

RE: updates after format

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.mediacenter/2004-05/0073.html>

From: S Vijay [MSFT] (svijay_at_online.microsoft.com)

Date: 05/02/04

Date: Sun, 02 May 2004 22:36:46 GMT

Hi,

The error does not occur, if the Microsoft Server is down. The error "The software you are installing has not passed Windows Logo testing verify its compatibility with Windows XP..." can be resolved by following the detailed instructions in the article given below:

<http://support.microsoft.com/default.aspx?kbid=822798>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;811263&Product=wupd>

or

SYMPTOMS

When you try to download an ActiveX control, install an update to Windows or to a Windows component, install a service pack for Windows or for a Windows component, or install a Microsoft or third-party software program, you may experience one or more of the following symptoms:

When you use the Windows Update Web site to install updates, the installation fails and the Windows Update.log file contains error 80070643.

You may receive the following error message when you try to install a program or update:

Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Name of software package

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at <http://windowsupdate.microsoft.com> to see if one

is available.

Do you want to continue the installation?

If you click More Info, you receive the following message:

Microsoft Windows

The signature on the software package you want to install is invalid. The software package is not signed properly.

After you click OK in the first error message dialog box, you may receive a message that indicates that the installation was successful, or you may receive the following error message:

Name of Update Package

The cryptographic operation failed due to a local security option setting. When you try to install an update (such as a service pack), you may receive an error message that is similar to one of the following:

Name of Update Package

Setup could not verify the integrity of the file Update.inf. Make sure the Cryptographic service is running on this computer.

–or–

Failed to install catalog files.

–or–

The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

This software will not be installed. Contact your system administrator.

–or–

The software you are installing has not passed Windows Logo testing to verify its compatibility with this version of Windows. (Tell me why this testing is important.)

When you try to install a Windows XP service pack, you may receive an error message that is similar to the following:

Service Pack 1 Setup could not verify the integrity of the file. Make sure the Cryptographic service is running on this computer

The %WINDIR%\System32\CatRoot2\Edb.log may grow to 20 megabytes (MB) even though the file is typically less than 1 MB.

CAUSE

This problem may occur for any of the following reasons:

Log file or database corruption exists in the

%Systemroot%\System32\Catroot2 folder.

Cryptographic Services is set to disabled.

Other Windows files are corrupted or missing.

The hidden attribute set is in the %Windir% folder and in its subfolders.

The Unsigned non-driver installation behavior Group Policy setting (Windows 2000 SP2 and earlier only) is set to Do not allow installation or Warn but allow installation, or the Policy binary value is not set to 0 in the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Non-Driver Signing

The Enable trusted publisher lockdown Group Policy setting is turned on, and you do not have the appropriate certificate in your Trusted Publishers certificate store. This Group Policy setting is located under User Configuration, under Windows Settings, under Internet Explorer Maintenance, under Security, under Authenticode Settings in the Group Policy MMC snap-in. You are installing Internet Explorer 6 SP1, and the 823559 (MS03-023) security patch is installed. For additional information about this issue, click the following article number to view the article in the Microsoft Knowledge Base:

828031 The Software You Are Installing Has Not Passed Windows Logo Testing..." Error Message When You Try to Install Internet Explorer 6 Service Pack

RESOLUTION

To resolve this behavior, use the following methods. After you perform the steps in each method, test to see if the problem is resolved before you go to the next method. If the problem is resolved with any method, you do not have to use the remaining methods.

Method 1: Rename the Edb.log File

To resolve this behavior, rename the Edb.log file, and then try to install the program again. To rename the Edb.log file, follow these steps:

Click Start, and then click Run.

In the Open box, type cmd, and then click OK.

At the command prompt, type the following command, and then press ENTER:

```
ren %systemroot%\system32\catroot2\Edb.log *.tst
```

Method 2: Set Cryptographic Services to Automatic

Set the Cryptographic Services to Automatic, and then try to install the program again. To set the Cryptographic Services to Automatic, follow these steps:

Start the Administrative Tools utility in Control Panel.

Double-click Services.

Right-click Cryptographic Services, and then click Properties.

Click Automatic for Startup type, and then click Start.

Note Windows 2000 does not list Cryptographic Services in the SERVICES Administrative Utility.

Method 3: Rename the Catroot2 Folder

Rename the Catroot2 folder, and then try to install the program again. To rename the Catroot2 folder, follow these steps:

Click Start, and then click Run.

In the Open box, type cmd, and then click OK.

At the command prompt, type the following commands, pressing ENTER after each line:

```
net stop cryptsvc
ren %systemroot%\System32\Catroot2 oldcatroot2
net start cryptsvc
exit
```

Important Do not rename the Catroot folder. The Catroot2 folder is automatically recreated by Windows, but the Catroot folder is not recreated if it is renamed.

Method 4: Re-register DLL Files That Are Associated With Cryptographic Services

To register .dll files that are associated with Cryptographic Services, follow these steps:

Click Start, and then click Run.

In the Open box, type cmd, and then click OK.

At the command prompt, type the following commands, pressing ENTER after each line:

Note Click OK if you are prompted to do so.

```
regsvr32 softpub.dll
regsvr32 /u wintrust.dll
regsvr32 /u initpki.dll
regsvr32 /u dssenh.dll
regsvr32 /u rsaenh.dll
regsvr32 /u gpkcsp.dll
regsvr32 /u sccbase.dll
regsvr32 /u slbcsp.dll
regsvr32 /u cryptdlg.dll
regsvr32 /u softpub.dll
exit
```

Restart your computer.

Click Start, and then click Run.

In the Open box, type cmd, and then click OK.

