Remote Diagnostics Tool (RDT)

Overview:

Desktop Administrators and Helpdesk staff will benefit from using this tool. No Installation is required. Free fully functional Product.

This remote diagnostics tool (RDT) was designed and written to aid in the diagnostics and overall investigation of a remote PC whilst it is on a corporate network, without interrupting the user in their daily work.

The tool was originally designed as a replacement to a few different well-known script tools like the "SCCM Client tools" and "Dameware" as we were not allowed to use them on the corporate network anymore. "They were too intrusive" and not secure enough!

The aim of interrogating information from the PC like: SCCM execution reports and Installed software lists was the main key but the tool seems to have grown much larger than first anticipated and it now does many other helpful functions as they were requested by people over the years.

Please make sure you are allowed to use this tool on your domain and have read this help file and the disclaimer at the bottom of this file thoroughly before continuing!

This tool Encrypts every "Windows management connection" it makes with packet.privacy and every "Powershell connection" it makes, so your "Admin Credentials" stay safe across the network.

This tool was written in VB.Net which requires .NET 4.0 to be on the running Administrators PC (or server) where the tool is being run from. Windows 8/10/11 or Server 2012/2016/2019 has this by default. This tool supports Microsoft Windows OS only.

Any feedback good or bad welcome: Please email <u>RemoteDiagnosticsTool@outlook.com</u>. Improvements and refinements are always being made. Please check the web for a copy of the latest version which may just have the fix or added information you requested already.

Donations Welcome Via Paypal: We can accept Visa / Mastercard etc...

Thank you for your support. I hope this tool aids your daily remote working and Administration tasks.

Main tool functions:

The tool has been split into many tabs and buttons to ease use of functions as can be seen when launched.

When you launch this tool you will be defaulted to the Main screen once you have entered your required domain login details.

Main connection screen for Adding / Removing / Pinging / Connecting to a PC and to be able to interrogate it. (Right Click in left panel)

- Pinged Online PC.
- Pinged Offline computer.
- Change your connecting username and password and domain information.
- Force a restart of the remote PC.
- Open the \\ Remote PC \ C\$ drive in one click.
- Check the Antivirus version and status of the remote PC.
- Defrag the remote PC C Drive.
- Open the Eventlog of the remote PC.
- Gather information about Microsoft's APP-V client if installed on the remote PC, Version 4.x and 5.x
- Connect to Microsoft's built in "Manage Computer" settings of the remote PC.
- Open the Microsoft "registry editor" so you can connect to the remote PC registry.
- NLTest what logon server the Remote PC used at logon.
- NSLookup machine IP addresses list (Sometimes laptops and tablets have multiple) you can use the IP to connect too.
- Connect to a Microsoft "PowerShell session" on the remote PC.
- RDT registry Editor, Shows HKLM and HKCU (of the logged on user selected on the HOME.)
- Run a Microsoft "RDP connection" to the remote PC.
- Etart-up List viewer: gives an overview of all starting actions on the remote PC (Run / Shell / network / print).
- Task Schedule allows you to connect to a remote PC and see what scheduled tasks are setup.
- You Can also run any command specified directly on the remote PC if required. Just enter the command e.g. CMD.EXE /C Del /F /Q C:\temp*.*
- "Shadow Desktop" Button is used to ask a user if you can view their desktop session, so they can show you errors and issues. (MSTSC)



Interrogates these features:

• Get basic pc details: (Includes site, Internet Explorer version, JAVA version that is currently plugged into IE, domain, Hardware driver versions for video and network cards, memory and OS values, Etc.

<u>AD</u>

DISK

DOTNET

Execute

Readonly - shows All AD Users and Computers - shows All AD Groups - shows selected Group members.

when connected to a PC via **right-click "connect > "** button, you can use the DISK tab to interrogate further the partitions and what actual disks are installed on the PC. Check what free space is available. In addition, you can choose to move the swap file to the D or E partition if the space is low on c partition. (NOTE: there is no disk space checking done for the swap file move, if you try to move the swap file to the D partition that doesn't exist you could make the machine NON-bootable, use with caution!)

Once connected to a PC via right-click "connect > " button, you can use the .NET tab to list any "DotNET Core" or "DotNET Framework" versions installed on the PC.

Use this tab to connect to a server share and install (or remove) a package. There are 2 methods that can be used on this tab. 1) Powershell run without a drive letter needed. Copies file to machine (Robocopy) then runs the install locally.

2) Powershell run with a drive letter of choice. Copies file locally (WMI) and then installs locally.

(Setup.exe /s) or package script (install.bat) or (mytestscript.vbs) or (msiexec.exe xxxx.msi /qn) etc can be used.

NOTE: The A: drive mapping is used here by default (can be changed) while it performs the actions.

Please wait for the install / remove to happen, a visible indicator runs whilst these actions are performed.

Note: User messages and pop-ups will halt the install or removal routines. Make sure there no pauses or pop-up messages in the routines. Make sure the routines are "NOT" user interactive before running them.

Please make sure there is enough disk space for these actions before performing them. Be Warned!

FType

when connected to a PC via right-click "connect > " button, you can use the file types tab to list the machines file types.

Groups

when connected to a PC via **right-click "connect > "** button, you can use the GROUPS tab to list the local groups and add domain groups to local groups / Add local user etc...

Installed

You can use the INSTALLED tab to list the installed software on the PC (same as ADD/REMOVE programs). You can remove selected software from here by the way of a push of a button. Also shows hidden software not listed usually (MSI removal only). Use Install / Remove tab to run package Installs / removals or scripts etc.

KB-Installed

Once connected to a PC via right-click "connect > " button, you can use this tab to list any "other hotfixes" or "Microsoft KB Patches" installed on the PC and when they got there. Uninstall any KB selected (Win7 or newer only).

KB-Missing

Once connected to a PC via right-click "connect > " button, you can use this tab to list any "missing hotfixes" or "Microsoft KB Patches" needed on the PC. This takes a minimum of 2 minute to run so please be patient!

MBSA

Once connected to a PC via right-click "connect > " button, you can use the MBSA tab to run a "Microsoft Baseline Security Analyzer" report to see if the remote computer is missing any security updates for products or the operating system. This is done with the help of the file "Scan-UpdatesOffline.zip" (Available from the RDT website) which contains the following files: wsusscn2.cab from Microsoft and the modified file Scan-UpdatesOffline.ps1 from Microsoft to work with RDT specifically.

MSI

Once connected to a PC via right-click "connect >" button, you can use the MSI List tab to remove a selected MSI.

Processor

shows a snapshot in time (via perf counters) of CPU usage of the remote PC. (Note: Click the button to manually refresh

the list.)

Profiles

Provides details for profiles in use and their sizes. Profile deletion is also available like in AdvancedSystemSettings.

Reboot?

Added a reboot detection tab to help see if a reboot is needed on the remove PC.

SCCM

when connected to a PC via right-click "connect > " button, you can use the SCCM tab to find out what SCCM jobs have been run on the remote PC, trigger a "client action task" and many other SCCM tasks including the re-running of an Advert (Machine based or User based).

Execution History provides a list of tried Executions whilst the Advertisements tab provides what packages have been downloaded to the PC. View running SCCM tasks and Client information.

Added SCCM Remote Commands tab to allow remote trigger of the SCCM client inventory tasks.

Added SCCM patch missing tab to detect missing SCCM applied patches.

Added SCCM patch Installed tab to detect Installed SCCM applied patches.

Services

when connected to a PC via right-click "connect > " button, you can use the SERVICES tab to start / stop / set to manual / set to automatic and Delete services on the remote PC. (Use caution when using the Delete Services button as this will delete a service permanently).

Task-Manager

when connected to a PC, you can use the TASK MANAGER tab to list the processes running on the remote PC (via WMI). You can also kill a remote process if required. (Handy for looking to see if the user is running word2010 or excel2003)

User

shows the logged on "users" printers, what network drives they have connected and ODBC Connections the user has setup. Also shown is what keyboard layout they are currently using. Select the user via the "User selection on Begin page".

WIM_3rd_Party_Drivers shows the non-Microsoft drivers installed on the remote computer

WIM OptionalFeatures shows the Windows OS Features that are currently installed and that they are Enabled or Disabled.



this is for 1E Nomad and PXE agent diagnostics information.

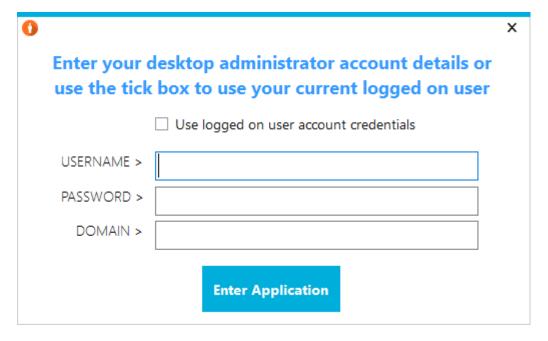
Print Screen Button

this button will take a snapshot of the RDT application screen when clicked. (alt print)

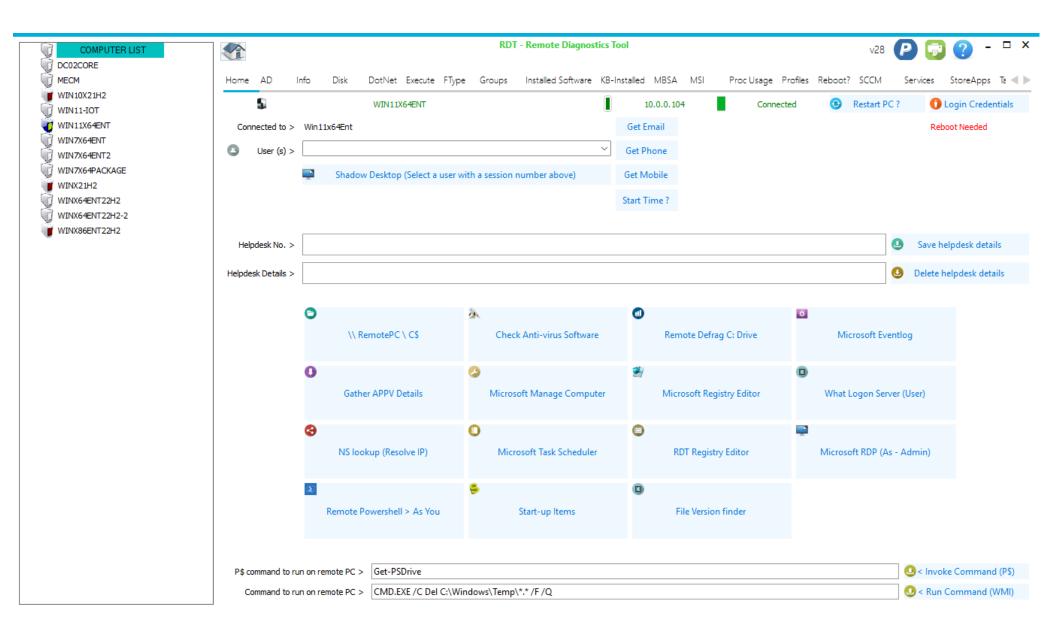


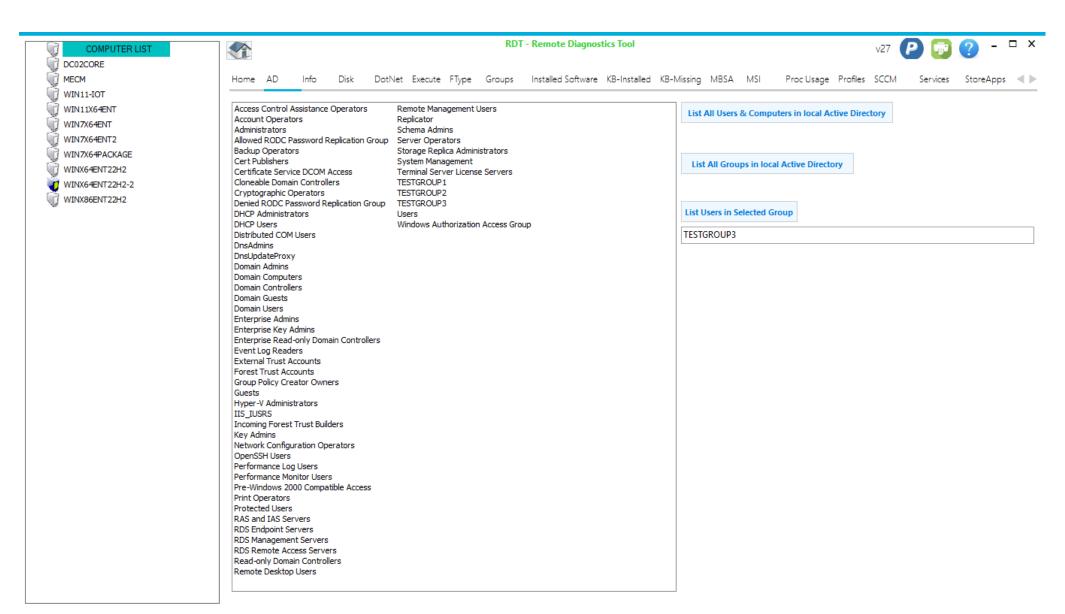
is seen on many pages and can be used to generate an excel export of the tabled information on the page selected. This file is usually saved in a file called %appdata%\export.xls

