

# Error handling cannot install updates and program settings

When trying to download an ActiveX control, install an upgrade or install a service pack for Windows or a certain component of Windows, or install a third-party software program you may encounter some problems. and the installation failed.

**When trying to download an ActiveX control, install an upgrade or install a service pack for Windows or a certain component of Windows, or install a third-party software program you may encounter some problems. and the installation failed.** This article will provide error messages and some ways to correct the errors so you can continue your installation or updating.

Symptoms may be encountered as follows:

1. You may receive an error message when installing a program or an upgrade:

```
Digital Signature Not Found
Microsoft digital signature affirms mà t?p tin ?ã ???c ki?m tra
v?i Windows và b?n không ???c h? tr?
Máy ?nh b?n ?ang ???c cài ??t không ch?a m?t ký hi?u Microsoft digital.
So, không có quy?n th?c hi?n máy này ???c th?c hi?n ?úng v?i Windows.
Name of software package
N?u b?n mu?n tìm ki?m s? digitally ?ã ??ng ký t?p tin,
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 will receive the following message:

```
Microsoft Windows
Ch? ký trên gói gói b?n mu?n ??t là không h?p l?.
Ng??i dùng gói không ???c ??ng ký ?úng.
```

After clicking OK in the first error message dialog box, you may receive a message indicating that the installation was successful or could be an error message below:

```
Name of Update Package
L?i cryptographic ho?t ??ng b? l?i v?i m?t thi?t l?p ??a ch?
Security Security.
```

When installing an upgrade or installing a service pack, you may receive an error message as below:

1. Name of Update Package: Setup could not verify the integrity of the file Update.inf. Hãy xác ??nh các Cryptographic service ?ang ch?y trên máy tính này.
2. L?i cài ??t t?p tin danh sách: B?n ?ang cài ??t có không ??a ra Windows Logo ?? ki?m tra nó t??ng thích v ?i Windows XP. (Tell me why this testing is important.)
3. Máy ?nh này s? không ???c cài ??t. Contact your system administrator.
4. Máy ?nh b?n cài ??t không ??a ra Windows Logo ?? th? ki?m tra nó t??ng ?ng v?i phiên b?n này. (Tell me why this testing is important.)

When installing a Windows XP service pack, you may receive an error message as shown below:

1. Service Pack 1 Setup could not verify the integrity of the file. Hãy xác ??nh các Cryptographic service ?ang ch?y trên máy tính này

When you install Microsoft Data Access Components (MDAC) 2.8 you may receive an error message as shown below.

1. INF Install failure. Lý: L?i ký hi?u timestamp và / ho?c ch?ng nh?n không th? xác ??nh ho?c là malformed.

File size% WINDIR% System32CatRoot2Edb.log can be up to 20MB even though the typical file is smaller than 1MB.

When installing the software package from the Windows Update website, you may receive a notification similar to the one below:

1. Ph?n m?m ?ã không ???c phép ??ng nh?p t?p tin ki?m tra và s? không ???c cài ??t.

When checking the% systemroot% Windowsupdate.log file, you will be able to see an item with one of the following errors:

1. 0x80096001
2. 0x800B0003
3. 0x80096005
4. 0x800B0004
5. 0x80096010
6. 0x800B0109
7. 0x800B0001
8. 0x8007f0da

When you use Microsoft Windows upgrade on a Windows XP computer, the upgrade process may fail and you may receive a "0x8007f007" error message. This error message does not appear on what type of upgrade you choose.

The Svcpack.log file may include the following items:

```
937,406: GetCatVersion: Failed to retrieve version information from C: WINDOWS
937.437: GetCatVersion: Failed to retrieve version information from C: WINDOWS
940,344: DoInstallation: MyInstallCatalogFiles failed: STR_CATALOG_INSTALL_FAI
955.125: UnRegisterSpuninstForRecovery, failed to delete SpRecoverCmdLine valu
955.125: DoInstallation: Failed to unregistering spuninst.exe for recovery.
```

```
962.656: DeRegistering the Uninstall Program -> Windows Server 2003 Service Pa
962.656: Failed to install catalog files.
1448.406: Message displayed to the user: L?i c?i ??t t?p tin Catalog.
1448.406: User Input: OK
1448.406: Update.exe extended error code = 0xf01e
1448406: Update.exe return code was masked to 0x643 for MSI custom action comp
```

## Reason

This issue may appear if one or more of the following conditions are true:

1. Error log file or data in% Systemroot% System32Catroot2 directory
2. **Cryptographic Services** is set to disabled ( **disabled** ).
3. Other Windows files are wrong or lost.
4. The timestamp signature or certificate may not be verified or changed.
5. The hidden attribute is set to the% Windir% folder or one of its subdirectories.
6. Set up a Group Policy **un-driver installation behavior** (for Windows 2000 only) set to **Do not allow installation** or **Warn but allow installation** , or **Policy** 's binary value cannot be set to zero in the registration key below:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Non-Driver Signing
```

1. The **Enable trusted publisher lockdown** of Group Policy setting is enabled, and you do not have the appropriate certificate in the Trusted Publishers certificate store. Setting this Group Policy is set under **User Configuration** , **Windows Settings** , **Internet Explorer Maintenance** , **Security** , and **Authenticode Settings** in the Group Policy MMC snap-in.
2. You are installing Internet Explorer 6 SP1, and the 823559 (MS03-023) security package is installed.
3. The software distribution folder is misleading.

