

TECHNICAL BULLETIN 43

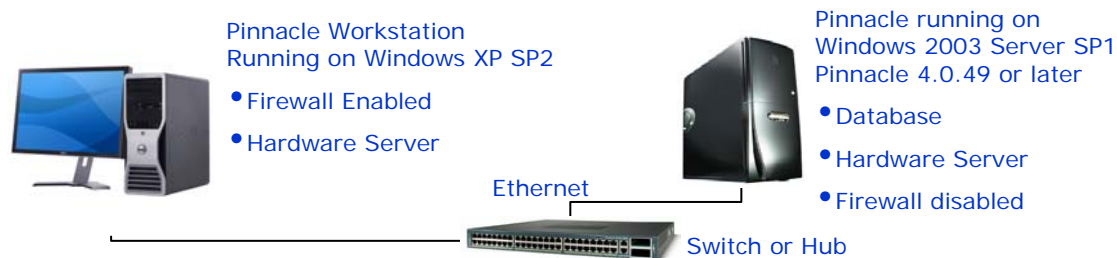
Firewall Settings for Pinnacle

Pinnacle's installation program opens ports and adds firewall exceptions so that server components can be remotely accessed. This technical bulletin discusses how Pinnacle components communicate remotely and what steps are required to allow the application to run normally between the Pinnacle Server and Workstations.

Pinnacle utilizes a number of technologies in support of its thick client implementation. For example:

- 1 Event Grid receives and retrieves messages from the Database.
- 2 Device Setup Tree use DCOM.
- 3 Cardholder Screen Images use Remote File Access.

Typical Pinnacle Server – Workstation Configuration



Note: Network configuration will vary per installation

In order to determine a successful configuration, the user should be able to perform the following tasks on the workstation:

- 1 View recorded events and receive new events in real-time
- 2 Open the nodes in the Device Setup Tree and perform an action on a device
- 3 View and update a Cardholder record, including the image
- 4 Run a Cardholder Summary report

Firewall Program Exception List (Pinnacle default installation)

The following program exceptions are added to the firewall during Pinnacle's installation:

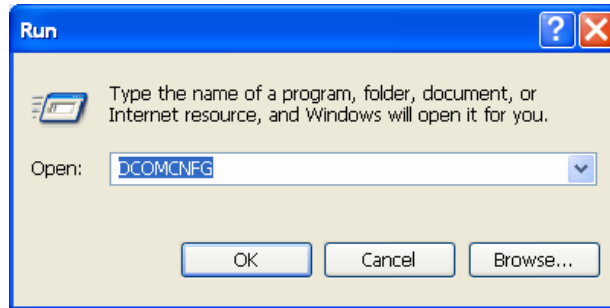
1. **AMTLicenseMgr**
2. **AMTNetworkComm**
3. **CKPScheduler**
4. **DCS**
5. **Pinnacle**

The purpose of these exceptions is to allow unrestricted access to all ports used by these programs. If program exceptions are not permitted by the end-user or IT department, see the following sessions to specify the range of ports to be used and open those ports in the firewall.

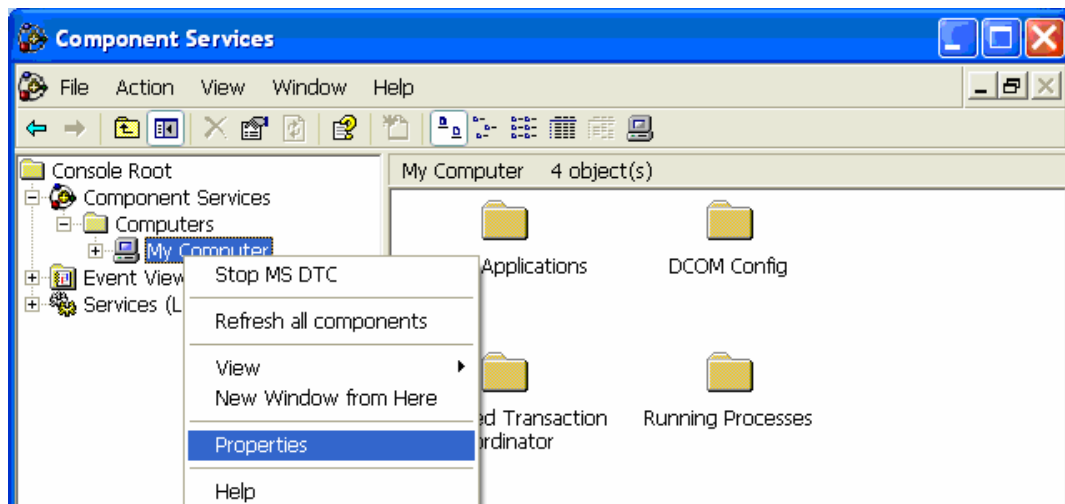
1. Specifying a range of ports for DCOM (Windows Server 2000/2003 or Windows XP) Firewall Settings for Pinnacle