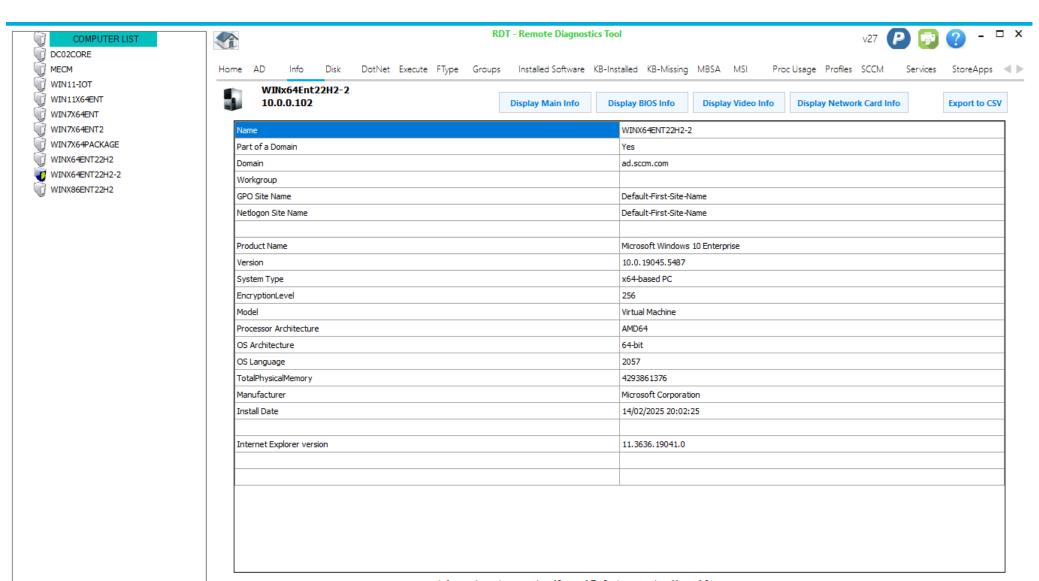
Example screen shots >



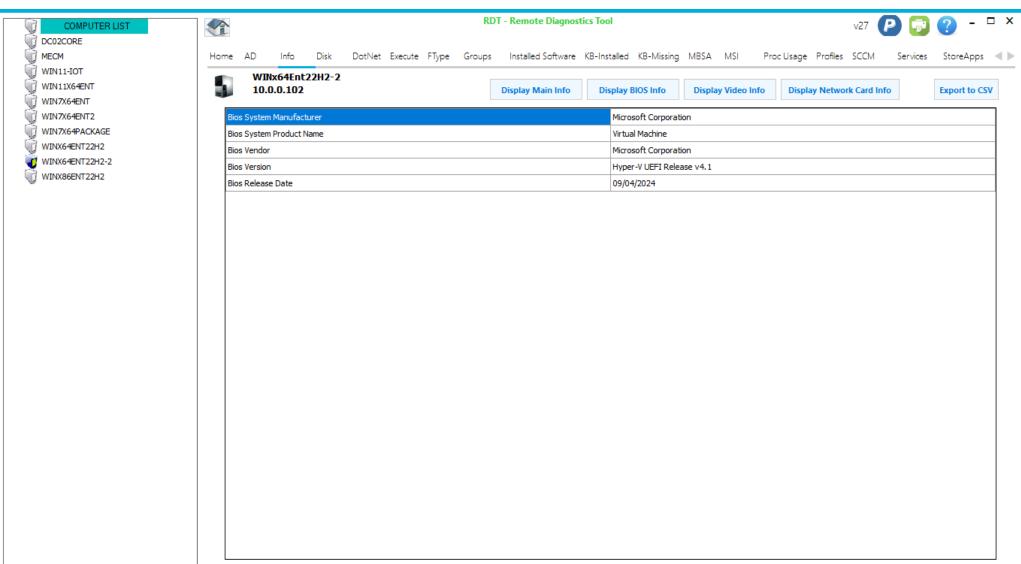
Note: to use the "logged on Users" details tick the box provided at launch.



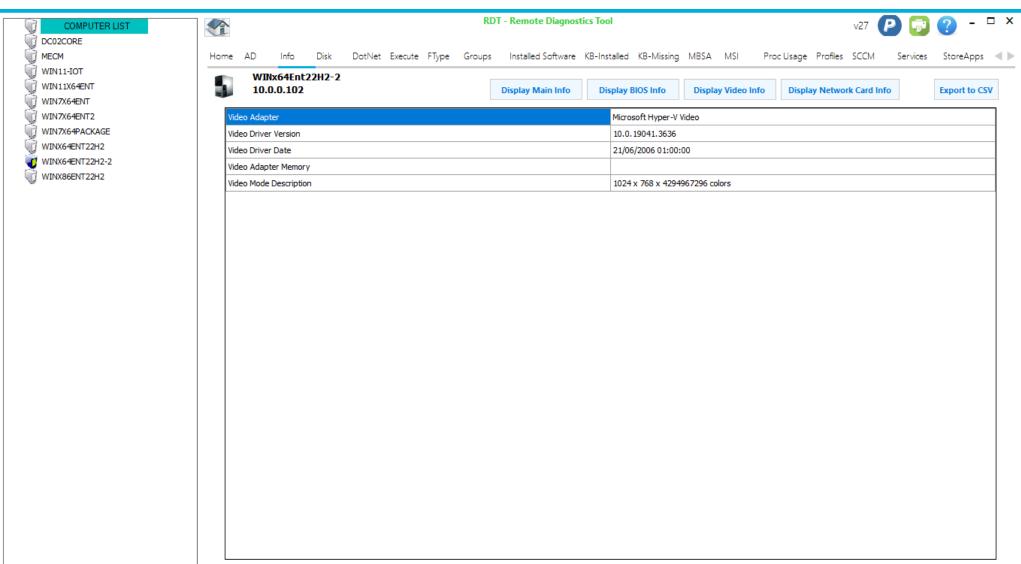




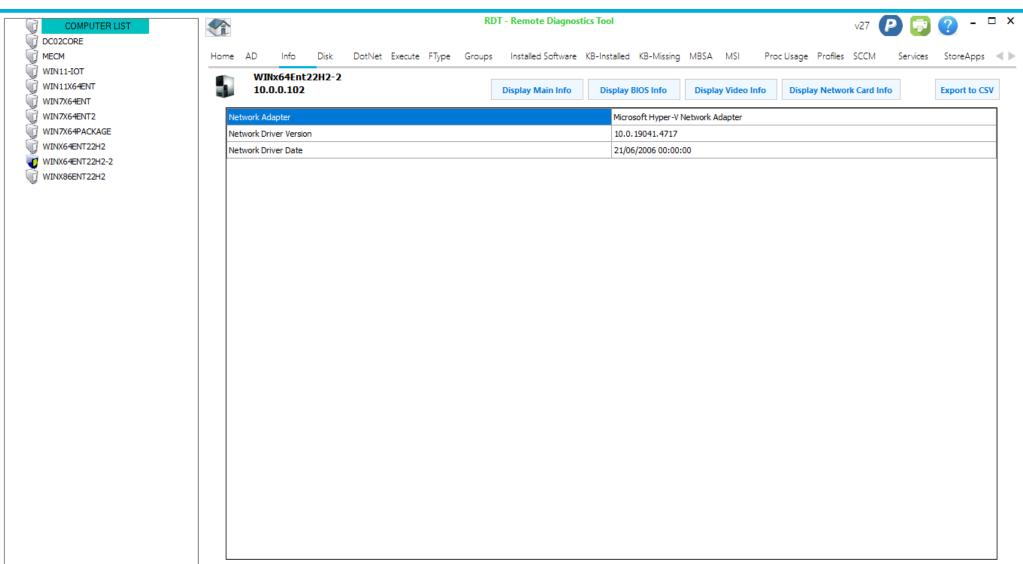
Information: Java version 10. x = 1.7 & Java version 11. x = 1.8



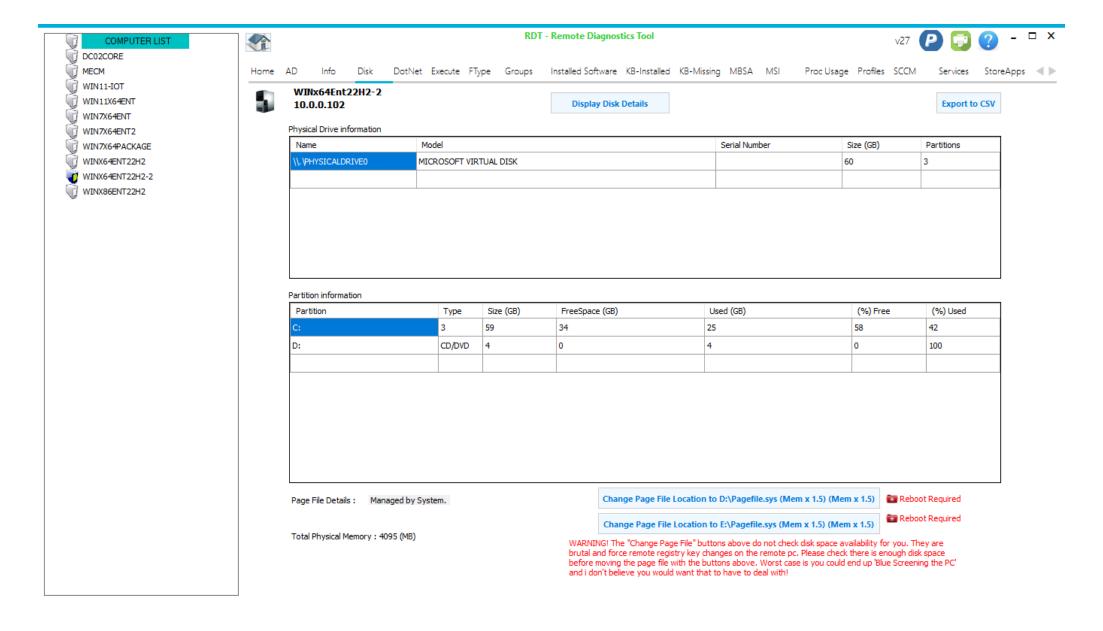
Information: Java version 10. x = 1.7 & Java version 11.x = 1.8

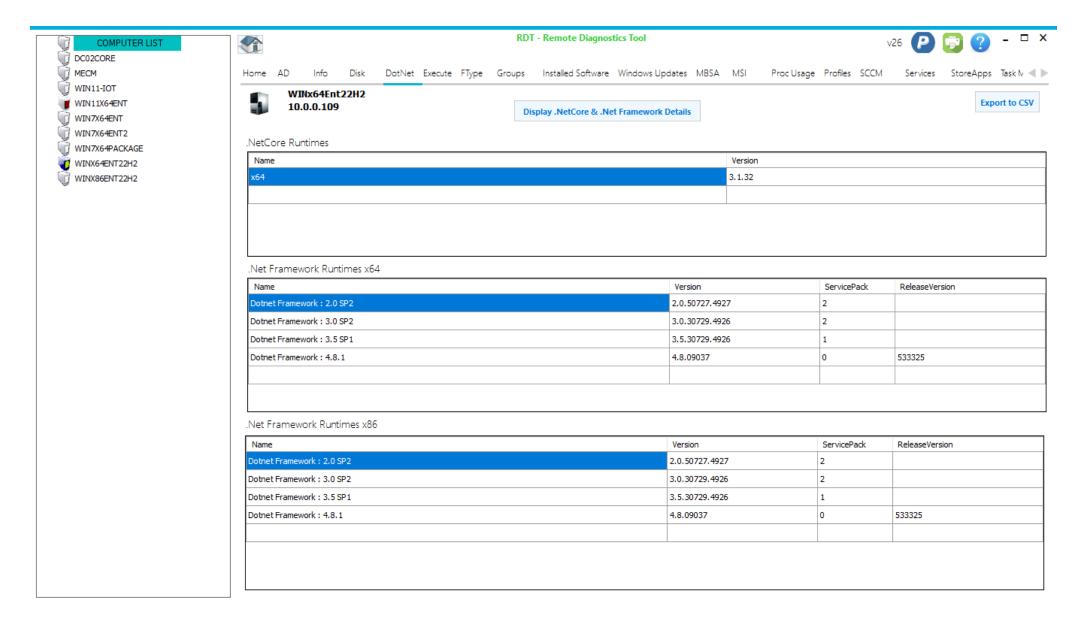


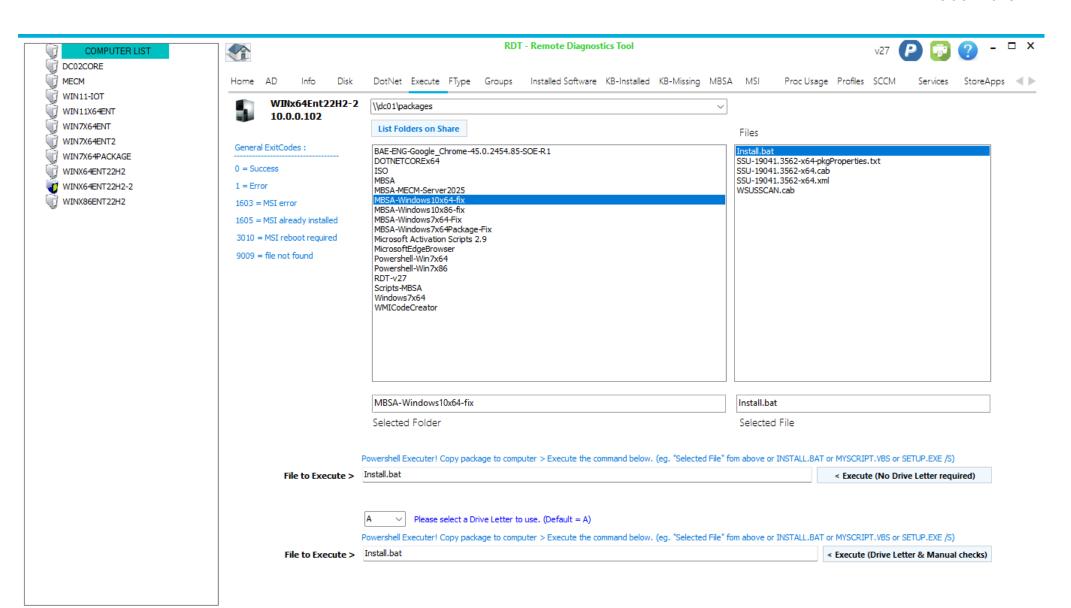
Information: Java version 10. x = 1.7 & Java version 11.x = 1.8

