



## Knowledge Base Article

### Configuring AMS Device Manager to be used with Windows XP, SP2

|                         |                     |
|-------------------------|---------------------|
| <b>Article ID:</b>      | NA-0400-0080        |
| <b>Publish Date:</b>    | 07 Sep 2004         |
| <b>Article Status:</b>  | Approved            |
| <b>Article Type:</b>    | Product Issues/Tips |
| <b>Required Action:</b> | As Needed           |

#### Recent Article Revision History:

| Revision/Publish | Description of Revision                                   |
|------------------|---|
| 07 Sep 2004      | Updated to include Terminal Services and update PLD & RCD |

(See end of article for a complete revision history listing.)

#### Affected Products:

| Product Line | Category      | Device          | Version |
|--------------|---------------|-----------------|---------|
| AMS          | General (FAQ) | Common Problems |         |

## Description

Microsoft is incorporating new security features in Service Pack 2 for Windows XP which will impact the operation of AMS Device Manager and AMS Device Manager Web applications. Effectively, this Service Pack automatically enables the firewall protection built into Windows XP and this has implications for any application that employs varying types of communications or access methods.

This document contains the changes required for AMS Device Manager 6.2 and AMS Device Manager Web users to allow these applications to function properly when installed on the Windows XP operating system with Service Pack 2 installed. The following configuration procedures are required for proper application operation.

#### 1) Configuring 'Local Security Settings'

The 'Local Security Settings' needs to be modified on each AMS Device Manager Workstation and any remote AMS Device Manager Web server installation PCs. This is necessary for AMS Device Manager to function when all XP Professional stations are in a Workgroup. This is due to the fact that all of the AMS Device Manager server processes set their DCOM 'Authentication Level' to 'None' in order to allow anonymous connections.

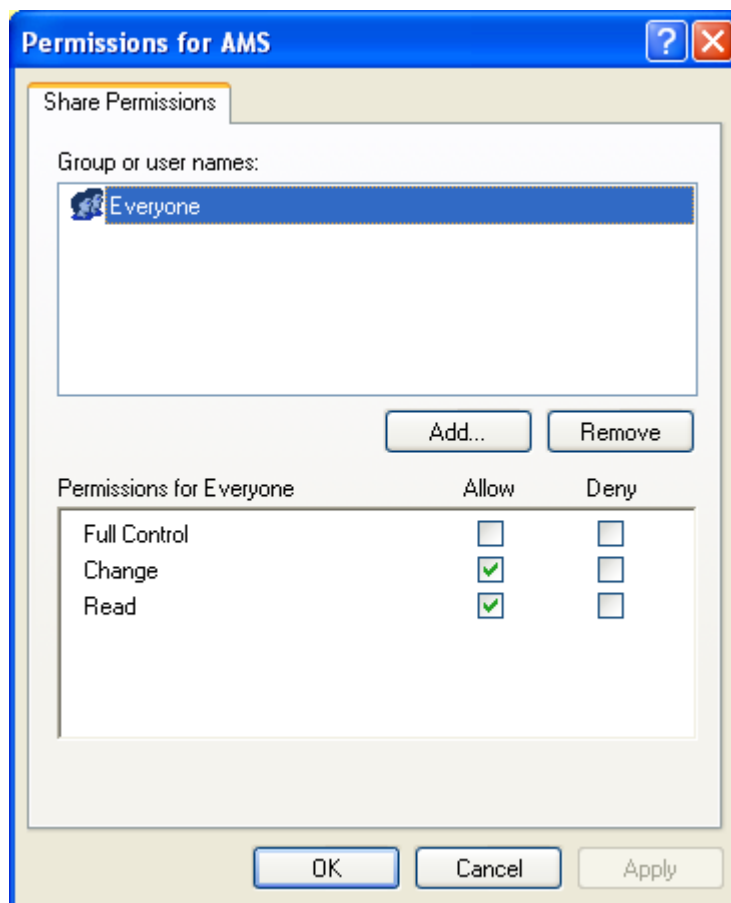
- i) Go to Start → Administrative Tools → Local Security Policy
- ii) When the Local Security Settings window open, traverse to; Local Security Settings → Local Policies → Security Options → Network access: 'Sharing and security model for local accounts' needs to be set to 'Classic – local users authenticate as themselves'.