1.1 Run DCOMCNFG

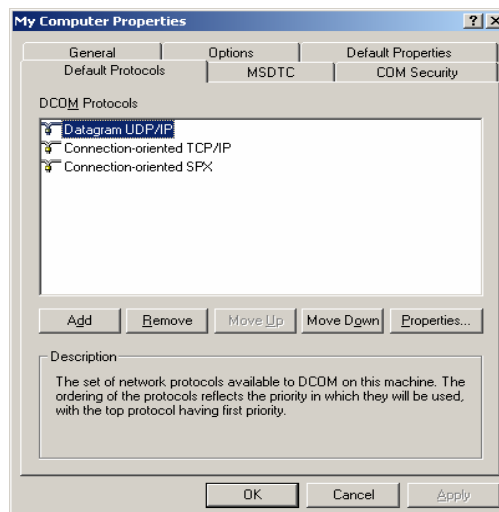
Click Start ->Run and type DCOMCNFG. Click OK.



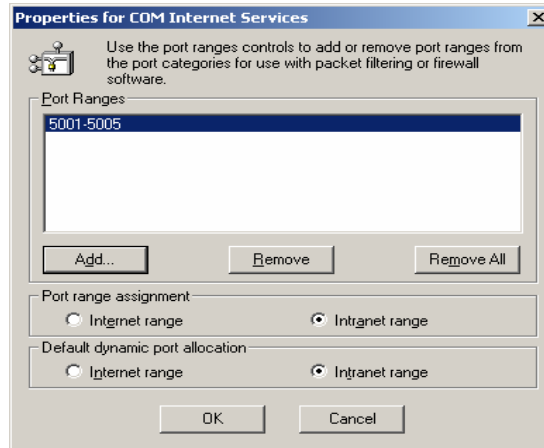
1.2 On the "Component Services" window expand the "Component Services" and "Computer" tree nodes. Right click on "My Computer" and select "Properties".



1.3 On the 'Default Protocols' tab, click 'Datagram UDP/IP' and click 'Properties'.

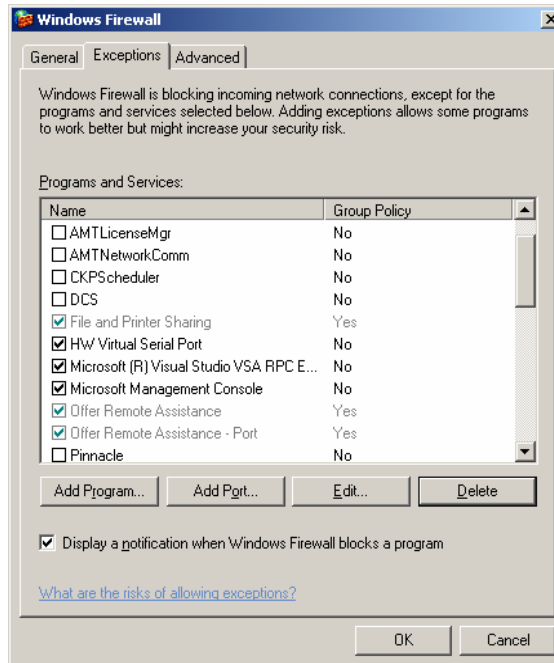


1.4 Click 'Add' and specify the desired port range (5001-5005 is used in this example).

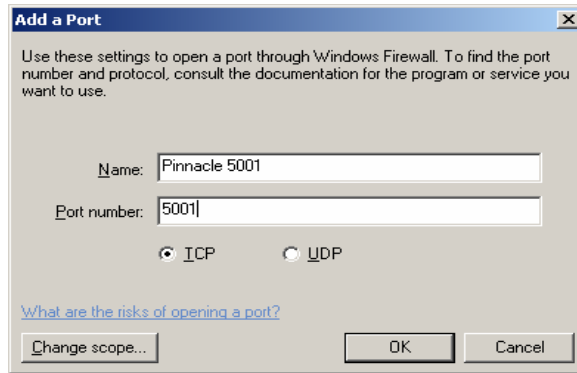


2. Opening ports on the Firewall

2.1 Open 'Windows Firewall' from within the Control Panel



2.2 Click 'Add Port' and add each of the ports specified on the table below, including its corresponding type (TCP or UDP)





Ports used by Pinnacle System

Port Range	Protocol	Description
135	TCP	RPC port negotiation for DCOM
1433-1434	TCP	MS SQL Server
5001-5005	UDP	Used by DCOM (Configurable)
4554	UDP	Pinnacle Multicast
4555	UDP	Pinnacle Heartbeat
9988	TCP	Pinnacle IP Tunneling, as configured (if used)

3. Uncheck the programs added to the Windows Firewall by Pinnacle's installation program

- 1 **AMTLicenseMgr**
- 2 **AMTNetworkComm**
- 3 **CKPScheduler**
- 4 **DCS**
- 5 **Pinnacle**

Repeat procedures above (Session 1 and 2) on all Servers and Workstations running Pinnacle with enabled firewall.

Pinnacle services must be restarted so that firewall changes can take effect. Run Pinnacle Manager and click Stop  "All Enable Services and Applications" after they stop click  Start to run "All Enabled Services".

