Running LabVIEW VIs or Executables That Use .NET Assemblies From a Network Drive

Primary Software: LabVIEW Development Systems>>LabVIEW Base Package
Primary Software Version: 8.5
Primary Software Fixed Version: N/A
Secondary Software: N/A

Problem:
I have created a LabVIEW executable that uses .NET assemblies and placed this executable on a network drive. When I attempt to run this executable, I receive error 1172. How do I solve this problem?

Solution:
.NET provides several layers of security for .NET applications. The .NET Common Language Runtime (CLR) grants varying levels of trust to code based on evidence attributes (i.e application directory, publisher, site, URL and Zone) that the code possesses. One of these layers is very similar to the Zone concept in Internet Explorer.

When an assembly is loaded into .NET, access is dependent on the file location. By default, if the assembly is loaded from the local disk, it is assumed to be fully trusted. However, if it comes from the network (even a mapped drive), it is not.

If you try and access a LabVIEW VI, EXE, or LabVIEW project that uses .NET assemblies from a network drive, you should receive a System.Security.SecurityException exception that says Request failed.

There are several ways to fix this problem using .NET Framework tools such as the Code Access Secuirty Policy Tool or the .NET Framework Configuration Tool.

The Code Access Security Policy Tool creates security policy settings that tell .NET to consider a given network drive to have full trust. For example, suppose that your code was located on your E: drive, which happens to be a network mapped drive. You can add it to the trusted list by saying:

caspol -q -machine -addgroup 1 -url file://e:/* FullTrust -name "E Drive"

The .NET Framework Configuration Tool allows you to manage and configure assemblies in the GAC, adjust code access security policies, and adjust remoting services. Using this tool, you can increase your assemblies trust to full trust and thus allowing LabVIEW to run the code. Refer to the .NET Framework Configuration Tool link below for instructions and steps for increasing assembly trust.

Related Links:
KnowledgeBase 2XSBFPHM: LabVIEW and .NET Exceptions
MSDN: .NET Framework Configuration Tool (Mscorcfg.msc)
MSDN: Code Access Security Policy Tool (Caspol.exe)

Attachments:

Report Date: 09/08/2004