#### 2) Setting Permissions For Drawings / Notes

In order to open and edit a Device Service Notes file on a remote station, the AMS directory on the Server Plus station must have Read and Change permissions set for the Everyone account. This can be accomplished by doing the following:

- i) Right-click on the AMS directory and select Properties
- ii) Select the Sharing tab on the AMS Properties dialog

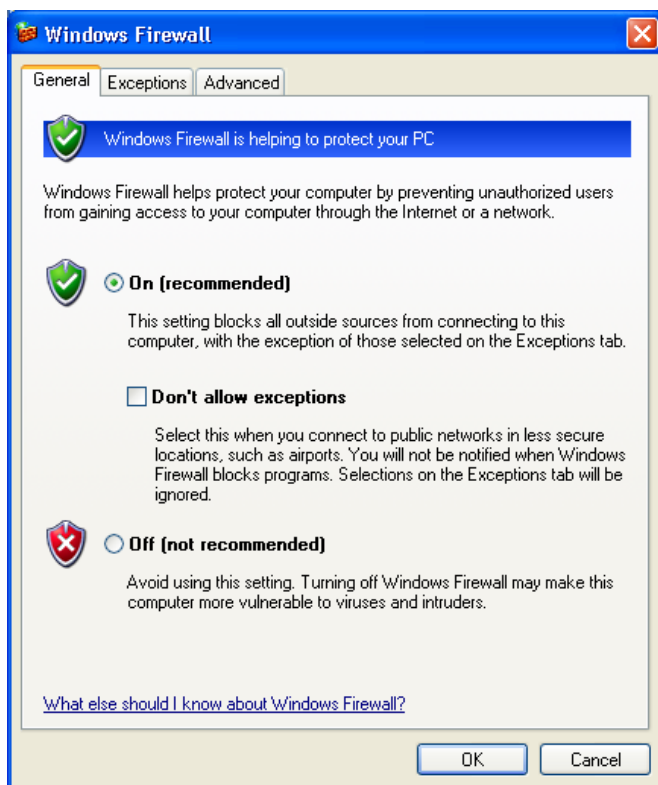
- iii) Select the Permissions button on the AMS Properties dialog
- iv) Select the Everyone user name in the 'Group or user names' window on the Permissions for AMS dialog
- v) Select the Change and Read check boxes in the 'Permissions for Everyone' window on the Permissions for AMS dialog



### 3) How to access and configure the Windows Firewall (This will be used in sections 3, 4, and 5)

#### a) Turning Windows Firewall On/Off

- i) By default the Windows Firewall is set to "On". This setting is recommended by Microsoft to give your machine the highest possible protection. For trouble shooting communication failures or if the machine is sufficiently protected behind a corporate firewall, it may be appropriate to turn off the Windows Firewall.



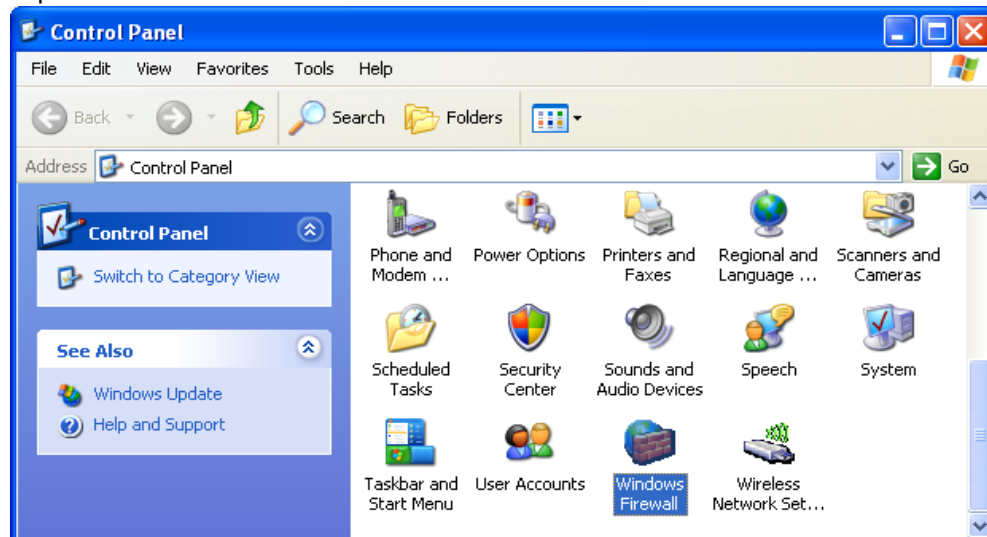
b) Setting up FIREWALL EXCEPTIONS

- i) The Windows Firewall allows traffic across the network interface when initiated locally, but by default stops any incoming “unsolicited” traffic. However, this firewall is “exception” based, meaning that the administrator can specify applications and ports that are exceptions to the rule and can respond to unsolicited requests.  
The firewall exceptions can be specified at two main levels-