At the command prompt, type the following commands (press ENTER after each command):

Note Click OK if you are prompted to do so.

```
regsvr32 softpub.dll
regsvr32 wintrust.dll
regsvr32 initpki.dll
regsvr32 dssenh.dll
regsvr32 rsaenh.dll
regsvr32 gpkcsp.dll
regsvr32 sccbase.dll
regsvr32 slbcsp.dll
```

```
regsvr32 cryptdlg.dll  
regsvr32 softpub.dll  
exit
```

Method 5: Remove the Hidden Attribute from %Windir% and from Its Subfolders
Click Start, and then click Run.

In the Open box, type cmd, and then click OK.

At the command prompt, type the following commands, pressing ENTER after each line:

```
attrib -s -h %windir%  
attrib -s -h %windir%\system32  
attrib -s -h %windir%\system32\catroot2  
exit
```

Method 6: Set Non-Driver Signing Policy to Silently Succeed

If you are running a version of Windows 2000 that is before Windows 2000 Service Pack 3 (SP3), set the Unsigned non-driver installation behavior Group Policy setting to Silently succeed. This Group Policy setting is located under Computer Configuration, under Windows Settings, under Security Settings, under Local Policies, under Security Options in the Group Policy MMC snap-in. If you are running Windows 2000 SP3 or later, this Group Policy setting is no longer supported. In this case, follow these steps to resolve this problem:

Click Start, click Run, type regedit, and then click OK.

Locate, and then click the following key in the registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Non-Driver Signing

Right-click the Policy binary value, and then click Modify.

The Value data will appear in the following format:

0000 02

Press DELETE to remove the current value (02 in this example), and then type 0 (the current value will now appear as 00).

Click OK, and then quit Registry Editor.

Method 7: Temporarily Turn Off Trusted Publishers Lockdown and Install the Appropriate Certificates to Your Trusted Publishers Certificate Store

You can continue to use the Enable trusted publisher lockdown Group Policy setting, but you must first add the appropriate certificates to your Trusted Publishers certificate store. To do this, turn off the Enable trusted publisher lockdown Group Policy setting, install the appropriate certificates in your Trusted Publishers certificate store, and then turn the Enable trusted publisher lockdown Group Policy setting back on. To install the appropriate certificate for Microsoft Windows and Microsoft Internet Explorer product updates, follow these steps:

Download the Microsoft product update that you want to install from the Microsoft Download Center or from the Windows Update Catalog. For additional information about how to download product updates from the Microsoft Download Center, click the following article number to view the article in the Microsoft Knowledge Base:

119591 How to Obtain Microsoft Support Files from Online Services

For additional information about how to download product updates from the Windows Update Catalog, click the following article number to view the article in the Microsoft Knowledge Base:

323166 HOW TO: Download Windows Updates and Drivers from the Windows Update Catalog

Extract the product update package to a temporary folder. The command-line command that you use to do this depends on the update that you are trying to install. Check the Microsoft Knowledge Base article that is associated with the update to determine the appropriate command-line switches that you will use to extract the package. For example, to extract the 824146 security patch for Windows XP to the C:\824146 folder, run Windowsxp-kb824146-x86-enu -x:c:\824146. To extract the 828750 security patch for Windows XP to the C:\828750 folder, run q828750.exe /c /t:c:\828750.

Right-click the KBNumber.cat file from the product update package in the temporary folder you created in step 2, and then click Properties.

Note The KBNumber.cat file may be in a subfolder (for example, C:\824146\sp1\update or C:\824146\sp2\update).

On the Digital Signatures tab, click the digital signature and then click Details.

Click View Certificate, and then click Install Certificate.

Click Next to start the Certificate Import Wizard.

Click Place all certificates in the following store, and then click Browse.

Click Trusted Publishers, and then click OK.

Click Next, click Finish, and then click OK.

Method 8: Verify the Status of All Certificates in the Certification Path and Import Missing or Damaged Certificates from Another Computer

To verify certificates in the certificate path for a Windows or Internet Explorer product update, follow these steps:

Step 1: Verify Microsoft Certificates

In Internet Explorer, click Tools, and then click Internet Options.

On the Content tab, click Certificates.

On the Trusted Root Certification Authorities tab, double-click Microsoft Root Authority. If this certificate is missing, go to step 2.

On the General tab, make sure that the Valid from dates are 1/10/1997 to 12/31/2020.

On the Certification Path tab, verify that This certificate is OK appears under Certificate Status.

Click OK, and then double-click the NO LIABILITY ACCEPTED certificate.

On the General tab, make sure that the Valid from dates are 5/11/1997 to 1/7/2004.

On the Certification Path tab, verify that This certificate is OK appears under Certificate Status.

Click OK, and then double-click the GTE CyberTrust Root certificate. You may have more than one of these certificates with the same name. Check the certificate that has an expiration date of 2/23/2006.

On the General tab, make sure that the Valid from dates are "2/23/1996 to 2/23/2006."

On the Certification Path tab, verify that This certificate is OK appears

under Certificate Status.

Step 2: Import Missing or Damaged Certificates

If any of these certificates are missing or corrupted, export the missing or corrupted certificates to another computer, and then install the certificates on your computer. To export certificates on another computer, follow these steps:

In Internet Explorer, click Tools, and then click Internet Options.

On the Content tab, click Certificates.

On the Trusted Root Certification Authorities tab, click the certificate that you want to export.

Click Export, and then follow the instructions to export the certificate as a DER encoded Binary x.509(.CER) file.

After the certificate file has been exported, copy it to the computer where you want to import it.

On the computer where you want to import the certificate, double-click the certificate.

Click Install certificate, and then click Next.

Click Finish, and then click OK.

Vijay.S

This posting is provided "AS IS" with no warranties, and confers no rights