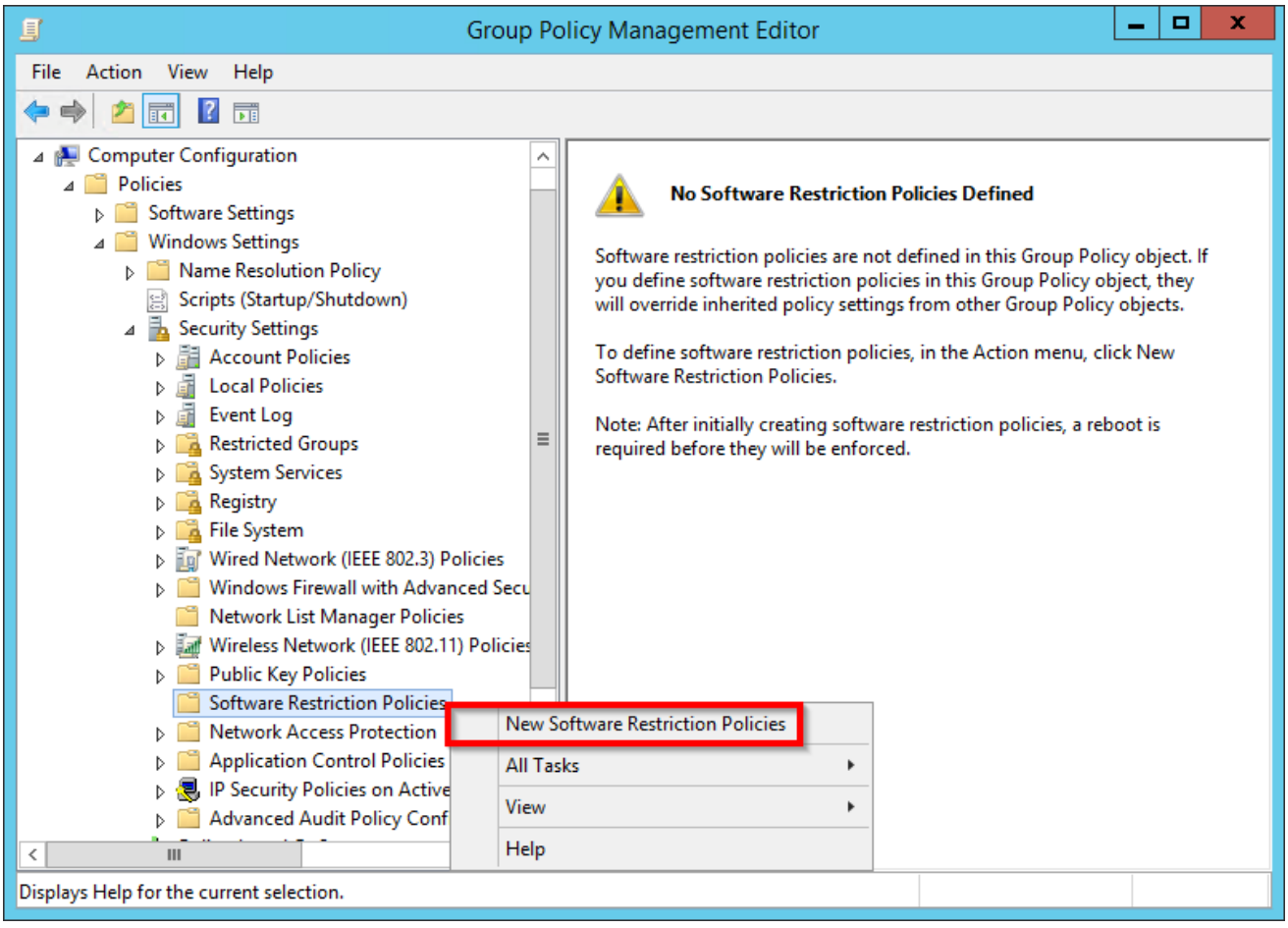
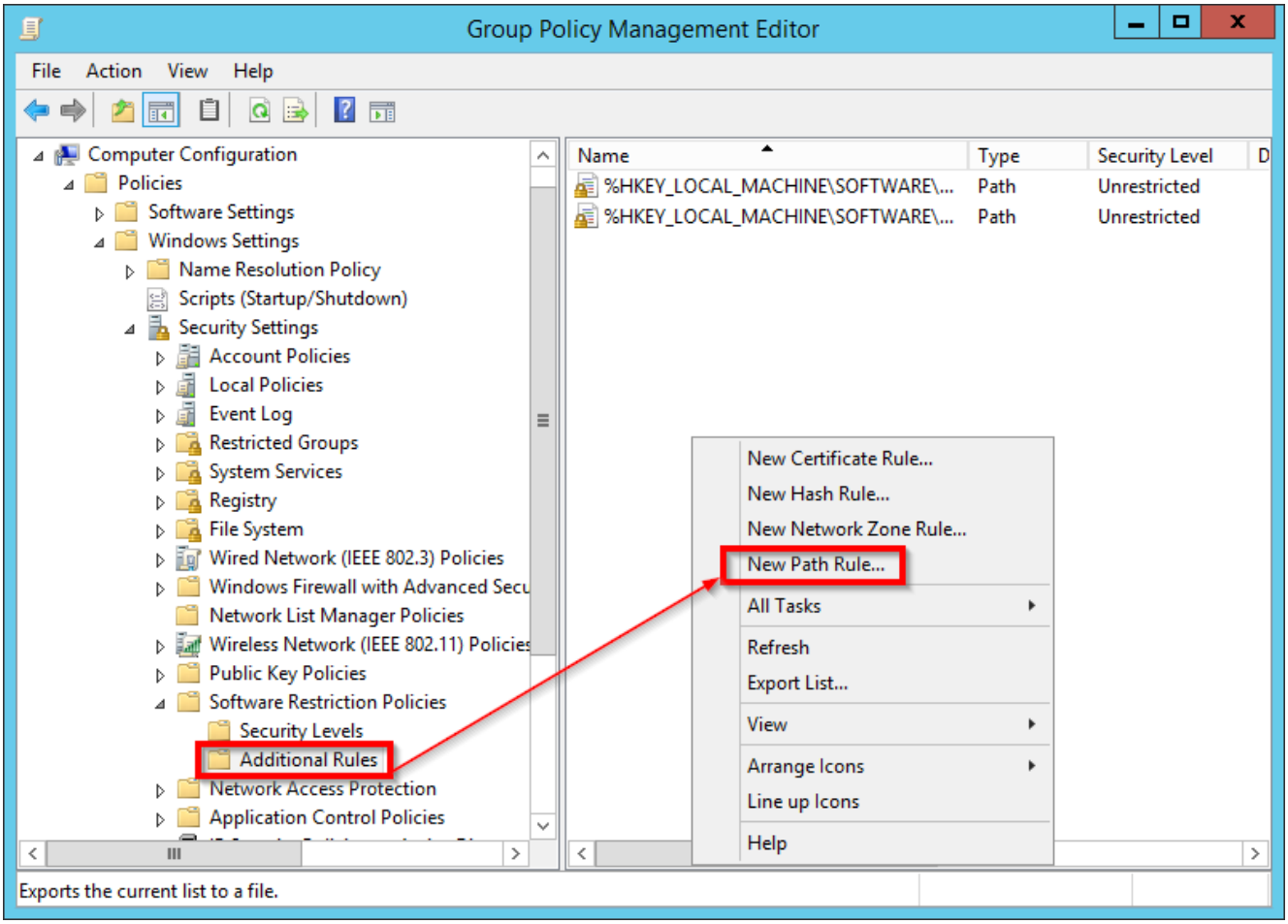
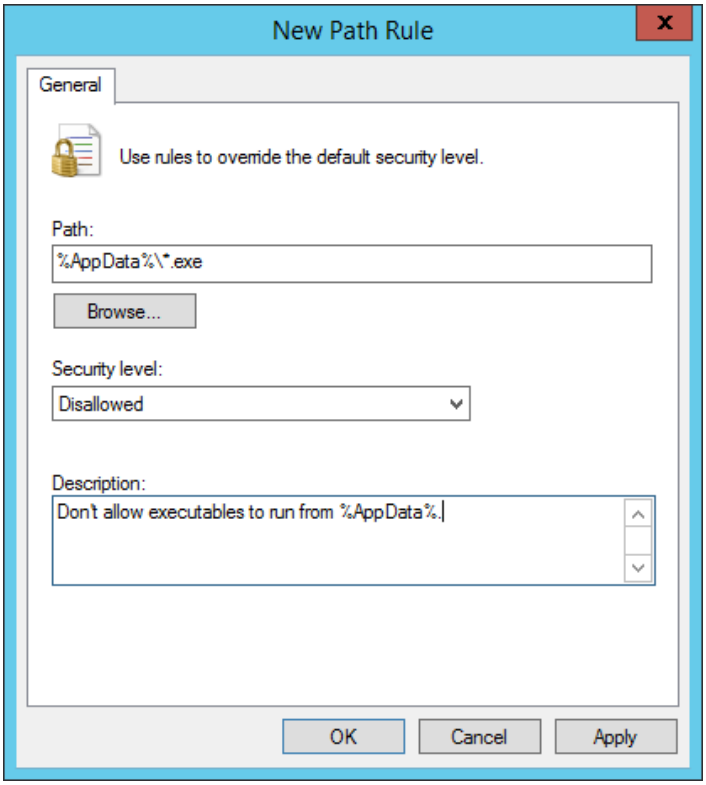
You got a virus protection in place and maybe also some other mitigation tools to protect your or company computers, but still viruses and malware can get thru into the system. Here is a method to create an extra layer of defense for your systems. We'll be using **Software Restriction Policies** that can be found in the **Local Security Policy** for standalone PC's or in the **Group Policy Management** for domain joined systems. We will be using this for blocking executables from **%APPDATA%** and **%USERPROFILE%** directories, but also from compressed archives that can be mailed with an executable as attachment, for example the Cryptovirus (TorrentLocker) or Ransomware you get nowadays from DHL and For this blogpost the screenshots and examples are made with Windows Server 2012 and Group Policy Management, but are also usable and tested by me in environments with Windows Server 2003/Windows XP and newer operation systems.