- the application level
- the port and protocol level

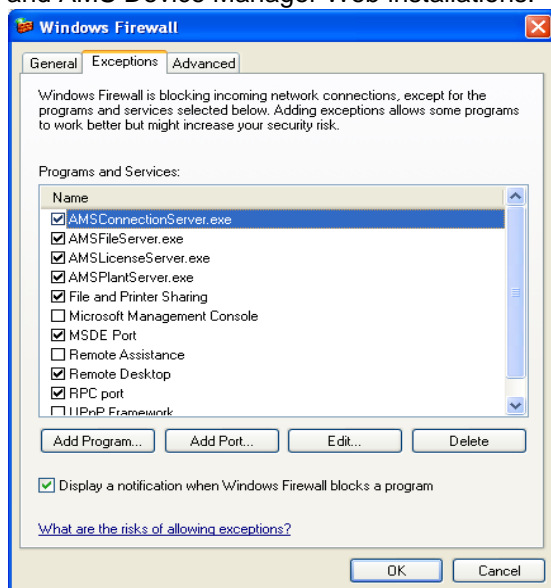
The application level is where you specify which applications are able to respond to unsolicited requests. The port and protocol level is where you can specify the firewall to allow or disallow traffic on a specific port for either TCP or UDP traffic. To make AMS Device Manager work in a client/server configuration, changes need to be made on both levels.

- ii) The following procedure shows how to add programs and services to the list of network connections so they do not get blocked by the Windows Firewall.  
(1) Open Control Panel and double click on the Windows Firewall icon.



The Windows Firewall window will open.

- (2) The following Windows Firewall screen capture may not accurately reflect the complete list of exceptions. Refer to the tables in the following sections for the complete list of programs and ports that should be added to this exceptions list for the perspective AMS Device Manager and AMS Device Manager Web installations.



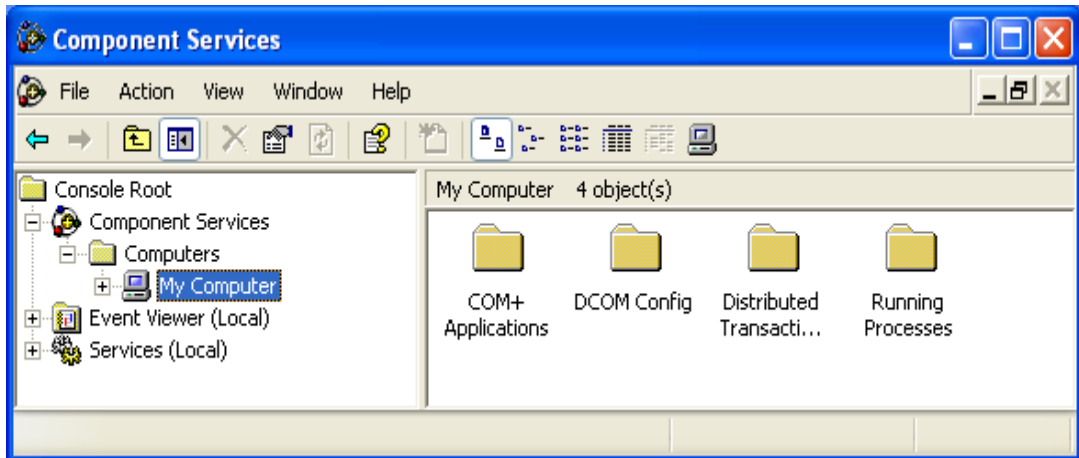
- (3) The following will define each button on the “Exceptions” tab:
- Add Program: This button allows the user to select a program to be added to the list.
  - Add Port: This button allows the user to specify a port number along with a descriptive name which will be added to the list.
  - Edit: This button allows the user to specify/change the set of computers for which the port or program is unblocked.
  - Delete: This button will remove the selected name from the exceptions list.
- c) Changing Exception Scope
- When opening a port or allowing a program, the set of IP addresses from which the unsolicited incoming traffic is allowed can be defined. This set of IP addresses from which unsolicited incoming traffic are allowed is the scope of the exception. There are three options when defining the scope for a Windows Firewall exception:
    - All IP addresses – This is the default scope for a Windows Firewall exception, and it allows unsolicited incoming traffic that matches the exception from any computer.
    - Local subnet only – This scope allows unsolicited incoming traffic that matches the exception from any computer on the same subnet as the network connection on which the traffic was received through Windows Firewall, while dropping unsolicited incoming traffic from all other computers.
    - Custom – The final option is to define a custom scope, which is a list of IPv4 addresses and address ranges that typically correspond to subnets. Unsolicited incoming traffic that matches the exception and originates from a computer with an IPv4 address in the defined list is allowed through Windows Firewall. Unsolicited incoming traffic from computers with IPv4 addresses that are not in the list is dropped.