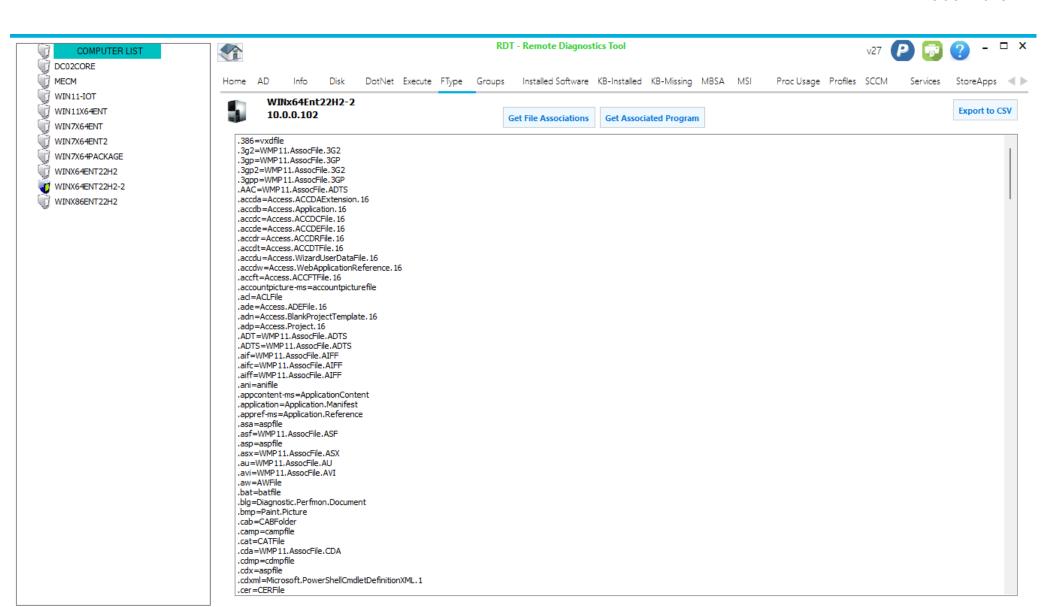


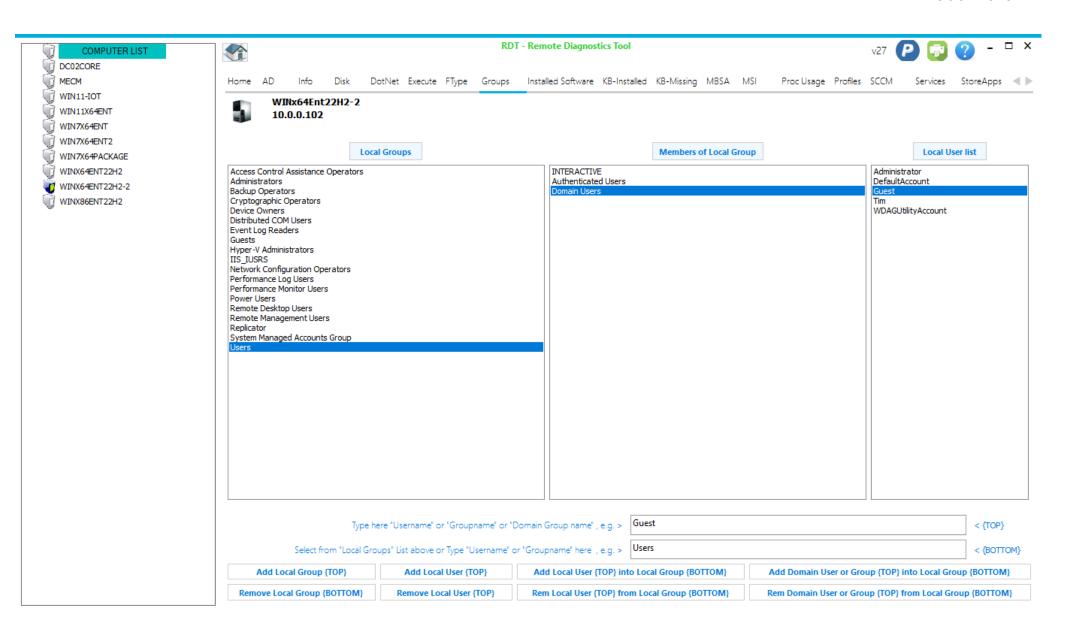
Information: Java version 10. x = 1.7 & Java version 11.x = 1.8





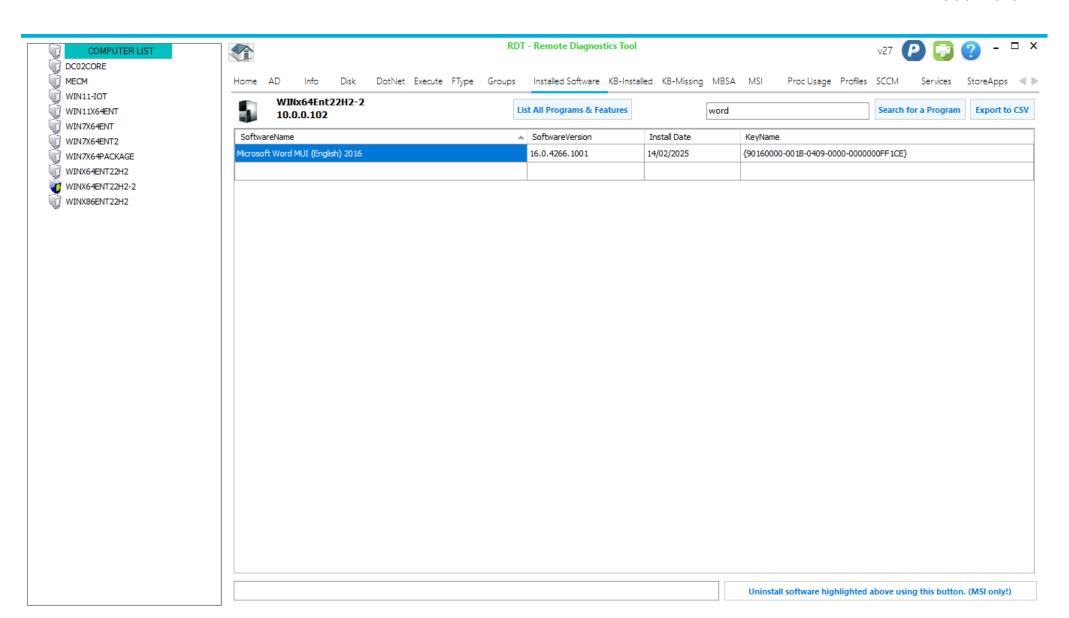


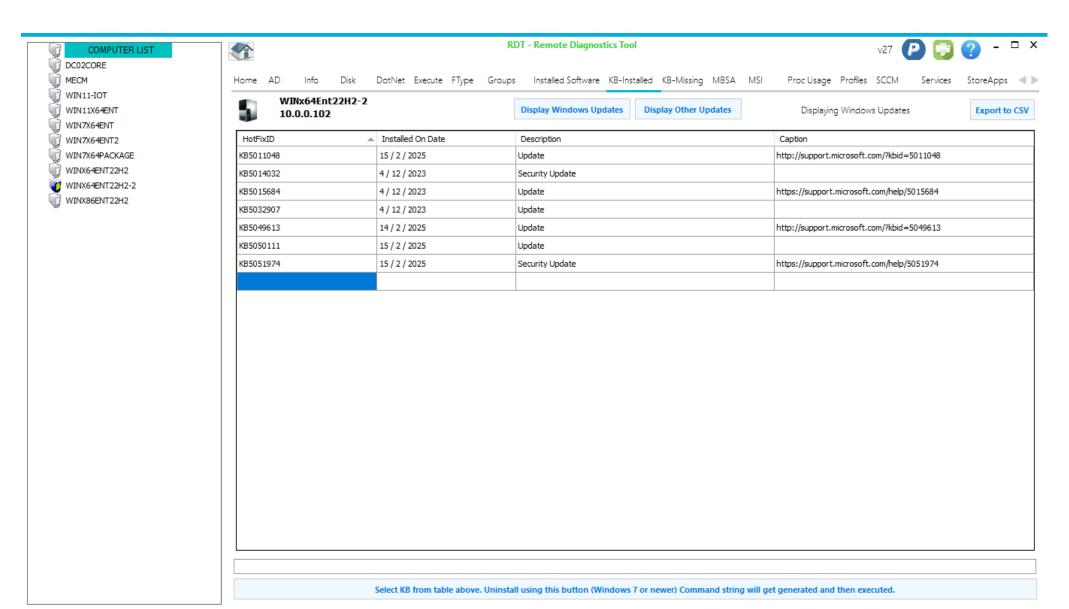


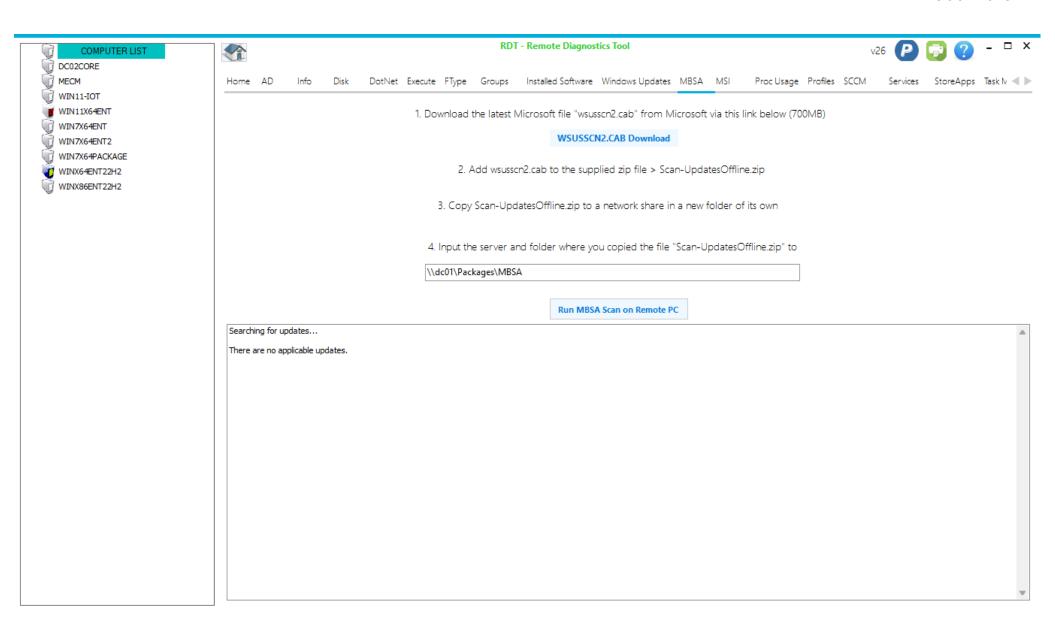


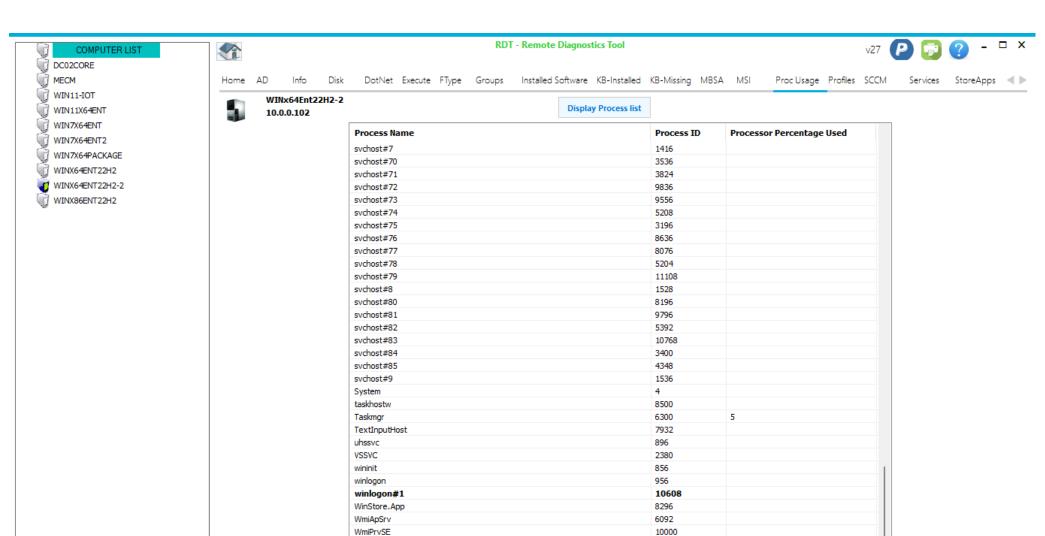
Uninstall software highlighted above using this button. (MSI only!)