Go to **Computer Configuration** -> **Policies** -> **Windows Settings** -> **Security Settings** -> **Software Restriction Policies** and right click it to open a menu where you choose **New Software Restriction Policies**.



Open **Additional Rules** and right click it to create a **New Path Rule**.



Import the rules that are listed below.

Block executable in **%AppData%:**

- **Path:**
  %AppData%*.exe
- **Security Level:**
  Disallowed
- **Description:**
  Don't allow executables to run from %AppData%.

Block executable in **%LocalAppData%:**

- **Path if using Windows XP:**
  %UserProfile%\Local Settings*.exe
- **Path if using Windows Vista/7/8:**
  %LocalAppData%*.exe

- **Security Level:**
  Disallowed
- **Description:**
  Don't allow executables to run from %AppData%.

Block executable in **%AppData%** subfolders:

- **Path:**
  %AppData%**.exe
- **Security Level:**
  Disallowed
- **Description:**
  Don't allow executables to run from immediate subfolders of %AppData%.

Block executable in **%LocalAppData%** subfolders:

- **Path if using Windows XP:**
  %UserProfile%\Local Settings**.exe
- **Path if using Windows Vista/7/8:**
  %LocalAppData%**.exe
- **Security Level:**
  Disallowed
- **Description:**
  Don't allow executables to run from immediate subfolders of %AppData%.