The default scope is used for all programs and ports that we add to the Windows Firewall exceptions list. At a minimum all of the AMS Device Manager stations and remote client stations need to be within the defined scope. Therefore, if the defined scope is changed to:

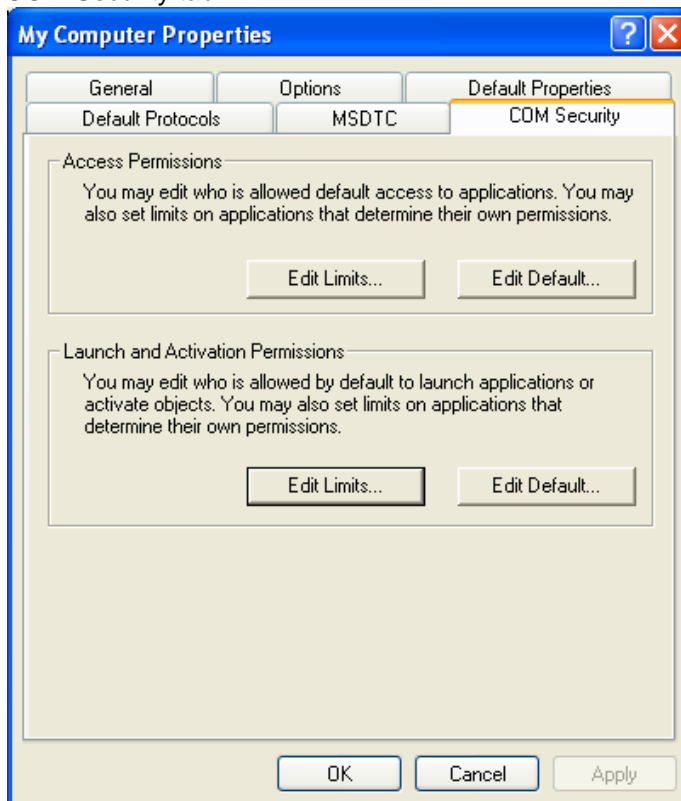
    - ‘Local subnet only’ - All AMS Device Manager stations and remote client stations need to be located in the local subnet.
    - ‘Custom’ - Each of the IPv4 addresses of the AMS Device Manager stations and remote client stations need to be defined in the custom list.
- d) Setting up COM SECURITY LIMITS
- To overcome a security issue, Microsoft has added “limits” to the DCOM security settings from Launch and Access to limit the permissions that an application can use. This limit prevents the application from using permissions beyond what is specified in the DCOM configuration settings. By default the limits set by Service Pack 2 will not allow for AMS Device Manager to communicate over the network. One must now specify if the user or group specified has permissions locally or

remotely (or both). In order for AMS Device Manager to work over the network with DCOM, the permissions must be set such that remote users can launch and/or access the AMS Device Manager servers.

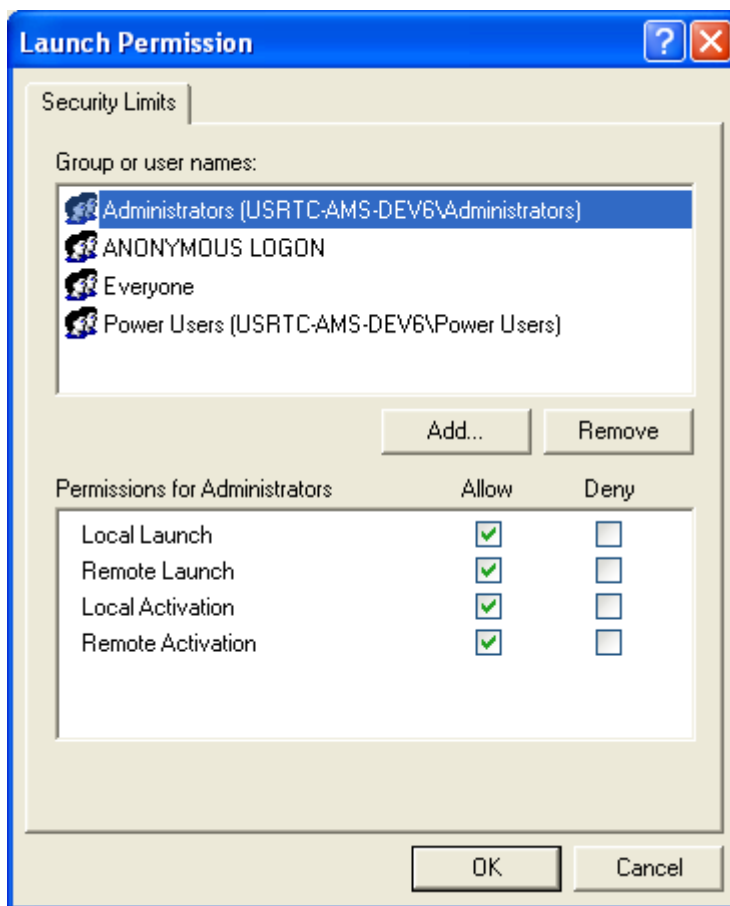
- ii) The following shows how to modify the system wide default Launch and Activation permissions. Similar steps are taken to modify the system wide default Access permissions
  - (1) Open Control Panel and double click on Administrative Tools.
  - (2) From Administrative Tools, double click on the Component Services icon. The Component Services window will open.
  - (3) Under Console Root, expand Component Services and then expand Computers.



