language:
 - ♦ On Windows, specify the appropriate user language and file encoding as a value for the `JVM_STARTUP_OPTIONS` property in `ZENworks_Installation_directory\Micro Focus\ZENworks\conf\zman\properties\zman-config.properties`.
For example, to run zman in English, set the value of `JVM_STARTUP_OPTIONS` to `-Duser.language=en -Dfile.encoding=cp850`. After editing the file, change the code page of the command prompt to cp850 by using the `chcp 850` command.
 - ♦ On Linux, edit `/opt/microfocus/zenworks/bin/zman` to add `-Duser.language=<language>` after `/opt/microfocus/zenworks/lib/java/bin/java`.

For example, to run zman in English, change the zman script file as follows:

```
/opt/microfocus/zenworks/lib/java/bin/java -Duser.language=en -  
Djava.library.path="${LD_LIB_PATH}" .....
```