COMPUTER LIST		RDT - Remote Diagnostics Too	ıl		v27 P	? - 🗆	
DC02CORE MECM	Home AD Info Disk DotNet Execute FType Gro	ups Installed Software KB-Ins	talled KB-Missing MBS	A MSI Proc Usage Profile:	s SCCM Services	StoreApps <	
WIN11-IOT WIN11X64ENT	WINx64Ent22H2-2 10.0.0.102	List All Programs & Features	Searc	h	Search for a Program	Export to CS\	
WIN7X64ENT WIN7X64ENT2	SoftwareName	▲ SoftwareVersion	Install Date	KeyName			
WIN7X64PACKAGE	Herramientas de corrección de Microsoft Office 2016: español	16.0.4266.1001	14/02/2025	{90160000-001F-0C0A-0000-00000	00FF1CE}		
WINX64ENT22H2	Microsoft Access MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0015-0409-0000-0000000FF1CE}			
WINX64ENT22H2-2	Microsoft Access Setup Metadata MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0117-0409-0000-000000	00FF1CE}	F1CE}	
WINX86ENT22H2	Microsoft DCF MUI (English) 2016	16.0.4266.1001	16.0.4266.1001 14/02/2025 {90160000-0090-0409-0000-0000000FF				
	Microsoft Edge	133.0.3065.59	14/02/2025	Microsoft Edge			
	Microsoft Edge WebView2 Runtime	133.0.3065.59	14/02/2025	Microsoft EdgeWebView			
	Microsoft Excel MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0016-0409-0000-000000	00FF1CE}		
	Microsoft Groove MUI (English) 2016	14/02/2025	{90160000-00BA-0409-0000-0000000FF1CE}				
	Microsoft InfoPath MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0044-0409-0000-000000	00FF1CE}		
	Microsoft Office 64-bit Components 2016	16.0.4266.1001	14/02/2025	{90160000-002A-0000-1000-00000	00FF1CE}		
	Microsoft Office OSM MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-00E1-0409-0000-0000000FF1CE}			
	Microsoft Office OSM UX MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-00E2-0409-0000-000000	00FF1CE}		
	Microsoft Office Professional Plus 2016	16.0.4266.1001	14/02/2025	{90160000-0011-0000-0000-000000	00FF1CE}		
	Microsoft Office Professional Plus 2016	16.0.4266.1001		Office 16.PROPLUS			
	Microsoft Office Proofing (English) 2016	16.0.4266.1001	14/02/2025	{90160000-002C-0409-0000-00000	00FF1CE}		
	Microsoft Office Proofing Tools 2016 - English	16.0.4266.1001	14/02/2025	{90160000-001F-0409-0000-000000	00FF1CE}		
	Microsoft Office Shared 64-bit MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-002A-0409-1000-00000	00FF1CE}		
	Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0116-0409-1000-000000	00FF1CE}		
	Microsoft Office Shared MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-006E-0409-0000-000000	00FF1CE}		
	Microsoft Office Shared Setup Metadata MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0115-0409-0000-000000	00FF1CE}		
	Microsoft OneNote MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-00A1-0409-0000-00000	00FF1CE}		
	Microsoft Outlook MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-001A-0409-0000-00000	00FF1CE}		
	Microsoft PowerPoint MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0018-0409-0000-000000	DOFF1CE}		
	Microsoft Publisher MUI (English) 2016	16.0.4266.1001	14/02/2025	{90160000-0019-0409-0000-000000	00FF1CE}		









9824

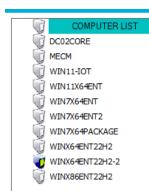
7032

11164

WmiPrvSE#1

WmiPrvSE#2

WUDFHost



RDT - Remote Diagnostics Tool

27 **P**







Home AD Info Disk DotNet Execute FType Groups Installed Software KB-Installed KB-Missing MBSA MSI Proc Usage Profiles SCCM Services StoreApps

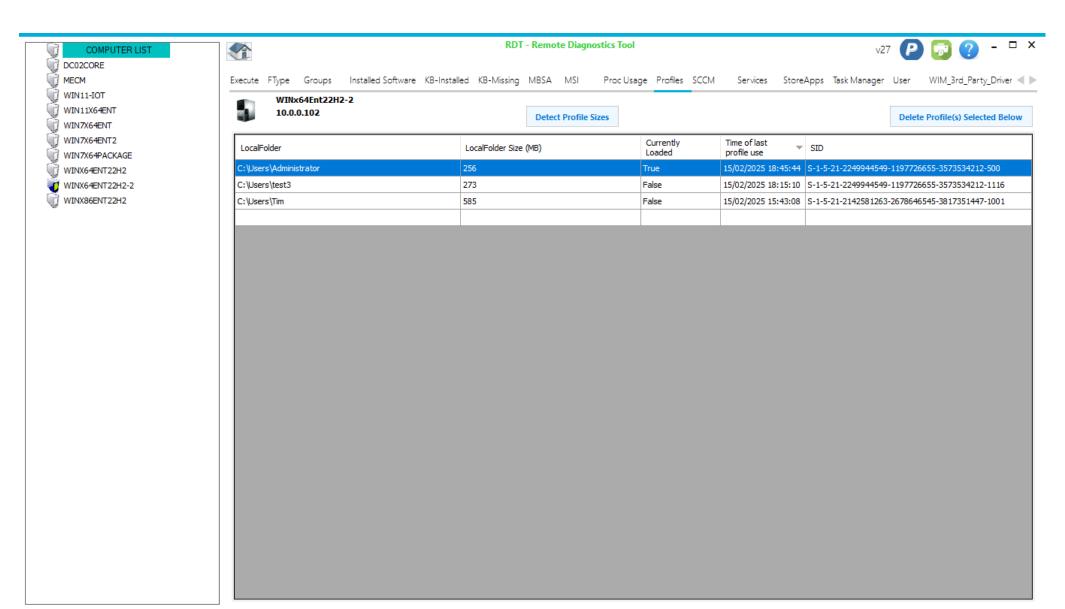
١.	WINx64Ent22H2-2
4	10.0.0.102

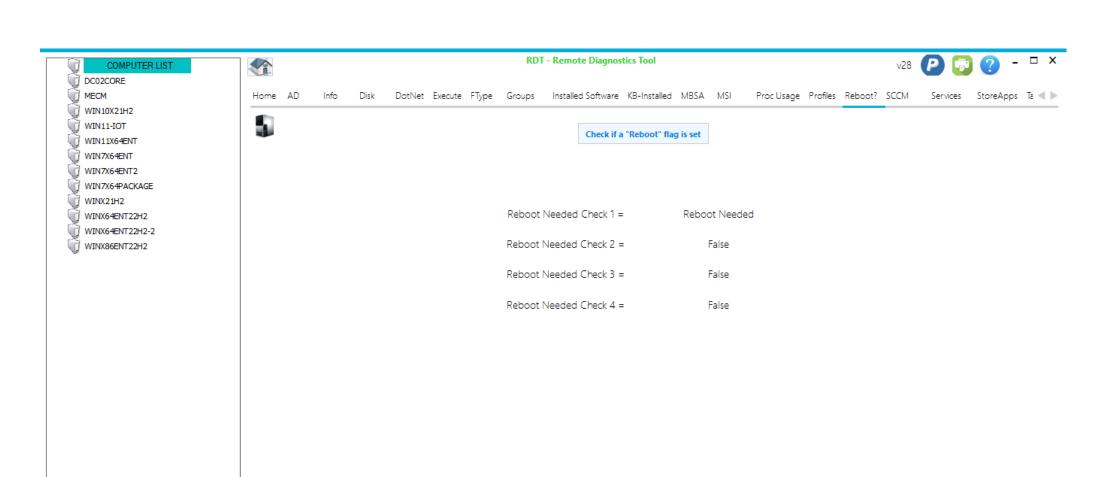
Display MSI List

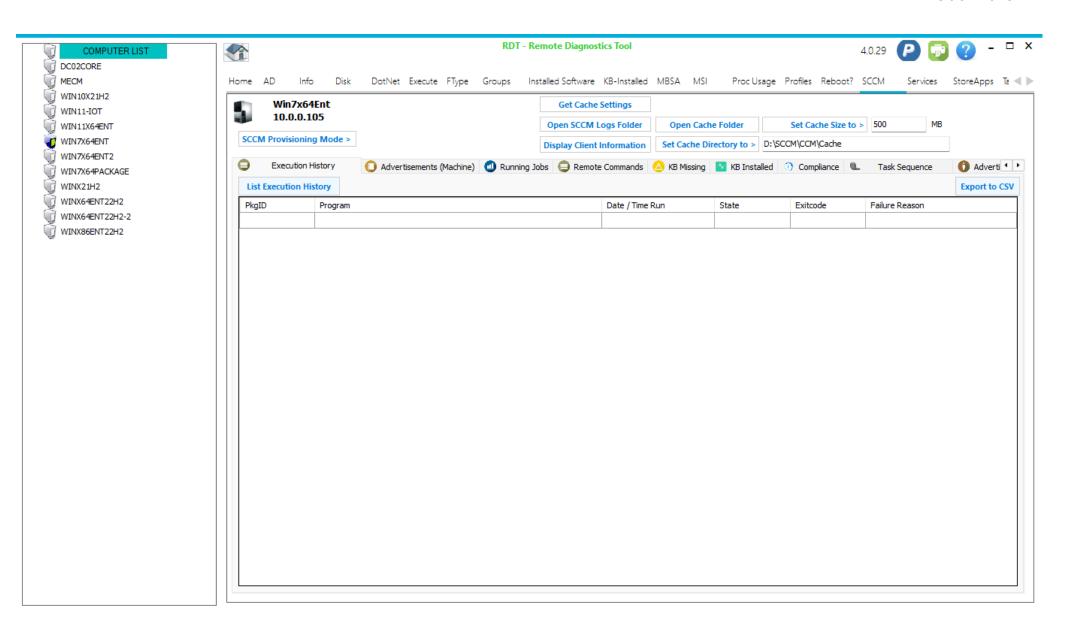
Export to CSV

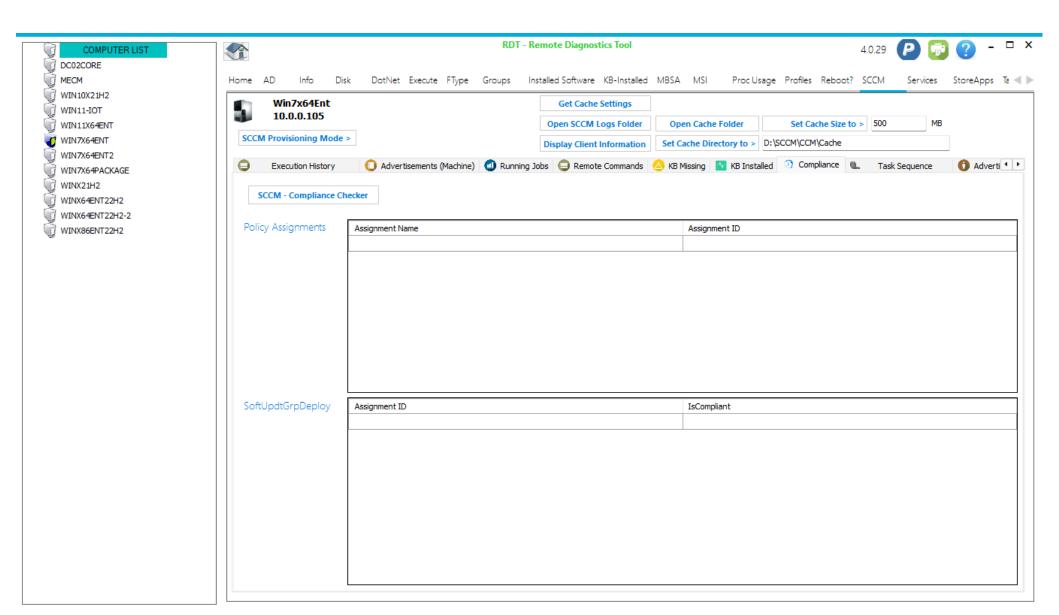
MSI Application Name	Version	MSI filename	(dd/mm/yyyy) MSI First Install Date
Herramientas de corrección de Microsoft Office 2016: español	16.0.4266.1001	C:\Windows\Installer\43ee9.msi	14/02/2025 22:32:44
Microsoft Access MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ea9.msi	14/02/2025 22:32:47
Microsoft Access Setup Metadata MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ead.msi	14/02/2025 22:32:47
Microsoft DCF MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43eb9.msi	14/02/2025 22:32:50
Microsoft Excel MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ebd.msi	14/02/2025 22:32:50
Microsoft Groove MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ec1.msi	14/02/2025 22:32:51
Microsoft InfoPath MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ec5.msi	14/02/2025 22:32:51
Microsoft Office 64-bit Components 2016	16.0.4266.1001	C:\Windows\Installer\43e98.msi	14/02/2025 22:30:24
Microsoft Office OSM MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43eb5.msi	14/02/2025 22:32:50
Microsoft Office OSM UX MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ed5.msi	14/02/2025 22:32:53
Microsoft Office Professional Plus 2016	16.0.4266.1001	C:\Windows\Installer\43eee.msi	14/02/2025 22:30:30
Microsoft Office Proofing (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ea5.msi	14/02/2025 22:32:39
Microsoft Office Proofing Tools 2016 - English	16.0.4266.1001	C:\Windows\Installer\43ea1.msi	14/02/2025 22:32:39
Microsoft Office Shared 64-bit MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43e8f.msi	14/02/2025 22:30:24
Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43e93.msi	14/02/2025 22:30:24
Microsoft Office Shared MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ecd.msi	14/02/2025 22:32:51
Microsoft Office Shared Setup Metadata MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ed1.msi	14/02/2025 22:32:51
Microsoft OneNote MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43eb1.msi	14/02/2025 22:32:48
Microsoft Outlook MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ed9.msi	14/02/2025 22:32:54
Microsoft PowerPoint MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43edd.msi	14/02/2025 22:32:54
Microsoft Publisher MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ee1.msi	14/02/2025 22:32:55
Microsoft Skype for Business MUI (English) 2016	16.0.4266.1001	C:\Windows\Installer\43ec9.msi	14/02/2025 22:32:51
ALL LINE WITE I	0.74.0.0	Clur I I I I I I I I I I I I I I I I I I I	05/00/0000 00 00 40

