Uninstall Endpoint Agent - Master Copy

Doc ID	TECH220214
Version:	6.0
Status:	Published
Published date:	10/23/2014
Updated:	10/23/2014
Categories:	How To , 10.0 , 12.0 , 11.0
Available To:	Internal
Author:	bernard_martinez@symantec.com

Problem

This is the complete instruction set, and options for removing the Endpoint Agent. Most customers will either call in for the issue of removing the agent, or trying to install/upgrade the agent with errors. In some cases customers are unable to confirm whether or not if a previous version of the Agent has been installed. This KB will allow you to confirm if a previous Agent has been installed. How to use tools to remove the Agent. How to manually remove the Agent. End results should be a clean state and a system ready for a DLP Agent install without error...

Solution

Recommended procedures for first attempts to remove agent:

I) Uninstall.bat

II) MSIEXEC

- Login as an administrator user.
- Start a command prompt (Administrator command prompt if Windows Vista or higher).
- Run the command: `msiexec /x`

NOTE: Substitute the appropriate value from the following table for in the command line above (include the curly braces).

Version	Product ID
8.1	{69E7464F-6E7E-4607-9C9E-085DA243D807}
9.0	{0C9B68A6-63B4-473F-B281-24774FBBFF73}
9.0.1	{0C9B68A6-63B4-473F-B281-24774FBBFF73}
9.0.2	{1BE4CCA3-9B6C-4943-B03E-19CBFA51A88F}
9.0.3	{D26F44C8-44BB-47FA-81E8-8F5EDA53E3AA}
10.0	{BB81F635-3CDB-405A-9AF3-0428D42EA605}
10.5.x (10.5.0, 10.5.1, 10.5.2, 10.5.3)	{ADBACBC0-05F4-4610-BBB7-007A543D5B47}
11.0	{BC705572-C8CD-49e4-9693-BDC8E4D35570}
11.1.x (11.1.0, 11.1.1, 11.1.2)	{2AF3B399-42A5-42bd-A5E0-72B657110363}
11.5.x (11.5.0, 11.5.1)	{2AF3B399-42A5-42bd-A5E0-72B657110363}
11.6	{8790B246-A2CF-43b1-BDB0-2B4383BB9785}
11.6.1	{9E983F62-FFE9-4A92-AA24-2CA97B353A73}
11.6.2	{E818C222-AC57-46B4-9689-83DFB591D8F4}
11.6.3	{70365353-32F7-4367-8E71-ABDC966D0488}
12.0	{D39272A1-C04C-4295-8558-79E1991BA4FC}
12.0.1	{1C4B1778-B5E7-4A2F-98D2-F8FBDE968B6C}
12.5	{B29DE059-FEC4-4304-96BB-50308729BEDE}
12.5.1	{9967A8CA-E48C-4AE9-99C8-6A48AF57669A}

You can identify which version of the Endpoint Agent is installed by checking the properties of the file "edpa.exe", or by navigating to the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Search for the value called "DisplayName" that contains the string "AgentInstall". The uninstall command (including the Product ID) will be under that key's UninstallString.

III) Clean_agent.exe

Please find the latest version of the tool attached with this KB article, which is backwards compatible with all previous versions of the Endpoint agent.

Optional clean_agent.exe parameters:

```
[-installdir=<agent install directory>]
[-log=<console, or a filename (default is clean_agent.log)>]
[-loglevel=<silent, finest, fine, info, warning, severe>]
[-prompt=<on, off>]
```

How to use the Tool:

1. Open a command prompt

2. Go to the directory where the tool was extracted and run it as follows:

```
C:\Documents and Settings\Administrator\Desktop>clean_agent.exe

Product Code: {BC705572-C8CD-49e4-9693-BDC8E4D35570}
Product Install Dir: C:\Program Files\Manufacturer\Endpoint Agent\
Product Version: 11.0.0.19031
Product ID: 275507CBDC8C4e946939DB8C4E3D5507


WARNING: All files in the directory shown above will be removed, along
with all drivers named 'vfsmfd.sys', 'vrtam.sys', 'tdifd.sys', as well
as all driver services named 'vfsmfd', 'vrtam', 'tdifd' and
'tdifd10'.  In addition, all installer registry entries referencing
the 'Product ID' value above will be removed.


Proceed with clean operation [Y / N]: y
Cleaning agent...

The Agent clean operation was successful.
```

After running the tool and a subsequent reboot, the agent should be completely removed from the system.

IV) Time for a Manual Uninstall

1. Ensure the Agent and Watchdog processes are stopped

NOTE: DLP 11.6 on will require using the service_shutdown tool which is part of the SymantecDLPWinAgentTools_.zip package that comes with the agent installer. Run service_shutdown from the command line from the folder ks.ead resides in.

Example:

```
sc stop edpa && sc stop wdp

taskkill /f /im edpa.exe & taskkill /f /im wdp.exe
```

Repeat the taskkill command until the output resembles:

```
ERROR: The process "edpa.exe" not found.
ERROR: The process "wdp.exe" not found.
```

2. Delete the Agent and Watchdog services from the SCM

example:

```
sc delete edpa
sc delete wdp
```

NOTE: This example uses the default service names.