- (4) Right click on My Computer and choose properties, the following window will open. Go to the COM Security tab.



- (5) Click on the 'Edit Limits...' under the 'Launch and Activation Permissions' section of the window. Note: You would click on the 'Edit Limits...' under the 'Access Permissions' section of the window to display the Access permissions dialog.



- (6) Click on each group and verify that all permissions are set appropriately. Refer to the tables in sections 3, 4, and 5 for the Group names and permissions that should be set on each station type. For each user or group that participates in AMS Device Manager communication (e.g. Power Users and ANONYMOUS LOGON), make sure that both the **Local Allow** and **Remote Allow** checkboxes are checked.

**4) Configuring the Windows Firewall**

**a) Server+, Server and Client PC configuration Changes**

- i) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for all stations within a Server+, Server and Client configuration. The "Ref #" in this table references the "Ref #" in the Troubleshooting table found in section (6) to find out what problem is solved by the given firewall configuration change.

| Change  | Server+ | Server | Client | Ref # |
|---|---------|--------|--------|-------|
| Add File and Printer Sharing to the exceptions list   | X       | X      | X      | 23    |
| Add AMSLicenseServer.exe to the exceptions list   | X       |        |        | 3     |
| Add AMSRemoteCheck.exe to the exceptions list   | X       | X      |        | 4     |
| Add STARTUP.exe to the exception list   | X       | X      |        | 5     |
| Add PtmServer.exe to the exception list   | X       | X      |        | 5     |
| Add AMSPlantServer.exe to the exception list  | X       | X      |        | 10    |
| Open port 135   | X       | X      |        | 7,8   |
| Open port 1433  | X       |        |        | 9     |
| Add ANONYMOUS LOGON to the Access Permissions and Launch and Activation Permissions Limits dialog (local and remote). | X       | X      |        | 1,2   |
| Add Power User to the   | X       | X      |        | 6     |

|  |  |  |  |  |
|--|--|--|--|--|
| Launch and Activation<br>Permissions Limits (local and remote) |  |  |  |  |
|--|--|--|--|--|

**Note:** When AMS Device Manager is installed on a Client station that is in a network Workgroup (instead of on a network domain), the current logged on user name and password on the Client station must exist on the Server+ and or Server station that the Client is connecting to. If not, AMS Device Manager will not be able to be started from the Client station because it will fail to start the Plant Server. This is a known issue and is by (Microsoft) design.

**b) Terminal Services**

i) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for the local and remote pc. The Ref # in this table can be used with the Ref # in the Troubleshooting table to find out what problem is solved by the given firewall configuration change. Local PC is the machine where Remote Desktop Connection is run. Remote PC is the machine you connect to via Remote Desktop Connection.

| Change                                   | Remote PC | Local PC | Ref # |
|--|-----------|----------|-------|
| Add Remote Desktop to the exception list | X         |          | 31    |

**c) ValveLink SNAP-ON**

i) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for all stations within a Server+, Server and Client configuration and the user has installed and is attempting to launch the ValveLink SNAP-ON from the client or server station. The "Ref #" in this table references the "Ref #" in the Troubleshooting table found in section (6) which describes what problem is solved by the given firewall configuration change.

| Change  | Server+ | Server | Client | Ref # |
|---|---------|--------|--------|-------|
| Add VLCOMM.exe to the exception list.   |         |        | X      | 18    |
| Open port 6660  |         | X      | X      | 18    |
| Open port 135   |         |        | X      | 18    |
| Add Power User to the Access Permissions and Launch and Activation Permissions Limits (local and remote)          | X       | X      | X      | 18    |
| Add ANONYMOUS LOGON to the Access Permissions and the Launch and Activation Permissions Limits (local and remote) |         |        | X      | 19    |

**Note:**

1. The errors described in #18 are also seen when refreshing the device list in ValveLink while the plant and file servers are not running on each of the configured server stations.
2. The error message; "Unable to Connect to PlantServer <server station name>" is written to the NT event log on the Client station if a configured server station does not have at least one network (HSL/modem) configured.

**d) Remote OPC Client**

i) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for all stations within a client/server/server+ configuration and the user is attempting to launch a remote OPC client from the client or server station. Examples of SNAP-ONS that are considered OPC clients are as follows:

- Engineering Assistant (EA)
- QuickCheck
- Plugged Line Diagnostic (PLD) \*
- Root Cause Diagnostic (RCD) \*\*
- ValVue

The Ref # in this table can be used with the Ref # in the Troubleshooting table to identify what problems might be solved by the given firewall configuration change.