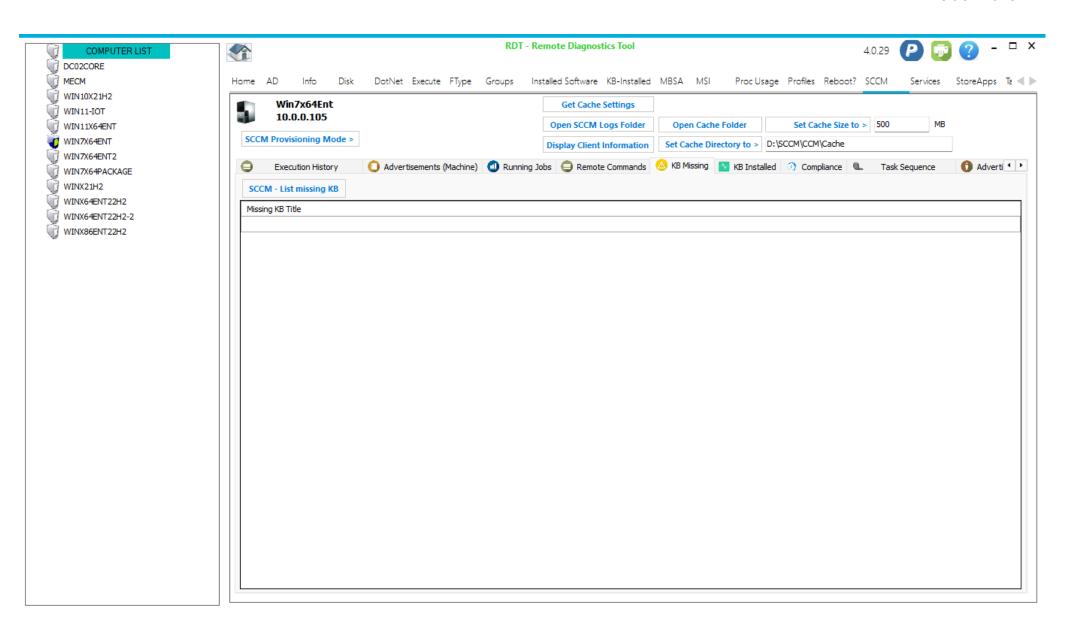
Select any MSI from table above, then Uninstall using the command here /\ . Log file generated = C:\Windows\Installer\MSI_Removal.log

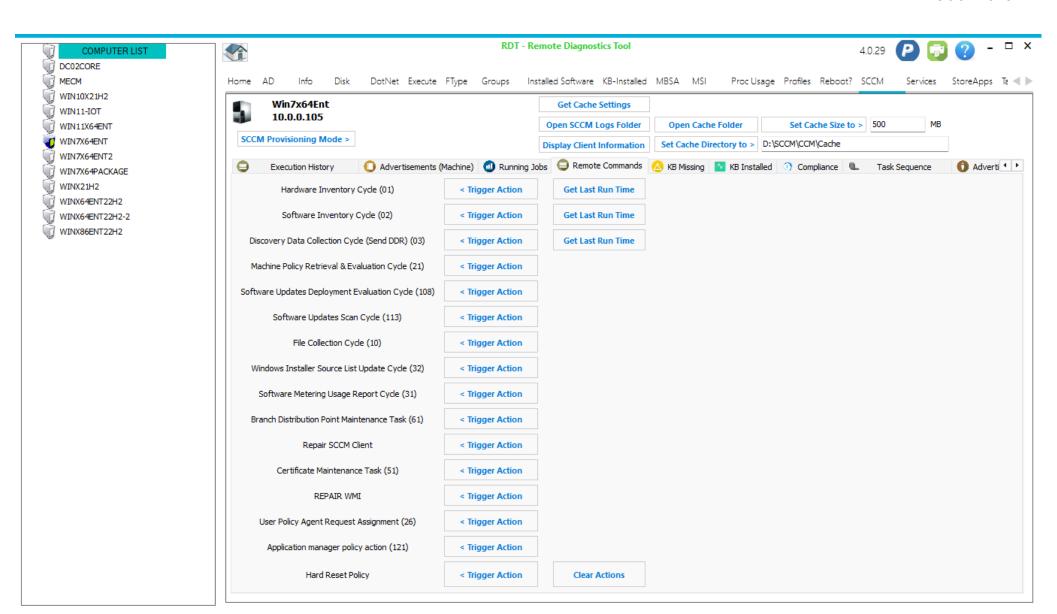


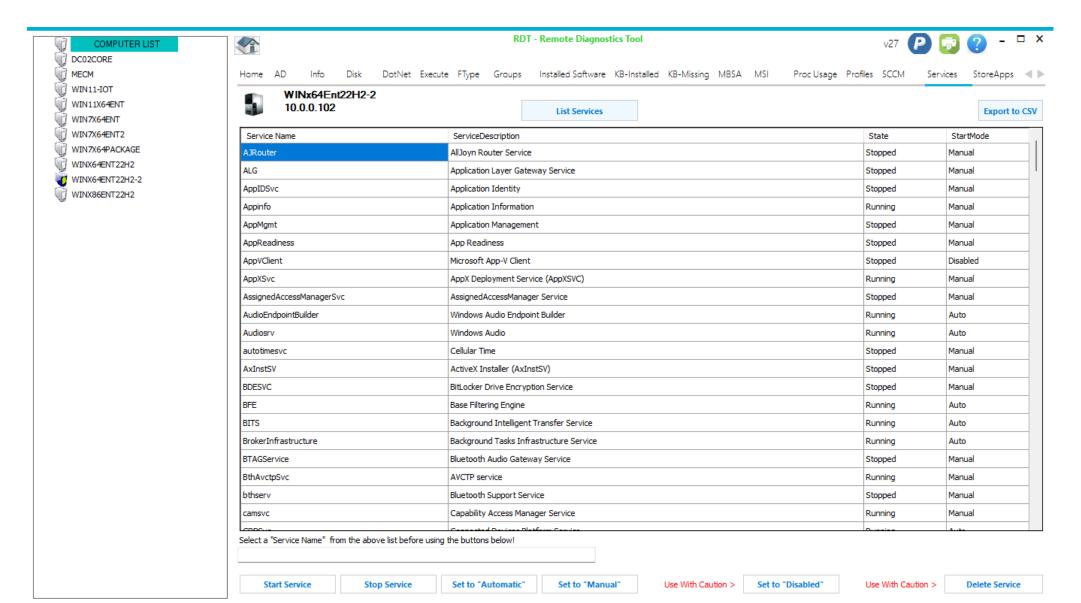












COMPUTER LIST
DC02CORE
MECM
WIN11-IOT
WIN11X64ENT
WIN7X64ENT2
WIN7X64ENT2
WIN7X64PACKAGE
WINX64ENT22H2
WINX64ENT22H2
WINX64ENT22H2-2
WINX86ENT22H2

RDT - Remote Diagnostics Tool

/27 🔑







AD Info Disk DotNet Execute FType Groups Installed Software KB-Installed KB-Missing MBSA MSI Proc Usage Profiles SCCM Services StoreApps Task Man 🔻 🕨

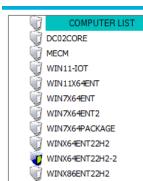


WINx64Ent22H2-2 10.0.0.102

Display Store Apps

Export to CSV

Name	Version	Architecture	ProgramId	Language	Vendor
1527c705-839a-4832-9118-54d4Bd6a0c89	10.0.19041.3636	Neutral	1527c705-839a-4832-9118-54d4Bd	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
1527c705-839a-4832-9118-54d4Bd6a0c89	10.0.19041.4239	Neutral	1527c705-839a-4832-9118-54d4Bd	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
:5e2524a-ea46-4f67-841f-6a9465d9d515	10.0.19041.3636	Neutral	c5e2524a-ea46-4f67-841f-6a9465	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
c5e2524a-ea46-4f67-841f-6a9465d9d515	10.0.19041.4239	Neutral	c5e2524a-ea46-4f67-841f-6a9465	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
E2A4F912-2574-4A75-9BB0-0D023378592B	10.0.19041.3636	Neutral	E2A4F912-2574-4A75-9BB0-0D023	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
E2A4F912-2574-4A75-9BB0-0D023378592B	10.0.19041.4239	Neutral	E2A4F912-2574-4A75-9BB0-0D023	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE	10.0.19041.3636	Neutral	F46D4000-FD22-4DB4-AC8E-4E1D	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE	10.0.19041.4239	Neutral	F46D4000-FD22-4DB4-AC8E-4E1D	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washin
Microsoft. 54998 1C3F5F10	1.1911.21713.0	X64	Microsoft.549981C3F5F10_1.1911	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.AAD.BrokerPlugin	1000.19041.36	Neutral	Microsoft.AAD.BrokerPlugin_1000	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.AAD.BrokerPlugin	1000.19041.42	Neutral	Microsoft.AAD.BrokerPlugin_1000	0	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.AccountsControl	10.0.19041.3636	Neutral	Microsoft.AccountsControl_10.0.19	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.AccountsControl	10.0.19041.4239	Neutral	Microsoft.AccountsControl_10.0.19	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.Advertising.Xaml	10.1808.3.0	X64	Microsoft.Advertising.Xaml_10.180	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.AsyncTextService	10.0.19041.3636	Neutral	Microsoft.AsyncTextService_10.0	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.AsyncTextService	10.0.19041.4239	Neutral	Microsoft.AsyncTextService_10.0	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.BingWeather	4.25.20211.0	X64	Microsoft.BingWeather_4.25.2021	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.BioEnrollment	10.0.19041.3636	Neutral	Microsoft.BioEnrollment_10.0.1904	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.BioEnrollment	10.0.19041.4239	Neutral	Microsoft.BioEnrollment_10.0.1904	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft, Copilot	0.4.2.0	Neutral	Microsoft.Copilot_0.4.2.0_neutral	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft, CredDialogHost	10.0.19041.4239	Neutral	Microsoft.CredDialogHost_10.0.19	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft, CredDialogHost	10.0.19041.3636	Neutral	Microsoft.CredDialogHost_10.0.19	1033	CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washir
Microsoft.DesktopAppInstaller	1.0.30251.0	X64	Microsoft.DesktopAppInstaller_1.0	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.ECApp	10.0.19041.4597	Neutral	Microsoft.ECApp_10.0.19041.4597	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was
Microsoft.ECApp	10.0.19041.3636	Neutral	Microsoft.ECApp 10.0.19041.3636	1033	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Was



RDT - Remote Diagnostics Tool









Info Disk DotNet Execute FType Groups Installed Software KB-Installed KB-Missing MBSA MSI Proc Usage Profiles SCCM Services StoreApps Task Manager Us 🬗