Block executables run from archive attachments opened with **WinRAR**:

- **Path if using Windows XP:**
  %UserProfile%\Local Settings\Temp\Rar**.exe
- **Path if using Windows Vista/7/8:**
  %LocalAppData%\Temp\Rar**.exe
- **Security Level:**
  Disallowed
- **Description:**
  Block executables run from archive attachments opened with WinRAR.

Block executables run from archive attachments opened with **7zip**:

- **Path if using Windows XP:**
  %UserProfile%\Local Settings\Temp\7z**.exe
- **Path if using Windows Vista/7/8:**
  %LocalAppData%\Temp\7z**.exe
- **Security Level:**
  Disallowed
- **Description:**
  Block executables run from archive attachments opened with 7zip.

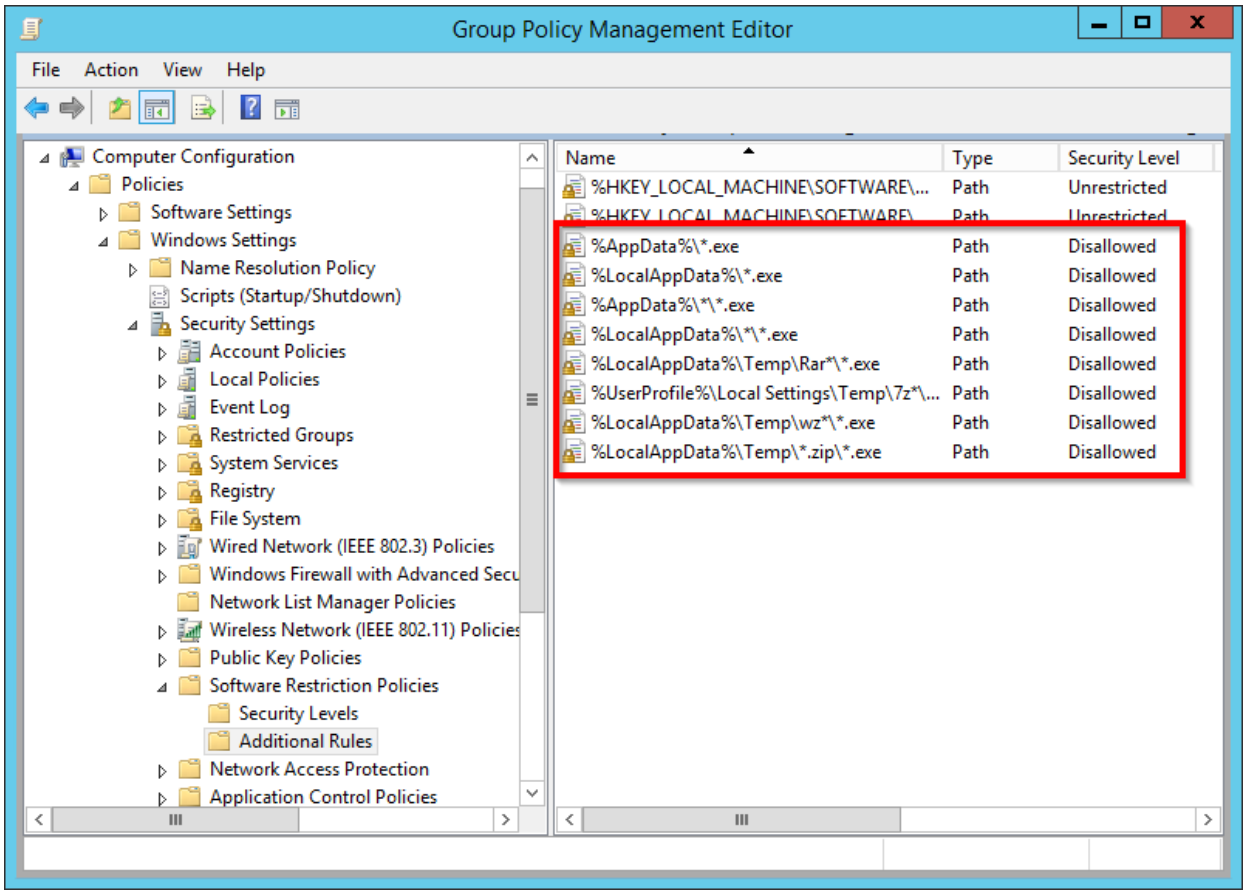
Block executables run from archive attachments opened with WinZip:

- **Path if using Windows XP:**
  %UserProfile%\Local Settings\Temp\wz**.exe
- **Path if using Windows Vista/7/8:** %LocalAppData%\Temp\wz**.exe
- **Security Level:**
  Disallowed
- **Description:**
  Block executables run from archive attachments opened with WinZip.

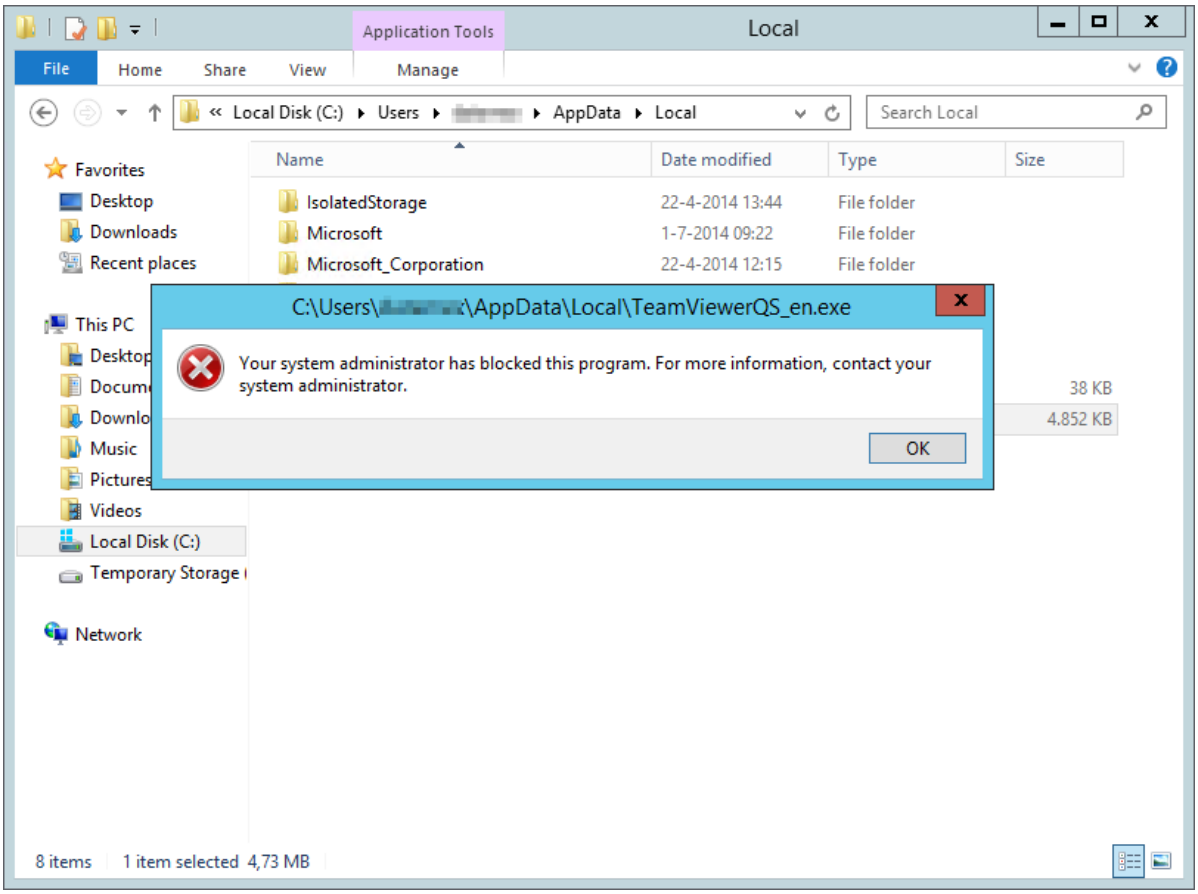
Block executables run from archive attachments opened using **Windows built-in Zip support:**

- **Path if using Windows XP:**
  %UserProfile%\Local Settings\Temp*.zip*.exe
- **Path if using Windows Vista/7/8:**
  %LocalAppData%\Temp*.zip*.exe
- **Security Level:**
  Disallowed
- **Description:**
  Block executables run from archive attachments opened using Windows built-in Zip support.

