Windows 10

Table Of Conents

Common CLI Commands

Command	Name	Desc
certmgr	Certificate Manager	Manages security certs for current user.
certlm	Certificate Manager Local Machine	Manages certs for local machine.
compmgmt	Computer Management	Task Scheduler, Event Viewer, Local Users and Groups, Performance Monitor, Device Manager, Disk Management, Services, WMI control
devmgmt	Device Manager	
diskmgmt	Disk Manager	
eventvwr	Event Viewer	
virtmgmt	Hyper-V Manager	Create, run, and modify VMs.
lusrmgr	Local Users and Groups	Manage local users and groups.
msinfo32	MS Info	Displays a GUI that shows low level details about the system. This can be saved in a .nfo file to be viewed later.
perfmon	Performance Monitor	

Command	Name	Desc
printmanagement	Print Management	Printers and Jobs.
regedit	Registry	
rstrui	Restore Points	
sdclt	Backup and Restore	
services	Services	
taskshd	Task Scheduler	
tpm	Trusted Platform Module	Configure the computer's TPM.
wf	Windows Firewall	

System Information

CLI tool that displays information regarding the current system.

```
# Displays local system info
systeminfo

# Remote system information
systeminfo /s [Hostname] /u [Remote Username] /p [Remote Password]

# Output to a file
systeminfo >> [File name].txt
```

Disk Partition

CLI tool that mirrors Disk Manager GUI

```
# Enter the CLI
diskpart

# Lists disks
> list disk

# Selects a disk
> select disk [Disk number]

# Lists partitions on a disk
> list partition
```

```
# Lists volumes on a disk
> list volume

# Additional Commands
> ?
```

Check Disk

Runs a service that checks the disk for competancy.

```
# Base Command
chkdsk

# Fix detected errors
chkdsk /f

# Identify bad sectors
chkdsk /r
```

Additional Troubleshooters

Lists all the advanced troubleshooters

```
Settings > Update & Security > Troubleshoot > Additional Troubleshooters
```

Problem Reports

Opens the Problem Reports GUI

```
Search: problem reports
```

Reliability Monitor

Shows a timeline of errors organized by application

```
Search: reliability
```

The Registry

Root

Key	Abrv	Desc
HKEY_CLASSES_ROOT	HKCR	Various app and security classes.
HKEY_CURRENT_USER	HKCU	Current hardware. Volatile.
HKEY_LOCAL_MACHINE	HKLM	Windows Config.
HKEY_USERS	HKU	Entries for every user account (SID).
HKEY_CURRENT_CONFIG	HKCC	Entries for the current user.

Entry Types

Type	Desc
REG_SZ	Zero-terminated string.
REG_BINARY	Binary.
REG_DWORD	Double word (32 bit numeric). Often used 0 or 1 as a bool.
REG_QWORD	64 bit numeric.
REG_MULTI_SZ	A group of zero-terminated strings.
REG_EXPANDED_SZ	Zero-terminated string. Good for variables such as %SystemRoot%.