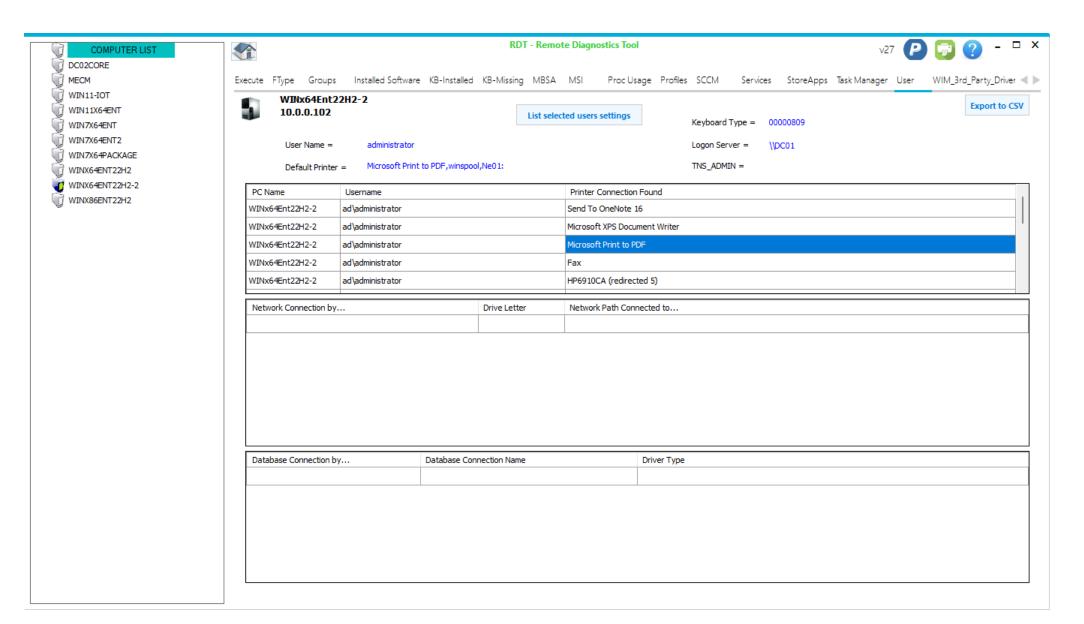
WINx64Ent22H2-2 10.0.0.102

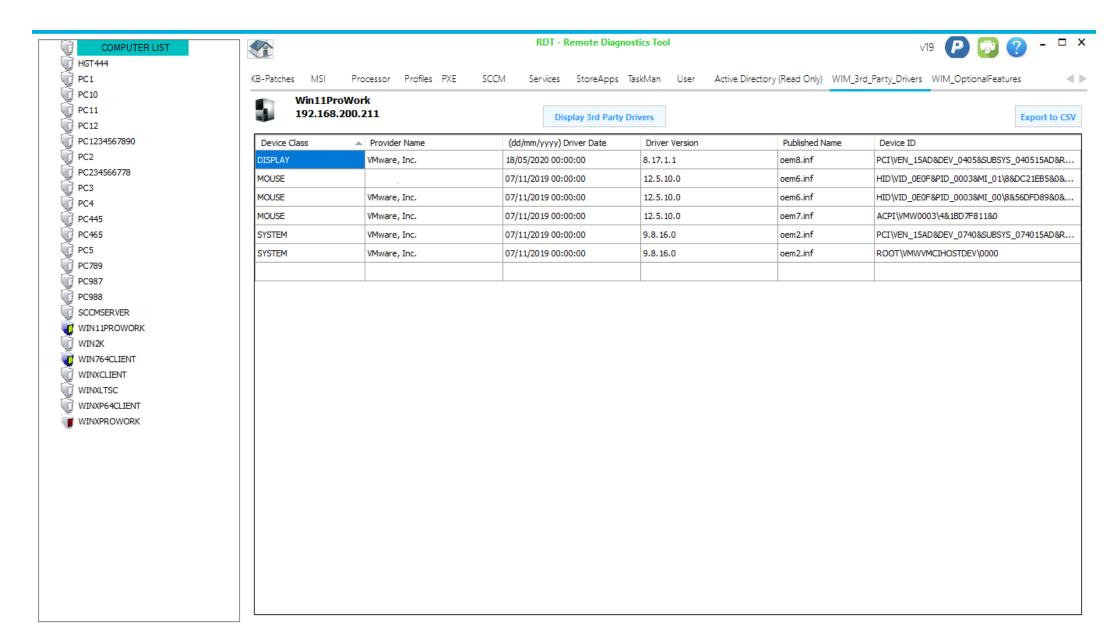
Display Full Process List

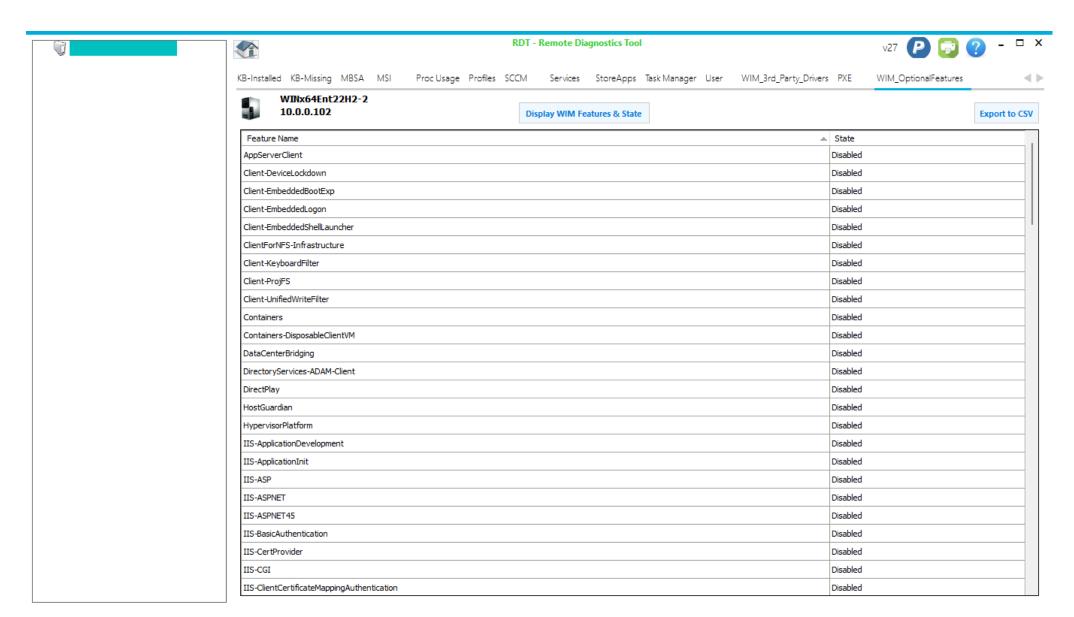
End selected process

Export to CSV

Process Name	Process ID	WhoRun	Exepath	
AggregatorHost.exe	5160	NT AUTHORITY\SYSTEM	C:\Windows\System32\AggregatorHost.exe	
ApplicationFrameHost.exe	8820	AD\Administrator	C:\Windows\system32\ApplicationFrameHost.exe	
ccmsetup.exe	7872	NT AUTHORITY\SYSTEM	C:\Windows\ccmsetup\ccmsetup.exe	
csrss.exe	780	NT AUTHORITY\SYSTEM		
csrss.exe	864	NT AUTHORITY\SYSTEM		
csrss.exe	10524	NT AUTHORITY\SYSTEM		
ctfmon.exe	4448	AD\Administrator	C:\Windows\system32\ctfmon.exe	
dllhost.exe	5028	NT AUTHORITY\SYSTEM	C:\Windows\system32\DllHost.exe	
dllhost.exe	9448	AD\Administrator	C:\Windows\system32\DllHost.exe	
dwm.exe	1944	Window Manager\DWM-1	C:\Windows\system32\dwm.exe	
dwm.exe	10800	Window Manager\DWM-4	C:\Windows\system32\dwm.exe	
explorer.exe	10220	AD\Administrator	C:\Windows\Explorer.EXE	
fontdrvhost.exe	1088	Font Driver Host\UMFD-1	C:\Windows\system32\fontdrvhost.exe	
fontdrvhost.exe	1096	Font Driver Host\UMFD-0	C:\Windows\system32\fontdrvhost.exe	
fontdrvhost.exe	10744	Font Driver Host\UMFD-4	C:\Windows\system32\fontdrvhost.exe	
.ogonUI.exe	10696	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe	
sass.exe	1008	NT AUTHORITY\SYSTEM	C:\Windows\system32\sass.exe	
Memory Compression	3132	NT AUTHORITY\SYSTEM		
MicrosoftEdgeUpdate.exe	3464	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	
MoUsoCoreWorker.exe	9444	NT AUTHORITY\SYSTEM	C:\Windows\System32\mousocoreworker.exe	
MpDefenderCoreService.exe	4208	NT AUTHORITY\SYSTEM		
MsMpEng.exe	4200	NT AUTHORITY\SYSTEM		
NisSrv.exe	5872	NT AUTHORITY\LOCAL SERVICE		
OneDrive.exe	1392	AD\Administrator	C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe	
rdpclip.exe	11156	AD\Administrator	C:\Windows\System32\rdpclip.exe	
Registry	148	NT AUTHORITY\SYSTEM		
RuntimeBroker.exe	2868	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
RuntimeBroker.exe	7600	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
RuntimeBroker.exe	5996	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
RuntimeBroker.exe	1684	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
RuntimeBroker.exe	2260	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
RuntimeBroker.exe	4836	AD\Administrator	C:\Windows\System32\RuntimeBroker.exe	
SearchApp.exe	6712	AD\Administrator	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	
SearchApp.exe	10368	AD\Administrator	C:\Windows\SystemApps\Microsoft,Windows.Search cw5n1h2txyewy\SearchApp.exe	







Example tab generated by pressing the Get APPV button on the HOME tab:

App-V Version : 4.6.3.	Remote CMD (As you)	
Cache Details Packages Shortcuts	Appv 4.6 Commands	
Total Size of APPV Cache =	12454	
File Size of APPV Cache =	9	
Percentage free of APPV Cache =	100% Free.	
Amount of APPV Cache used =		
APPV Cache Location >	C:\Documents and Settings\All Users\Documents\SoftGrid Client\sftfs.fsd	
APPV Min Free Disk Space >	0 0	

App-V Version: 4.6.3.24870 on: SCCMXP

Remote CMD (As you)

Cache Details Packages Shortcuts Appv 4.6 Commands

(CF6ACE9E-7BE1-4B14-BAB0-03B 1 CF6ACE9E-7BE1-4B14-BAB False False 8814592 file://C:\Docume	nts and Settings\Administrator.SCCM\Desktop\Package
	its and Settings violininistrator. See in Desktop (Lackage

App-V Version: 4.6.3.24870 on: SCCMXP

Remote CMD (As you)

Cache Details Packages Shortcuts Appv 4.6 Commands

	_					
Shortcut	*	Version	LastLaunchOnSystem	PackageGUID	Loading	OriginalOsdPath
Start Listening VNC Viewer		5.1.0.15125	01/01/1601 00:00:00	CF6ACE9E-7BE	False	C:\Documents and Settings\All Users\Documents\MSIUtility\{CF6ACE
VNC Address Book		5.1.0.15125	01/01/1601 00:00:00	CF6ACE9E-7BE	False	C:\Documents and Settings\All Users\Documents\MSIUtility\{CF6ACE
VNC Viewer 5.1.0.15125		01/01/1601 00:00:00	CF6ACE9E-7BE	False	C:\Documents and Settings\All Users\Documents\MSIUtility\{CF6ACE	

×

App-V Version: 4.6.3.24870 on: SCCMXP

Remote CMD (As you)

Cache Details Packages Shortcuts Appv 4.6 Commands

SFTMIME command examples:

Add Publishing Server

= SFTMIME ADD SERVER: "Production Environemt App-V" /HOST ***HOSTNAMEHERE*** /TYPE RTSP /PORT 554 /REFRESH ON

Delete Publishing Server Start Refresh of Server

= SFTMIME DELETE SERVER: "Production Environemt App-V" = SFTMIME REFRESH SERVER: "Production Environemt App-V"

Load Package Delete Package = SFTMIME LOAD PACKAGE:{4DE133E9-B54D-468F-9E7D-0B51A26CB538} = SFTMIME DELETE PACKAGE: {4DE133E9-B54D-468F-9E7D-0B51A26CB538}

Remove Complete App

= SFTMIME REMOVE APP: "Open Options User Application 7.2.0.0" /COMPLETE

Add FileType

= SFTMIME ADD TYPE:DOCX /APP "Microsoft Word 14.3.2.0" /ICON icon-pathname /CONTENT-TYPE content-type /GLOBAL /PERCEIVED-TYPE perceived-type /PROGID progid /CONFIRMOPEN NO /SHOWEXT YES /NEWMENU YES

Delete FileType

= SFTMIME DELETE TYPE:DOCX /GLOBAL

Standard command examples:

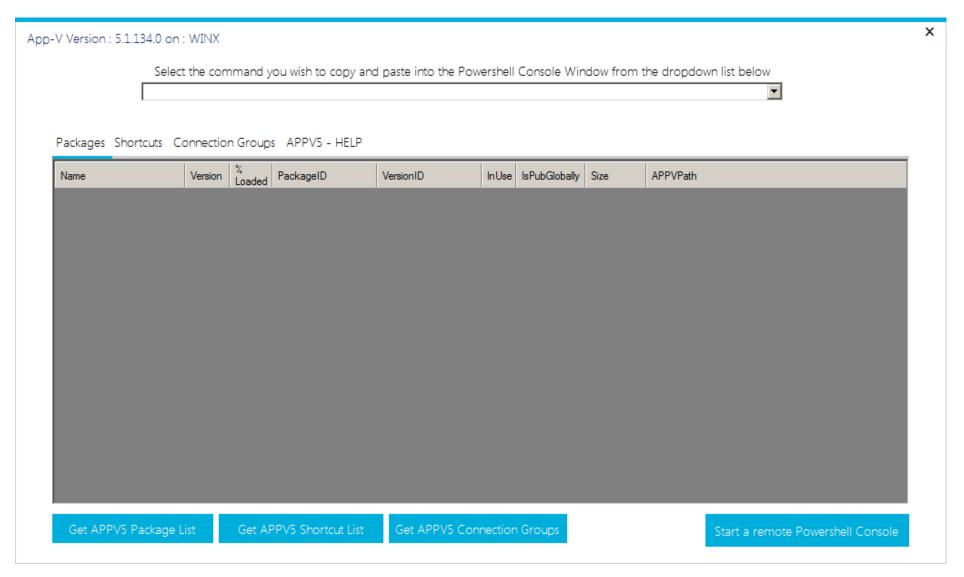
Remove Directory

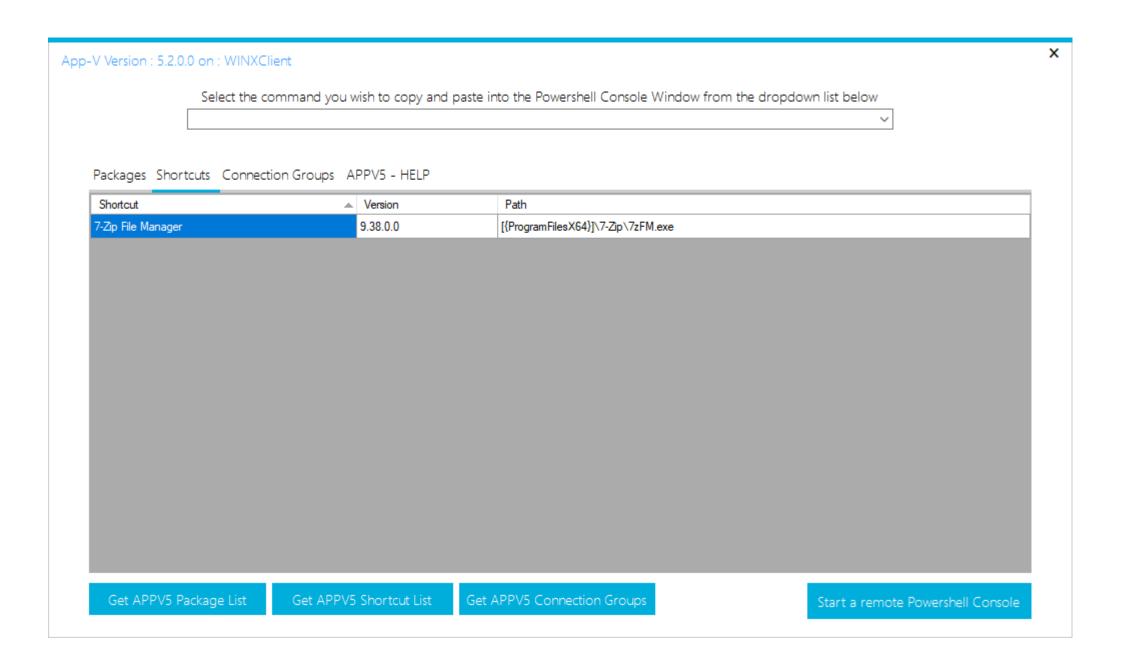
= RD /S /Q "C:\Program Files\RDT\Folder"