If the services could not be deleted, the machine will need to be rebooted to Safe Mode in order to complete the clean process.

```
sc query edpa
sc query wdp
```

If one of the services does not show as "does not exist", then a reboot to safe mode is necessary.

```
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.
```

3. Stop the FS driver and the RTAM driver

Order is important, stop the FS driver first

example:

```
sc stop vfsmfd
sc stop vrtam
```

Output of the commands should resemble:

```
SERVICE_NAME: vfsmfd
        TYPE   : 2 FILE_SYSTEM_DRIVER
        STATE  : 1 STOPPEDSERVICE_NAME: vrtam
        TYPE   : 1 KERNEL_DRIVER
        STATE  : 1 STOPPED
```

If either of the drivers could not be stopped, then a reboot to safe mode will be necessary to complete the clean.

4. Delete the FS driver, RTAM driver and TDI driver services

```
sc delete vfsmfd
sc delete vrtam
sc delete tdifd
```

Note: post-v9 agents include the version in the name of the TDI driver, such as: tdifd10, tdifd105, tdifd11, and tdifd111.

If the FS driver service or the RTAM driver service could not be deleted, the machine will need to be rebooted to Safe Mode in order to complete the clean process.

```
sc query vrtam
sc query vfsmfd
```

Note: the TDI driver is marked for deletion on reboot.

If one of the services does not show as "does not exist", then a reboot to safe mode is necessary.

```
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.
```

5. Delete the driver binaries

Delete the directories from %windir%\system32\drvstore that resemble:

```
rtam_*
vfsmfd_*
tdifd_*
```

Delete the following files from %windir%\system32\drivers

```
tdifd*.sys
vfsmfd.sys
vrtam.sys
```

6. Clean the Windows Installer Database Registry Entries

- Open the registry to the following location:**HKEY_CLASSES_ROOT\Installer\Features**
- Locate the key that has entries like FF_PLUGIN, tdifd, vrtam, etc - note the name of this key (the **PRODUCT_ID** for v9.0 is *6A86B9C04B36F3742B184277F4BBFF37*)
- Delete the following keys and their subkeys:

under *HKEY_CLASSES_ROOT\Installer*:

- Features*PRODUCT_ID*
- Products*PRODUCT_ID*
- UpgradeCodes\ (all keys with a NAME column that matches *PRODUCT_ID*) & (looking through all remaining keys in, and delete any that have the PRODUCT_ID as a value within the key)

Although the reasoning behind this has not been determined, MSI's can, at times, store registry information using the reverse of the original product code in the registry. This causes our searches for the original product ID to fail. This was found in this MSDN thread: MSDN

Remove the registry entry

Version	Product ID(Reversed from original)
8.1	F4647E69-XXXX-XXXX-XXXX-XXXXXXXXXXXX
9.0	6A86B9C0-XXXX-XXXX-XXXX-XXXXXXXXXXXX
9.0.1	6A86B9C0-XXXX-XXXX-XXXX-XXXXXXXXXXXX

9.0.2	3ACC4EB1-XXXX-XXXX-XXXX-XXXXXXXXXXXX
9.0.3	8C44F62D-XXXX-XXXX-XXXX-XXXXXXXXXXXX
10.0	536F18BB-XXXX-XXXX-XXXX-XXXXXXXXXXXX
10.5.x (10.5.0, 10.5.1, 10.5.2, 10.5.3)	0CBCABDA-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.0	275507CB-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.1.x (11.1.0, 11.1.1, 11.1.2)	993B3FA2-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.5.x (11.5.0, 11.5.1)	993B3FA2-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.6	642B0978-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.6.1	26F389E9-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.6.2	222C818E-XXXX-XXXX-XXXX-XXXXXXXXXXXX
11.6.3	35356307-XXXX-XXXX-XXXX-XXXXXXXXXXXX
12.0	1A27293D-XXXX-XXXX-XXXX-XXXXXXXXXXXX
12.0.1	8771B4C1-XXXX-XXXX-XXXX-XXXXXXXXXXXX
12.5	950ED92B-XXXX-XXXX-XXXX-XXXXXXXXXXXX
12.5.1	AC8A7699-XXXX-XXXX-XXXX-XXXXXXXXXXXX

*Note: In the unlikely event that you see more than 1 entry for the appropriate product code please reference the above and use the appropriate product code

under *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer*:

- UpgradeCodes\ (all keys with a NAME column that matches *PRODUCT_ID*)

- UserData\S-1-5-18\Components\ (all components with a NAME that matches*PRODUCT_ID*)
- UserData\S-1-5-18\Products*PRODUCT_ID*

under *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls*:

- all SharedDll entries whose path includes the Endpoint Agent installation directory

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall{0C9B68A6-63B4-473F-B281-24774FBBFF73}

7. Reboot the machine

8. Delete the Agent Installation directory

Attachment


Clean_agent_12.5.rar
943K • 3 minute(s) @ 56k, < 1 minute @ broadband

Attachment

 Clean_Agent_12.5.1.zip
1.2MB • 4 minute(s) @ 56k, < 1 minute @ broadband

Attachment Description

Clean Agent 12.5.1

Legacy ID

56466