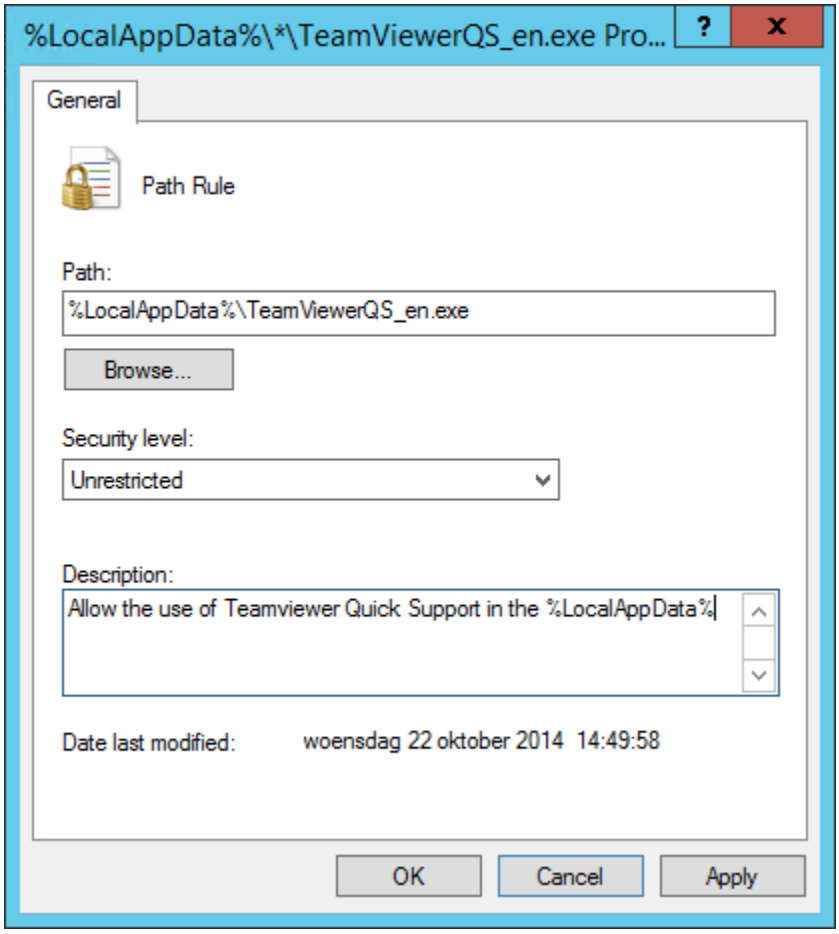
After everything is imported you get a list like this:



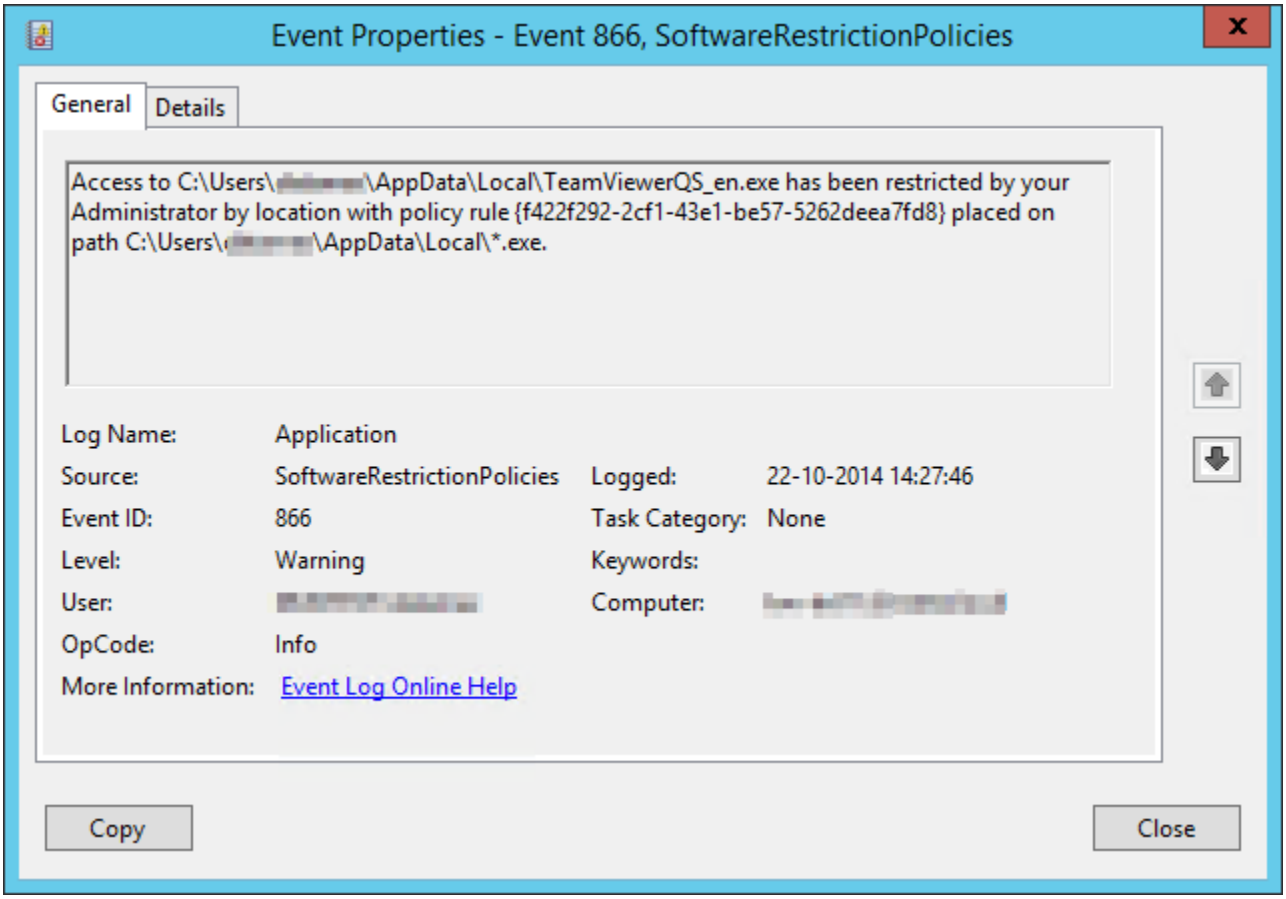
Now try running a .exe file that is located in that folder .



Voila, but the user cannot start Teamviewer with those rules what if you want an exception for this or other legitimate software. For this you can make other rules:



Make a **New Path Rule** but on the security level, choose '**unrestricted**'.


Event Properties - Event 866, SoftwareRestrictionPolicies
General
Details
Access to C:\Users\[redacted]\AppData\Local\TeamViewerQS_en.exe has been restricted by your Administrator by location with policy rule {f422f292-2cf1-43e1-be57-5262deea7fd8} placed on path C:\Users\[redacted]\AppData\Local*.exe.
Log Name: Application
Source: SoftwareRestrictionPolicies
Logged: 22-10-2014 14:27:46
Event ID: 866
Task Category: None
Level: Warning
Keywords:
User: [redacted]
Computer: [redacted]
OpCode: Info
More Information: Event Log Online Help
Copy
Close