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

| Change                                | Server+ | Server | Client | Ref #     |
|---------------------------------------|---------|--------|--------|-----------|
| Add AMSOPC.exe to the exception list. |         | X      |        | 20, 21,22 |

**\* The Plugged Line Diagnostic (PLD)**

Additional programs and ports need to be added to the exceptions list in addition to the Remote OPC Client requirement in the table above. See below for the additional requirements for PLD. The SNAP-ON column refers to the station where the SNAP-ON application is running. The OPC Server column refers to the station where the OPC Server (e.g. DeltaV OPC Server) is running.

| Change   | SNAP-ON | Server | OPC Server | Ref # |
|--|---------|--------|------------|-------|
| Add the OPC server to the exception list (e.g. DeltaV OPC Server). |         |        | X          | 24    |
| Add File and Printer Sharing to the exceptions list                |         |        | X          | 25    |
| Add PLD_Monitor.exe to the exception list.                         | X       |        |            | 20    |
| Add PLD_Configure.exe to the exception list.                       | X       |        |            | 26    |
| Open port 135  | X       |        | X          | 27    |

**\*\* The Root Cause Diagnostic (RCD)**

The Remote OPC Client requirement in the table above is not a requirement for RCD. The programs and ports that need to be added to the exceptions list for RCD can be found in the table below. The SNAP-ON column refers to the station where the SNAP-ON application is running. The OPC Server column refers to the station where the OPC Server (e.g. DeltaV OPC Server) is running.

| Change   | SNAP-ON | Server | OPC Server | Ref # |
|--|---------|--------|------------|-------|
| Add RCD_Monitor.exe to the exception list.                         | X       |        |            | 29    |
| Add RCD_Configure  | X       |        |            | 29    |
| Open port 135  | X       |        | X          | 30    |
| Add the OPC server to the exception list (e.g. DeltaV OPC Server). |         |        | X          | 29    |
| Add File and Printer Sharing to the exceptions list                |         |        | X          | 28    |

**5) AMS Device Manager Web Services**

- a) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for all stations within an AMS Device Manager Web Services configuration. The "Ref #" in this table references the "Ref #" in the Troubleshooting table found in section (6) to find out what problem is solved by the given firewall configuration change. The Web Services column represents the station where Web Services are deployed (Server Plus or Single Workstation).

| Change       | Web Services | Ref # |
|--------------|--------------|-------|
| Open port 80 | X            | 15    |

**6) AMS Device Manager Web Server/AMS Device Manager Web Client connecting to a Server+ or Single Workstation**

- a) The following table shows the list of changes that need to be made when the Windows Firewall has been turned on for all stations within an AMS Device Manager Web configuration. The "Ref #" in this table references the "Ref #" in the Troubleshooting table found in section (6) to find out what problem is solved by the given firewall configuration change. The Web Server column represents the station where the Web Server and IIS are installed. This may or may not be an AMS Device Manager station

| Change   | Web Browser   | Web Server | Server+ | Single Workstation | Ref # |
|--|---|------------|---------|--------------------|-------|
| Add AMSLicenseServer.exe to the exceptions list  |   |            | X       | X                  | 3     |
| Add AMSGenericExports.exe to the exception list  |   |            | X       | X                  | 11    |
| Add AMSConnectionServer.exe to the exception list  |   |            | X       | X                  | 12    |
| Add File and Printer Sharing to the exceptions list  |   | X          |         |                    | 23    |
| Open port 135  |   |            | X       | X                  | 13,14 |
| Open port 1433   |   |            | X       | X                  | 9     |
| Open port 80   |   | X          |         |                    | 15    |
| Add ANONYMOUS LOGON to the Launch and Activation Permissions Limits dialog (local and remote). |   |            | X       | X                  | 17    |
| Add Power User group to the Default COM Security Access Permissions list                       | X<br>Note: This was only needed when the web browser was on a non-XP SP2 station. |            |         |                    | 16    |

## 7) Troubleshooting

- a) The following table shows a list of problems that have been resolved by a particular Firewall configuration. The Ref # in this table can be used in conjunction with the Ref # in one of the Firewall Configuration tables to find out which firewall configuration change was made to fix the problem.