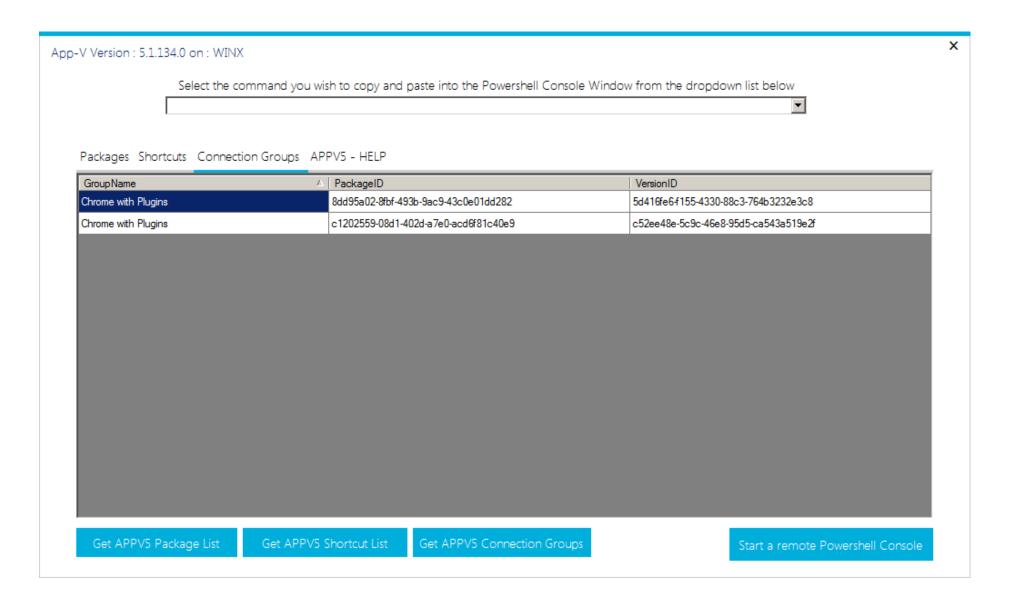
Remove File

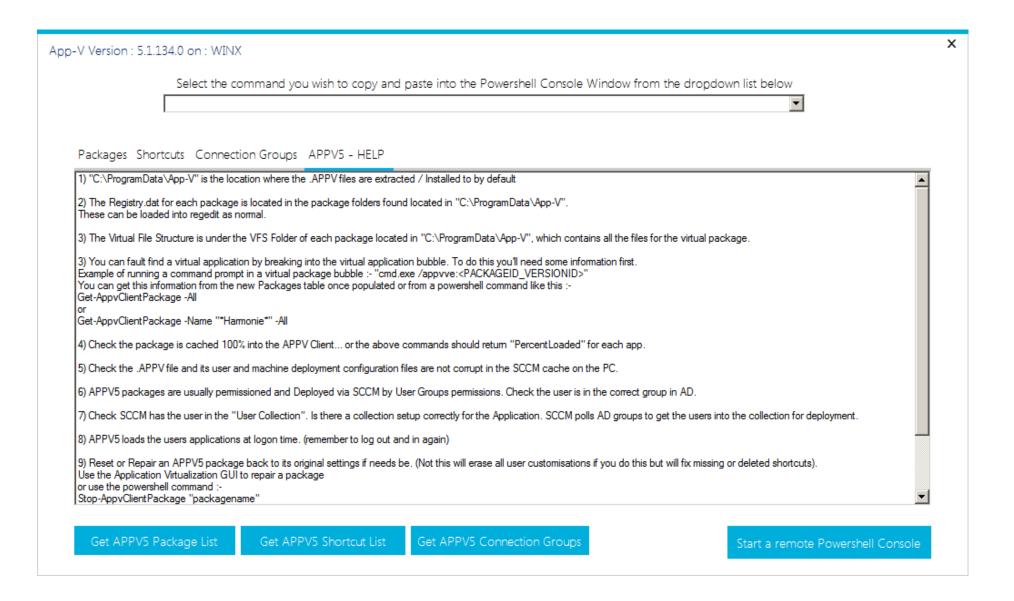
= Del /F /Q "C:\Program Files\RDT\RDT\RDT.EXE"

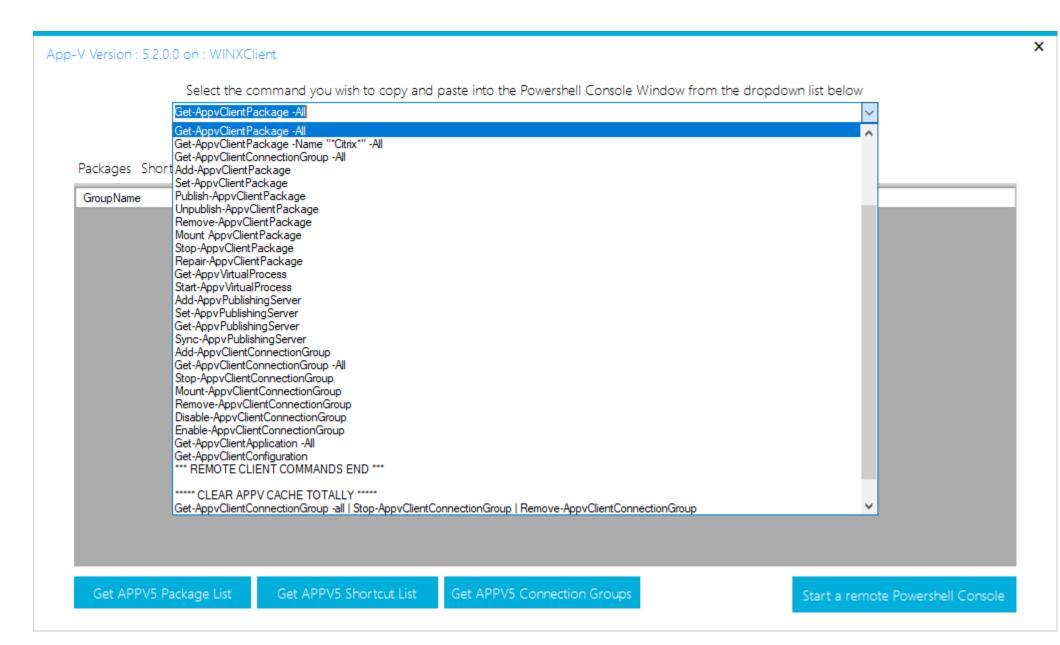
Example tab generated by pressing the Get APPV button on the HOME tab:











Example generated when Start-Up Items button is pressed:

ogin Items Run Shell Plug-ins Internet Plug-ins Network	c Plug	-ins Local Print Server
SOFTWARE\Microsoft\Windows\CurrentVersion\Run	_	Command Run at Login
Mware User Process		"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Mware VM3DService Process		"C:\Windows\system32\vm3dservice.exe" -u
OFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	_	Command Run at Login
SER > SOFTWARE\Microsoft\Windows\CurrentVersion\Run	_	Command Run at Login

X Startup Items on : Win11ProWork Login Items Run Shell Plug-ins Internet Plug-ins Network Plug-ins Local Print Server DRIVE Shell Plug-in C:\Program Files\Windows Defender\shellext.dll EPP ▲ Shell Plug-in DIRECTORY 7-Zip C:\Program Files\7-Zip\7-zip.dll C:\Program Files\Windows Defender\shellext.dll EPP C:\Windows\System32\WorkfoldersShell.dll WorkFolders FOLDER ▲ Shell Plug-in C:\Windows\System32\appresolver.dll PintoStartScreen C:\Windows\SysWOW64\appresolver.dll PintoStartScreen COPYHOOK Shell Plug-in

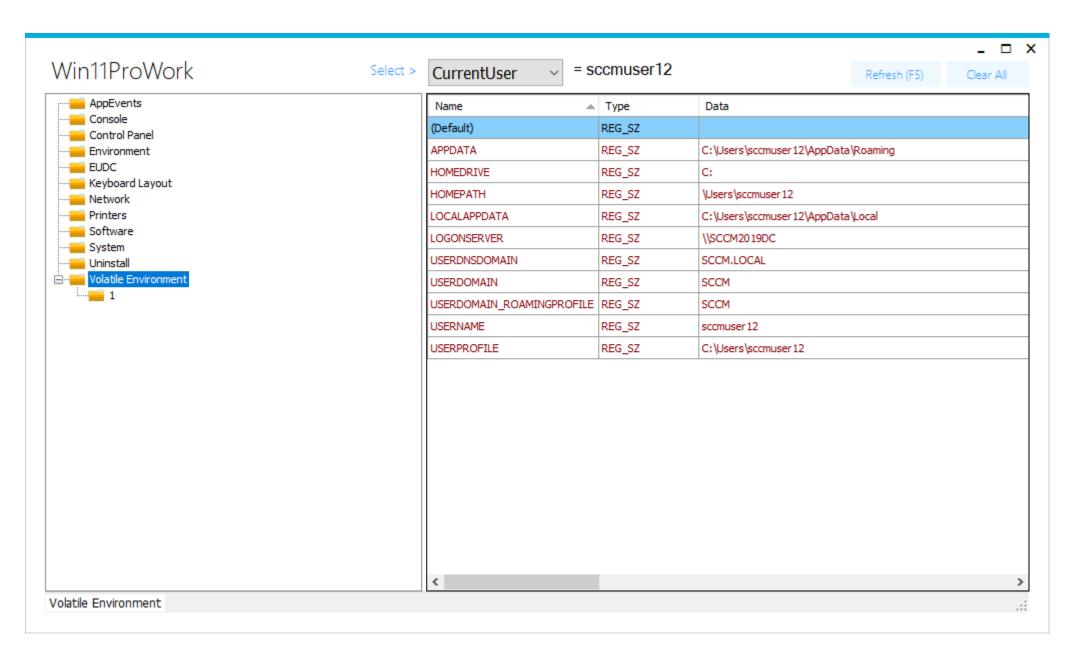
Startup Items on : WINXClient		×
Login Items Run Shell Plug-ins Internet Plug-ins Network Plug-ins Local Prin	it Server	
Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	▲ Plug-in	\neg
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	Plug-in	
Software\Microsoft\Internet Explorer\Extensions	▲ Plug-in	
C-A	. Diverse	=
Software\Wow6432Node\Microsoft\Internet Explorer\Extensions	▲ Plug-in	+

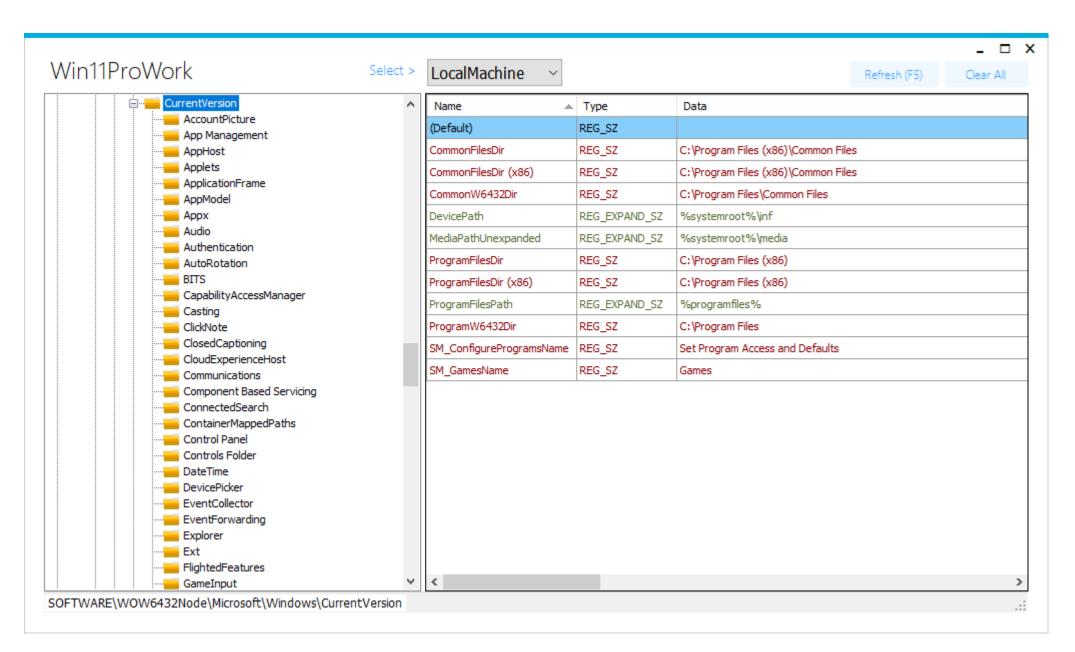
Startup Items on : Win11ProWork

Login Items Run Shell Plug-ins Internet Plug-ins Network Plug-ins Local Print Server

system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll
system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll
system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll
system32\mswsock.dll system32\mswsock.dll system32\mswsock.dll
system32\mswsock.dll
system32\mswsock.dll
system32\mswsock.dll
· · · · · · · · · · · · · · · · · · ·
system32\mswsock.dll
32\vsocklib.dll
s\system32\wshbth.dll

