



Pinnacle Advisory Flash Windows XP Pro SP2 Exceptions Handling (including SQL)

PinFlash #04-003-B

Issued: August 13, 2004 and updated October 7, 2004

With the introduction of Windows XP Pro SP2, it is critical to take the steps outlined in order to allow the SQL Server broadcast and other services to pass through the enhanced XP firewall. Essentially, one must create an exception for each instance. If these steps are not taken, events did not come in real-time.

1. In all cases, for adding to the Windows Firewall exception list, follow the instructions below:
 - a. Click Start, and then click Run.
 - b. In the Run dialog box, type Firewall.cpl, and then click OK.
 - c. In the Windows Firewall dialog box, click on the Exceptions tab to add the programs outlines.

2. For the Pinnacle Database Server layer, the following is required
 - a. Add AMTLicenseMgr.exe to the Windows Firewall exception list.
 - b. Add AMTNetworkComm.exe to the Windows Firewall exception list.
 - c. Add CkptScheduler.exe to the Windows Firewall exception list.
 - d. Add Pinnacle.exe to the Windows Firewall exception list.
 - e. Add DCS.exe to the Windows Firewall exception list.
 - f. Add TCP Port 135 to the Windows Firewall exception list.
 - g. Add sqlservr.exe to the Windows Firewall exception list thus allowing SQL server to open User Datagram Protocol (UDP) port 1434
 - h. Change the Local Security Policy Network Access/Sharing and security model for local accounts to Classic – local users authenticate as themselves.

Note #1:

With regards to SQL, reference: Microsoft Knowledge Base [841252](#) How to enable TCP/IP on Windows XP Service Pack 2 for SQL Server 2000. If you are running multiple instances of SQL Server, you will have to create an exception for each instance.

In the Add Program dialog box, you can select an instance of SQL Server or you can click the Browse button to locate the instance of SQL Server that you want to add to the exception list. The default installation locations for SQL Server are listed in the following table.

Version	File path
SQL Server 7.0	Mssql\Binn\Sqlservr.exe
SQL Server 2000 Default Instance	Program Files\Microsoft SQL Server\Mssql\Binn\Sqlservr.exe
SQL Server 2000 Named Instance	Program Files\Microsoft SQL Server\Mssql\$\instancename\Binn\Sqlservr.exe

Note #2:

Also found that when running Windows XP SP1a you need to make the same Local Security Policy change above when it is the Database server -- necessary when you have clients. The symptom when this is not done is that the application is fully accessible except for the Device Setup screen (e.g., an ADO connection error occurs)

3. For the Pinnacle Client layer, the following is required:
 - a. Add AMTLicenseMgr.exe to the Windows Firewall exception list.
 - b. Add AMTNetworkComm.exe to the Windows Firewall exception list.
 - c. Add Pinnacle.exe to the Windows Firewall exception list.
 - d. Add TCP Port 135 to the Windows Firewall exception list.
 - e. Change the Local Security Policy Network Access/Sharing and security model for local accounts to Classic – local users authenticate as themselves.

4. For the Pinnacle Hardware Server layer, the following is required:
 - a. Add AMTLicenseMgr.exe to the Windows Firewall exception list.
 - b. Add AMTNetworkComm.exe to the Windows Firewall exception list.
 - c. Add Pinnacle.exe to the Windows Firewall exception list.
 - d. Add DCS.exe to the Windows Firewall exception list.
 - e. Add TCP Port 135 to the Windows Firewall exception list.
 - f. Change the Local Security Policy Network Access/Sharing and security model for local accounts to Classic – local users authenticate as themselves.

-- END --