| Ref # | Description   |
|-------|---|
| 1     | This change is required to allow anonymous connection to the AMS Device Manager servers. Without these changes the user will get the following error message when attempting to launch AMS Device Manager: 'The Plant Server: <name> is not properly licensed.'   |
| 2     | This change is required to allow anonymous connection to the AMS Device Manager servers. Without these changes on the Server station, when performing a db backup on the Server Plus station, the following messages will be displayed in the NT event log:<br>a) Access is denied.<br>- Unable to determine if AMS servers are running on <server station name><br>b) Checking for Connection server mutex failed 80070005<br>c) Checking for Generic Export server mutex failed 80070005<br>d) Checking for file server mutex failed 80070005 |
| 3     | a) The user receives a Licensing is unable to connect to the License Server error message when attempting to launch the AMS Device Manager servers on a server station.<br>b) An error in the NT event log on the server station: DCOM got error "The RPC server is unavailable." from the computer <server plus name> when attempting to activate the server: {1453AA94-8299-11D3-8268-006097B5648F}.  |
| 4     | Without this change on the Server station, the user will get a DCOM error on the Server Plus when performing a database backup stating the RPC server is unavailable.   |
| 5     | Without this change on the Server station, the user will get PTM communication errors when AMS Device Manager is started and an RS3 HSI is configured.  |
| 6     | This change is required to allow the AMS Device Manager user the ability to launch and access the AMS Device Manager servers. Without this change, the user will be unable to launch AMS Device Manager on a Client station (access denied trying to activate the server).  |
| 7     | Without this port being opened, the AMS Device Manager application can not be launched on a Client station. The user would get a 'Licensing is unable to connect to the License Server' error. A DCOM error would also be written to the NT event log on the Client station   |

|    |  |
|----|--|
|    | stating DCOM was unable to communicate with the Server Plus station. The same may hold true when attempting to launch AMS Device Manager web from an AMS station via a web browser.  |
| 8  | Without this port being opened on the Server Plus station, the AMS Device Manager application can not be launched on a Server station. The user would get a 'Licensing is unable to connect to the License Server' error. A DCOM error would also be written to the NT event log on the Server station stating DCOM was unable to communicate with the Server Plus station.  |
| 9  | Database error (Error: Unable to initialize DbWrap layer.) if this port is closed.   |
| 10 | Without this change, a user is unable to launch AMS Device Manager from a Client station. The user would get an 'Error starting AMS server' error.   |
| 11 | DCOM got error "The RPC server is unavailable. " from the computer <server plus name> when attempting to activate the server: {A0C824EB-C599-4F3E-929B-FAF12DD5FECD}.  |
| 12 | <ol style="list-style-type: none"> <li>The following error is written to the NT event log on the web server station: "The launch and activation security descriptor for the COM Server application with CLSID {2A6D72F1-6E7E-4702-B99C-E40D3DED33C3} is invalid. It contains Access Control Entries with permissions that are invalid. The requested action was therefore not performed. This security permission can be corrected using the Component Services administrative tool."</li> <li>The message: "AMS Device Manager is not running" is displayed on the AMS Device Manager web logon page.</li> <li>DCOM got error "The RPC server is unavailable. " from the computer &lt;server plus name&gt; when attempting to activate the server: {108ACB43-3D46-455B-8AEB-CF6996453D83}.</li> </ol> |
| 13 | Get the following error when attempting to launch the DCOM servers on the server station: "DCOM was unable to communicate with the computer <server plus name> using any of the configured protocols."   |
| 14 | Without this port being opened on the Server Plus station, the user will be unable to logon to AMS Device Manager web via a web browser. They will receive the following error in their NT event log on the web browser station: "An error has occurred on the socket connecting the FMS Server!".   |
| 15 | Without this change the user will receive a "Cannot find server or DNS Error" within the browser window when attempting to launch AMS Device Manager web.  |
| 16 | This change is required to allow the AMS Device Manager user the ability to access the AMS Device Manager servers. Without this change the user is able to log onto AMS Device Manager web, but they will receive an Access Denied error when attempting to launch Alert Monitor, Audit Trail, or Record Manual Event from the Plant Locations icon.   |
| 17 | This change is required to allow anonymous connection to the AMS Device Manager servers. The message: "AMS Device Manager is not running." Is displayed on the AMS Device Manager web logon page.  |
| 18 | <p>This change is required to allow the AMS Device Manager user the ability to launch and access the AMS Device Manager servers. Without these changes the ValveLink SNAP-ON will be unable to display information about the device from which the SNAP-ON was launched.</p> <p>AND/OR</p> <p>The following errors/warnings can be found in the NT event log on the Client station:</p> <ul style="list-style-type: none"> <li>- Socket error connecting to server &lt;server plus name&gt; on port 6660 for reason 10060.</li> <li>- Cannot make connection to server &lt;server plus name&gt;.</li> <li>- Unable to perform newroot with &lt;server plus name&gt;.</li> <li>- Unable to connect to PlantServer</li> </ul>  |
| 19 | This change is required to allow anonymous connection to the AMS Device Manager servers. Without this change the ValveLink SNAP-ON will display an error message to the user on the Client station stating it could not communicate with the device whenever an attempt is made to access the device via ValveLink.  |
| 20 | <p>Without this change the monitoring of a transmitter via PLD_Monitor.exe will fail. A Plugged Line Diagnostic error message will be displayed to the user on the client station indicating the following:</p> <ul style="list-style-type: none"> <li>- Failed to read the device configuration for the transmitter.</li> <li>- Cannot connect to AMS OPC Server.</li> <li>- You may not have the appropriate rights.</li> </ul>  |
| 21 | A DCOM error is written to the NT event log on the client station indicating the RPC server is unavailable when trying to activate the AMS OPC Server.   |