C:		×				
Startup Items on : Win11ProWork						
Login Items Run Shell Plug-ins Internet Plug-ins Network Plug-ins Local Print Server						
SYSTEM\CurrentControlSet\Control\Print\Monitors	△ Driver					
Appmon	AppMon.dll					





Revision Changes:

- Version 4.0.29 = Added SCCM Compliance Checker tab see policy and if its compliant!
- Version 4.0.28 = Added SCCM Missing KB tab to detect KB patches missing or not installed through SCCM / WSUS.
 - Added SCCM Installed KB tab to detect KB patches that have installed successfully through SCCM / WSUS.
 - Added Reboot? Tab to try and detect if a pc needs a reboot or not (Work in progress) but first registry check seems ok so far.
- Version 4.0.27 = Fixed security issue in RDT-Registy button. Fixed KB-Installed ordering. New-Feature **KB-Missing tab** where you can detect missing KB fixes and patches missing from your PC to keep it up-to date.
- Version 4.0.26 = Fixed "DOTNET" connection security level to 6 packet.privacy. Fixed Windows Updates date now returned is correct and can be exported out to a csv file and filtered to latest date etc. Fixed a routine that wasn't exiting properly on the APPV detect button.
- Version 4.0.25 = Added MBSA tab, any remote PC can be security scanned using the MBSA from Microsoft to see if it conforms to baseline patch status and application patches. This tool needs the file **Scan-UpdatesOffline.zip** which can be downloaded from the RDT website.
- Version 4.0.24 = Added "File Version Finder" button to the start page, any file with a version can be detected on a remote pc.
- Version 4.0.23 = Fixed issue on "groups" tab where "domain group" not being removed from "local group" properly.
- Version 4.0.22 = Fixed Tab switching issue. Added "multi profile selection & deletion" on profiles tab. Added Icons to right click menu.
 - Re-arranged so app fits full screen better with certain tabs.
- Version 4.0.21 = Added .NET tab where you can accurately detect CORE and Framework versions (x86 and x64) on a remote PC.
- Version 4.0.20 = Added older "domain\user" detection back into connection gathering to aid in finding the cause of blank "domain\user" being given as a result in some very hit and miss instances.
- Version 4.0.19 = 1) Added "Shaddow Desktop" button for remote viewing of Users desktop (If the user accepts the connection!)
- Version 4.0.18 = 1) Added Add PCs from file to Computer's list. 2) Added Search for program on Installed Programs and features tab.
- Version 4.0.17 = Added Active Directory tab (Read-only) operation of users / computers / groups and group members.

Version 4.0.16 = Added Windows 11 support, fixed Microsoft registry screwup about "ProductName" reg key in Details Tab.

Version 4.0.15 = Added Profiles Tab for Christine. Profile sizes can be got and profiles deleted as you would if you were in system>profiles.

Version 4.0.14 = Added "Clear Computers List" right click menu option for Ian.

Version 4.0.13 = Added "StoreApps" tab with detection for Microsoft Store Apps and MSIX packages.

Version 4.0.12 = 1) Fixed – Package Execute (RunAs) account was not functioning with a restricted logged on user. Fixed WINRM configuration if not Connected to a domain and setup via Policies.

Version 4.0.11 = 1) Fixed - Package not deleted off of remote pc after Execute via WMI button (manual checks).

Version 4.0.10 = 1) New PowerShell Invoke command button added to start page. 2) New Install routines on Execute tab (PowerShell driven).

3) Dropped the need for all third-party executables (Remcom and paexec) are now no longer needed. 4) Droppdown server list now remembers.

5) Fixed create local user button. (Password length and complexity has changed in windows. 6) Changed helpdesk save details to be per computer.

7) Removed VNC tab as it wasn't working correctly.

Version 4.0.09 = 1) Missed this release number.

Version 4..008 = 1) New 3rd party Drivers tab which lists additional installed drivers on the WIM. 2) New WIM-Optional Features tab with current state.

Version 4.0.07 = 1) Updated Patches tab with Remote KB uninstall button for Windows 7, Windows 8 and Windows 10 Computers. (DISM based).

Version 4.0.06 = 1) New "Computer List". New "Right click" Add/Delete/Connect Items. ("Computer list" is now remembered next launch).

Version 4.0.05 = 1) Fixed What Logon-Server button. Fixed User Tab detections. Added APPV5 Detection help and new detection buttons.

Version 4.0.04 = 1) Product unlocked for everyone – FREE fully functional.

Version 4.0.03 = 1) Fully functional 30-day trial offered.

Version 4.0.02 = 1) GUI changed to Metro Interface.

Version 4.0.01 = 1) Added AD user buttons on Home page for Email Address / Phone numbers / mobile Number.

Version 4.0.00 = 1) Public Release Version supporting any PC with Dot-Net 4 installed.

Version 1.090 = 1) Encrypted serial number from prying eyes.

Version 1.089 = 1) Information updated on the Install / Remove packages tab.

Version 1.088 = 1) Removed REMCOM plain text password security issue. REMCOM Connections use NTLM security authentication now.

Version 1.087 = 1) Ordered buttons alphabetically on HOME.

Version 1.086 = 1) Added Hard Reset Policy SCCM client tools button.

Version 1.085 = 1) Added SCCM client tools buttons code (26) and (121).

Version 1.084 = 1) Changed SCCM user adverts list routine to use AD based SID detection rather than local PC (Explorer.exe).

Version 1.083 = 1) Cosmetic changes to fix full screen fitting.

Version 1.082 = 1) Added logged on user credential tick box and corrected checking for blank entries.

Version 1.081 = 1) Added RDT Registry Editor full key and value creation right click options.

Version 1.080 = 1) Added PayPal button on HOME. 2) Replaced PSEXEC with PAEXEC (commercially free redistributable).

Version 1.079 = 1) Install / Remove packages tab updated.

Version 1.078 = 1) Updated RDT Registry viewer to Editor.

Version 1.077 = 1) Added Start-up Item button and coded.

Version 1.076 = 1) Added RDT Registry Viewer.

Version 1.0.75 = 1) Added PayPal button on HOME. 2) Replaced PSEXEC with PAEXEC (commercially free redistributable).

Version 1.0.74 = 1) Added Helpdesk reference section on HOME.

Version 1.0.73 = 1) Minor cosmetic GUI re-arrangements and renaming / tidying up done.

Version 1.0.72 = 1) Fixed spurious connections issues on certain buttons if not connected to a PC. Cut initial connection test to max 5 seconds length.

Version 1.0.71 = 1) Non-Commercial Icons replace all previous part commercial and fully commercial Icons in the program.

Version 1.0.70 = 1) New GUI and layout applied for production and buttons added / moved etc.

Version 1.0.69 = 1) Changed connection check to TCP on port 3389 (RDP) and removed ping check.

Version 1.0.68 = 1) Added detection for Reader DC.

Version 1.0.67 = 1) Added PowerShell button (with included remote WINRM start) to the APPV5 form for proper Administration via PowerShell.

Version 1.0.66 = 1) Added Appv-5 detection and new APPV4 or APPV5 forms as seen screens above.

Version 1.0.65 = 1) Removed previous "." addition to the IP address to make the tool work on Windows 8.1 and Server 2012.

Version 1.0.64 = 1) Reboot button added (with check). 2) 1E Nomad and PXE tab added.

Version 1.0.63 = 1) Fixed Java detection on PC-info tab for new java versions > 1.7.0.55 and 1.8 or above. 2) Added TNS ADMIN detection to user tab.

Version 1.0.62 = 1) Fixed user detection on first connect button.

Version 1.061 = 1) Added User rerun Advert button.

Version 1.060 = 1) Added Machine rerun Advert button.

Version 1.059 = 1) Fixed Detica Agent detection on PC-Info tab.

Version 1.058 = 1) Added Lumensions server line detection to the PC-Info tab.

Version 1.057 = 1) Fixed x86 and x64 APPV Cache details tab. APPV Cache can now be measured properly.

Version 1.056 = 1) Added WMIFIX SCCM command.

Version 1.055 = 1) Fixed SCCM buttons remote commands.

Version 1.054 = 1) Fixed Install and Remove software buttons for Helpdesk.

Version 1.051-53 = 1) Fix the WMI cannot connect to PC that sometimes is seen. 2) Changed to Installer folder for logs.

Version 1.050 = 1) Added Office 2013 detection.

Version 1.047-49 = 1) Adobe Reader Detection on PC-INFO tab fixed. 2) Added APPV cache details tab (works for x86 only).

Version 1.046 = 1) Changed Start-up page to detect previously connected PC's at launch. 2) Added permanent comments field for selected PC.

Version 1.045 = 1) Added Adobe reader detection for version 11.

Version 1.044 = 1) Added VNC tab with remote VNC setup for remote control of user's PC.

Version 1.043 = 1) Few minor cosmetic appearance changes.

Version 1.042 = 1) Fixed Avecto version detection on PC info tab. 2) Added Running Jobs detection on SCCM tab.

Version 1.041 = 1) Added SCCM Provisioning check on connect. (Checks to see if SCCM jobs are halted or not) FALSE (Green) is good, TRUE (Red) is BAD.

Version 1.040 = 1) Added Processor Usage tab.

Version 1.039 = 1) Fixed initial connection problems. 2) Moved PC info to its own tab. 3) Added User tab (Printers and Network drives). 4) Added x64 detection for certain software.

Version 1.036 = 1) Fixed / enhanced "Windows Update Detection" and "Other Updates detection" on x64 PC's on the Installed patches tab.

Version 1.035 = 1) Added detection of Adobe Reader 11.0.00

Version 1.034 = 1) Corrected Adobe Reader blank string detection.

Version 1.033 = 1) Updated Groups tab. 2) Updated HOME to include Avecto version. 3) Added check to Uninstall (on installed software tab).

Version 1.032 = 1) Corrected "Installed Software" Uninstall button REBOOT=REALLYSUPPRESS tag added.

Version 1.031 = 1) Improved APPV tab layout and functionality. 2) Added help button.

Version 1.030 = 1) Improved the File Association detection tab.

Version 1.029 = 1) Added detection for Adobe Reader 9.5.1

Version 1.028 = 1) Added Install and Uninstall command line text entry boxes so any file can be run.

Version 1.025 - 1.027 = Minor application fixes and tweaks that were asked for by people.

Version 1.024 = 1) Re-worked so application will fit to minimum laptop 1200x600 size screen.

Version 1.023 = 1) Fixed Date ordering on Installed software and SCCM Execution history tabs.

Version 1.022 = 1) Added Lumensions detection.

Version 1.021 = 1) Fixed MSI list problem. 2) Fixed "select cell" issue.

Version 1.020 = 1) Updated SCCM tab (New features). 2) Corrected MIR agent versions detection issue.

Version 1.019 = 1) Changed Install Packages on Install Page to be Universal. (I.E. enter the package directory to install from...)

Version 1.018 = 1) Fixed Group-Member detection on x64. 2) Fixed Remote Command on x64. 3) Added "Who Run" to Task Manager (as seen above).

Version 1.017 = 1) Added Appsense agent detection. 2) Made tool universal.

Version 1.016 = 1) Added to MSI tab, the Installed date/time now shown for MSI's in the MSI Database.

Version 1.015 = 1) Fixed 32bit installed software detection as well as x64 software detection on x64 machine.

Version 1.014 = 1) Added Windows 7 x64 support. 2) Re-ordered Tabs. 3) Added colour to help button usage. 4) Updated Help File.

Version 1.013 = 1) Added Detica agent detection

Version 1.012 = 1) Fixed group membership issue.

Version 1.011 = 1) Added Disk tab.

Version 1.001 - 1.010 = 1) Primary design of tool.

DISCLAIMER

THIS RDT SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL Tim, OR ANY OF THEIR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Without limiting the foregoing, Tim makes no warranty that:

- i. the software will meet your requirements.
- ii. the software will be uninterrupted, timely, secure or error-free.
- iii. the results that may be obtained from the use of the software will be effective, accurate or reliable.
- iv. the quality of the software will meet your expectations.
- v. any errors in the software will be corrected.

The RDT Software and this documentation made available:

- vi. could include technical or other mistakes, inaccuracies or typographical errors. Tim may make changes to the software or documentation made available at any time.
- vii. may be out of date and Tim, its contributor, make no commitment to update such materials.

Tim, assume no responsibility for errors or omissions in the software or documentation available.

In no event shall Tim be liable to you or any third parties for any special, punitive, incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not Tim has been advised of the possibility of such damages, and on any theory of liability, arising out of or in connection with the use of this software.

The use of the software is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your computer system or loss of data that results from such activities. No advice or information, whether oral or written, obtained by you from Tim, shall create any warranty for the software.