## Solution

To solve this problem, you use the methods below. After taking the steps in each method, check to see if the problem is resolved before proceeding to the next step. If the problem is solved in any way, you don't need to use the remaining ways.

### *Method 1: Rename the Edb.log file*

Rename the file Edb.log then install the program again. To rename the Edb.log file, follow the steps below:

1. Click **Start** , click **Run** , type **cmd** in the **Open** box, and then click **OK** .
2. At the command window, type the following command, and then press ENTER:

```
ren% systemroot% system32catroot2Edb.log * .tst
```

### *Method 2: Set up automatic encryption services*

Setting Cryptographic Services encryption services to **Automatic** automatically, then installing the program again. To set up encryption services automatically, follow the steps below:

1. Go to the **Administrative Tools** utility in **Control Panel** .
2. Double-click **Services** .

3. Right-click **Cryptographic Services** , and then click **Properties** .
4. Click **Automatic** for the **Startup type** , and then click **Start** .

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

### ***Method 3: Rename the Catroot2 folder***

Rename the Catroot2 folder (Windows XP and Windows Server 2003 only), then install the program again.

*Note* : Ignore this method if the operating system is Windows 2000.

To rename the Catroot2 folder, follow these steps:

1. Click **Start** , select **Run** , type **cmd** , and then click **OK** .
2. At the command prompt, type the following commands, and then press ENTER

```
net stop cryptsvc
ren% systemroot% System32Catroot2
oldcatroot2
net start cryptsvc
exit
```

1. Remove all tmp \* .cat files from the following directory:

```
% systemroot% system32CatRoot {F750E6C3-38EE-11D1-85E5-00C04FC295EE}
```

If no files starting with tmp exist in this directory, you must not remove any other files. The .cat files in this directory are required to install hotfixes and service packs.

*Important* : Do not rename the Catroot folder. The Catroot2 folder is automatically recreated by Windows, but the Catroot folder will not be recreated if the Catroot folder is renamed.

### ***Method 4: Re-register the DLL files associated with Cryptographic Services encryption service***

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

1. Click **Start** , select **Run** , type **cmd** in the **Open** box, then click **OK** .
2. At the command prompt, type the following commands, then press ENTER after each command:

```
regsvr32 / u 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 mssip32.dll
regsvr32 / u cryptdlg.dll
exit
```

*Note* : Click **OK** if you are required.

*Note* : Microsoft Windows 2000 does not have the Sccbase.dll file. If you are using Windows 2000 version, skip the Sccbase.dll file

1. Restart the computer.
2. Click **Start** , select **Run** , type **cmd** in the box, then click **OK** .
3. At the command window, type the following commands, press ENTER after each command:

```
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 mssip32.dll
regsvr32 cryptdlg.dll
exit
```

*Note* : Click **OK** if you are required.

*Note* : Microsoft Windows 2000 does not have the Sccbase.dll file. If you are using Windows 2000 version, skip the Sccbase.dll file

1. Restart the computer.

***Method 5: Remove hidden properties from% Windir% and its subfolders.***

1. Click **Start** , select **Run** , type **cmd** in the **Open** box, then click **OK** .
2. At the command prompt, type the following commands, press ENTER after each line:

```
attrib -s -h% windir%
attrib -s -h% windir% system32
attrib -s -h% windir% system32catroot2
exit
```

***Method 6: Set the non-driver policy to silently succeed***

If you are using a Windows 2000 version, set up **Unsigned non-driver installation behavior** of Group Policy to **Silently succeed** . Setting this Group Policy is located in the **Computer Configuration** section, **Windows Settings** , **Security Settings** , **Local Policies** , and **Security Options** in the Group Policy MMC snap-in.

1. Click **Start** , select **Run** , type regedit, and then click **OK** .
2. Locate and select the key below in the registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Non-Driver Signing
```

1. Right-click the **Policy** binary value, then select **Modify** .
2. Value data will appear in the following format:

```
0000 02
```

1. Press **DELETE** to delete the current value (in this example, 02), then type 0 (the current value will appear in 00)
2. Click **OK** , and then exit Registry Editor.

***Method 7: Temporarily turn off Trusted Publishers Lockdown and install the appropriate certificates for your trusted publishers certificate store***

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

1. Download the Microsoft product upgrade that you want to install from the Microsoft Download Center, from Windows Update Catalog, or from the Microsoft Update Catalog.
2. Unzip the product upgrade package to a temporary folder. The command to use will depend on the upgrade you install. See basic knowledge related to upgrading to determine the appropriate command to use. For example, to extract security upgrade 824146 for Windows XP into folder C: 824146, you run **Windowsxp-kb824146-x86-enu -x: c: 824146** . To extract the security upgrade 828750 for Windows XP into folder C: 828750 you run **q828750.exe / c / t: c: 828750** .
3. Right-click the *KB Number* .cat file from the product upgrade package in the temporary folder that you created in step 2 and click **Properties** .

*Note* : The *KB Number* .cat file may be in a subdirectory. For example, the file may be in the directory C: 824146sp1update or in the folder C: 824146sp2update.

1. On the Digital Signatures tab, click the digital signature and then click **Details** .
2. Click **View Certificate** , and then click **Install Certificate** .
3. Click **Next** to start the Certificate Import Wizard.
4. Click **Place all certificates in the following store** , and then click **Browse** .
5. Click **Trusted Publishers** , and then click **OK** .
6. Click **Next** , **Finish** , and then click **OK** .

***Method 8: Verify the status of certificates and import broken or missing certificates from another computer.***

To verify the certificates in the certificate path or upgrade Internet Explorer products, follow the steps below:

***Step 1 : Verify Microsoft certificates***

1. In Internet Explorer, click **Tools** , then select **Internet Options** .
2. On the **Content** tab, click **Certificates** .
3. On the **Trusted Root Certification Authorities** tab, double-click **Microsoft Root Authority** . If this certificate is lost, go to step 2.
4. On the **General** tab, ensure that the **Valid** date is **from 1/10/1997 to 12/31/2020** .
5. On the **Certification Path** tab, verify that **This certificate is OK** appears under **Certificate Status** .
6. Click **OK**, then double-click the **NO LIABILITY ACCEPTED** certificate
7. On the **General** tab, ensure the **Valid from** date value is **November 5 , 1997 to 1/7/2004** .

8. On the **Certification Path** tab, verify that **This certificate has expired or is not yet valid** or **This certificate is OK** appears under **Certificate Status** .

*Note* : Although this certificate expires, it will continue to work. The operating system may not work if the certificate is lost or canceled.

1. Click **OK** , then double-click the **GTE CyberTrust Root certificate** . You can have multiple certificates with the same name. Check the certificate that has an expiration date of 2/23/2006.
2. On the **General** tab, make sure that the **Valid from** date value is "2/23/1996 to 2/23/2006".
3. On the **Certification Path** tab, verify that **This certificate is OK** appears under **Certificate Status** .

*Note* : Although this certificate expires, it will continue to work. The operating system may not work if the certificate is lost or canceled.

1. Click **OK** , then double-click **Thawte Timestamping CA**.
2. On the **General** tab, make sure the **Valid from** date value is "12/31/1996 to 12/31/2020".
3. On the **Certification Path** tab, verify that **This certificate is OK** appears under **Certificate Status** .

### Step 2 : *Import broken or lost certificates*

If one or more of these certificates are wrong or lost, you should export these missing or corrupted certificates to another computer, then install the certificates on your computer. To actually export certificates on another computer, follow these steps:

1. In Internet Explorer, click **Tools** , then click **Internet Options** .
2. On the **Content** tab, click **Certificates** .
3. On the **Trusted Root Certification Authorities** tab, click the certificate you want to export.
4. Click **Export** , and then follow the instructions to export the certificate as a **DER encoded Binary x.509** file (**.CER**).
5. After the certificate file is exported, copy it to the computer you want to import it.
6. On the computer on which you want to import the certificate, double-click the certificate
7. Click **Install certificate** , and then click **Next** .
8. Click **Finish** , then click **OK** .

### *Method 9: Delete temporary files and restart the hotfix installation or service pack installation.*

*Note* : Ignore this method if the operating system is Windows 2000.

To delete a temporary file and restart the installation of the hotfix and service pack installation, follow these steps:

1. Delete all tmp \* .cat files in the following directories:

```
% systemroot% system32CatRoot {127D0A1D-4EF2-11D1-8608-00C04FC295EE}  
% systemroot% system32CatRoot {F750E6C3-38EE-11D1-85E5-00C04FC295EE}
```

1. Delete all kb \* .cat files in the following directories:

```
% systemroot% System32CatRoot {F750E6C3-38EE-11D1-85E5-00C04FC295EE}  
% systemroot% System32CatRoot {127D0A1D-4EF2-11D1-8608-00C04FC295EE}
```

1. Delete all the oem \*. \* Files in the **% systemroot%** inf directories
2. At the command window, type the following command. Press ENTER after each command.

```
net stop cryptsvc
ren% systemroot% System32Catroot2
oldcatroot2
net start cryptsvc
exit
```

1. Restart the failed hotfix installation or install the service pack.

#### ***Method 10: Empty the software distribution directory***

1. Click **Start** , select **Run** , type services.msc, and then click **OK** .
2. In the Services (Local) section, right-click **Automatic Updates** , then click **Stop** .
3. Minimize Services (local) window
4. Select all the contents of the Windows distribution folder, then delete them.

*Note* : By default, these folders are located in the *drive* folder: WindowsSoftwareDistribution. Here, *drive* is the drive where Windows is installed.

1. Make sure that the Windows distribution folder is empty, and then maximize the Services (local) window.
2. In the **Services (Local) section** , right-click **Automatic Updates** , then click **Start** .
3. Restart the computer, then run Windows Update again.

You finished reading the article "**Error handling cannot install updates and program settings**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.