|    |   |
|----|---|
| 22 | Without this change the message "Connecting to OPX Server Failed" will be displayed to the user when attempting to launch the OPC Client application.   |
| 23 | "File & Printer Sharing" need to be added to the Exceptions List so other PC's can see/ping the station (for Terminal Services, Remote AT logging, other?)  |
| 24 | <p>a) Configuration of a transmitter via PLD_Configure.exe will fail. A PLD error message will be displayed to the user indicating that it could not connect to the OPC Server. An event is written to the NT event log indicating the RPC server is unavailable.</p> <p>b) Monitoring of a transmitter via PLD_Monitor.exe will fail. An error message will be displayed to the user indicating the following: failed to configure the transmitter with an AMS Tag, and cannot connect to the OPC Server.</p>  |
| 25 | <p>a) Configuration of a transmitter via PLD_Configure.exe will fail. An error message will be displayed to the user indicating it failed to get the OPC Servers.</p> <p>b) Monitoring of a transmitter via PLD_Monitor.exe will fail. An error message will be displayed to the user indicating the following: failed to configure the transmitter with an AMS Tag, and cannot connect to the OPC Server.</p>  |
| 26 | Configuration of a transmitter via PLD_Configure.exe will fail. An error message will be displayed to the user indicating it cannot connect to the OPC Server.  |
| 27 | <p>When port 135 is not opened on the OPC Server station:</p> <p>a) Unable to launch PLD_Configure.exe since the AMS Device Manager application cannot be started.</p> <p>b) Monitoring of a transmitter via PLD_Monitor.exe will fail. An error message will be displayed to the user indicating there was an error communicating with the AMS Server.</p> <p>When port 135 is not opened on the SNAP-ON station:</p> <p>a) Monitoring of a transmitter via PLD_Monitor.exe will fail. An error message will be displayed to the user indicating it cannot connect to the OPC Server.</p> <p>b) Monitoring of a transmitter via PLD_Monitor.exe will fail. A Plugged Line Diagnostic error message will be displayed to the user indicating it failed to read the device configuration for the transmitter and that it cannot connect to AMS OPC Server.</p> |
| 28 | An error message is displayed to the user indicating the configured OPC Server is not available from the remote machine.  |
| 29 | An error message is displayed to the user indicating a connection to the OPC Server could not be established.   |
| 30 | <p>When port 135 is not opened on the OPC Server station:</p> <p>a) Configuration of a transmitter via PLD_Configure.exe will fail. An error message will be displayed to the user indicating an OPC Server connection failure. An NT event log is written indicating DCOM was unable to communicate with the OPC Server station using any of the configured protocols.</p> <p>b) Monitoring of a transmitter via PLD_Monitor.exe will fail. An error message will be displayed to the user indicating there was an error communicating with the AMS Server.</p> <p>When port 135 is not opened on the SNAP-ON station an error message will be displayed to the user indicating the configured OPC Server is not available from the remote machine.</p>  |
| 31 | An error message is displayed to the user indicating the client could not connect to the remote computer.   |

#### Complete Article Revision History:

| Revision/Publish | Description of Revision                                   |
|------------------|---|
| 19 Aug 2004      | Original release of article                               |
| 07 Sep 2004      | Updated to include Terminal Services and update PLD & RCD |

Services Are Delivered Through  
 Our Global Services Network.  
 To Reach Us, Go To The World  
 Wide Web:  
[www.emersonprocess.com/systems/reach/](http://www.emersonprocess.com/systems/reach/)

DeltaV, PROVOX, AMS, RS3, and PlantWeb are marks of Emerson Process Management LLLP. All other marks are the property of their respective owners. While this information is presented in good faith and believed to be accurate, Emerson Process Management LLLP does not guarantee satisfactory results from reliance upon such information. NOTHING CONTAINED HEREIN IS TO BE CONSTRUED AS A WARRANTY OR GUARANTEE, EXPRESS OR IMPLIED, REGARDING THE PERFORMANCE, MERCHANTABILITY, FITNESS, OR OTHER MATTER WITH RESPECT TO THE PRODUCTS, NOR AS A RECOMMENDATION TO USE ANY PRODUCT OR PROCESS IN CONFLICT WITH ANY PATENT. Emerson Process Management LLLP reserves the right, without notice, to alter or improve the designs or specifications of the products described herein.

© 2004 Emerson Process Management LLLP All rights reserved.