Gallagher Security
Confidential Technical Document

Gallagher Command Centre - TCP/IP Port Assignments

Document Number: **10939**
Published: **16 January 2003**
Last Modified: **21 November 2011**

The information in this article applies to: **All Versions**

Gallagher Products: **Cardax FT Systems : Command Centre Series**

Third Party Products: **Network & Network Cards, Windows O/S**

View this article online at http://support.cardax.com/secure/techdocs.aspx?id=10939

Port assignments as currently used by Gallagher Command Centre software processes.

The following information is to assist IT professionals when configuring Gallagher Command Centre to connect through routers and firewalls.

Gallagher Controller to Gallagher Command Centre Server PC (ALL Versions):

```
Keyword Decimal Description Reference
------- ------- ----------- ---------
ftp 21/tcp File Transfer [Control] Software download to FTController(vEL5.21 or
lower)
bootps 67/udp Bootstrap Protocol Server BootP
bootpc 68/udp Bootstrap Protocol Client BootP
www 80/tcp World Wide Web HTTP Internet Explorer to FTController Connection
cardax 1072/tcp CARDAX FTController Connection (enable both ways)
```

Notes:

1. CARDAX port 1072 is required for Gallagher Controller to Server communications
2. FTP port 21 is only required for updating FTController software via CCFT Server
3. BootP ports 67/68 are only required if BootP/BootStrap Protocol required for assigning FTController IP addresses
4. WWW port 80 is only required if web browsing to FTController required
5. If a gateway is defined for the Controller, ICMP must be enabled between the FTController and its gateway as the FTController will first ping the gateway if it needs to send a message to an address outside of its subnet.

Gallagher Command Centre Client PC to Gallagher Command Centre Server PC (ALL Versions):

```
Keyword      Decimal    Description              Reference
-------      -------    -----------              ---------
epmap         135/tcp   DCE endpoint resolution  Client Connection
```

```
(various)   ????/tcp   DCOM (5 x dynamic ports)   Licence Verification, Alarms and
Events, CCNTSAD
cardax      1072/udp   CARDAX                     Intercom
(various)   ????/udp   ????                       Camera
```

Multi-Server (vEL6.00 or later):

```
Keyword         Decimal    Description                Reference
-------         -------    -----------                ---------
configurable    4840/tcp   GALLAGHER                  Multi-Server OPCUA connection
```

Visitor Management Client (vEL5.21 or later):

```
Keyword         Decimal    Description                Reference
-------         -------    -----------                ---------
microsoft-ds    445/tcp    Microsoft-DS Service       ClickOnce
configurable    4243/tcp   GALLAGHER                  Visitor Mangement Client
```

Premier Client (vEL7.00 or later):

```
Keyword         Decimal    Description                Reference
-------         -------    -----------                ---------
microsoft-ds    445/tcp    Microsoft-DS Service       ClickOnce
configurable    4840/tcp   GALLAGHER                  Premier Client
```

Sagem Biometric Reader (vEL5.10 or later):

```
Keyword         Decimal    Description                Reference
-------         -------    -----------                ---------
Sagem           11010/tcp  SAGEM                      Command Centre to Reader
communications
```

Notes:

1. Port 135 is required for initiating Client/Server connection
2. Port 1072 is only required for the Gallagher Command Centre Client connection if intercom functionality is required.
3. Restricting DCOM dynamic port assignment is discussed below. See also Testing DCOM below.
4. Command Centre Camera live viewing - currently the camera to client UDP port is dynamically assigned and there is no mechanism for restricting it.
5. In a WAN environment, DNS (or at least HOSTS file) may need to be enabled/configured
6. For Premier Client, TCP port 445 is only required if using ClickOnce. If client files are copied it is not required.

Testing port 1072 using Telnet

In a situation when ports are restricted on the network, you can ping the Gallagher Controller but it won't come on-line, you can use telnet to test if port 1072 has been opened.

The following 2 examples show a failed and OK telnet connection to a Gallagher Controller from the Gallagher Command Centre Server PC.

Note: this must work both ways - from the Server to Gallagher Controller and Gallagher Controller to Server.

1. Failed Connection:

   ```
   C:\TELNET <FTC IPAddress> 1072
   Connecting To <FTC IP Address>... Could not open a connection to host on port
   ```

```
1072: Connection failed
```
2. OK Connection:

```
C:\TELNET <FTC IPAddress> 1072
(screen blanks, cursor top left for 25 seconds)
Connection to host lost.
```

Testing DCOM
The following may be used for troubleshooting a client PC failing to connect to the Gallagher Command Centre server. This may be either unable to logon or partial performance of the client e.g. no events or alarms, MLWs not updating (Hardware window blank or not updating), Find tool not finding items, etc.

1. For a network where the TCP/UDP ports have been restricted ensure you have allocated a DCOM range for use of the client PC(s) as per "Restricting DCOM port assignments" below, you will require 5 ports reserved for each concurrent client connection that is required.
2. If the site has a DNS sever, ensure that its IPAddress is configured in "Network and Dial-up Connections\Local Area Connection - Properties\Internet Protocol (TCP/IP) - Properties\".
3. If there is no DNS server available then add an entry in the HOSTS file of each PC in the following format:
   ```
   <IPADDRESS>    <HOSTNAME>
   ```
   e.g. If the Server was called FTSERVER and its IPAddress was 192.168.1.1 then the entry in the Client PC's HOSTS file would be:

   ```
   192.168.1.1 FTSERVER
   ```

   The HOSTS file is located in the <SYSTEM>\SYSTEM32\DRIVERS\ETC directory where <SYSTEM> is normally C:\WINNT or C:\WINDOWS
4. Reboot the PC to ensure all changes take effect
5. Ensure that you can ping the PC host names (client to server and server to client).
6. Test the DCOM connection. This can be by either starting the Gallagher Command Centre Client and ensuring events/alarms/items are displayed or there is a Microsoft utility available for testing DCOM between 2 pc's. It can be downloaded from the Microsoft Web site by searching for the Microsoft Knowledge Base Article: 259011 - SAMPLE: A Simple DCOM Client Server Test Application.

Note: DCOM will not work thru a firewall where NAT is used. See Microsoft Knowledge Base article 154596
The client must be able to reach the server by its actual IP address.

You cannot use DCOM through firewalls that do address translation (i.e. where a client connects to virtual address 198.252.145.1 which the firewall maps transparently to the server's actual address of, say, 192.100.81.101). This is because DCOM stores raw IP addresses in the interface marshaling packets and if the client cannot connect to the address specified in the packet, it won't work.

Testing network connectivity using PING
If you are using PING to test the connectivity of a network using routers/firewalls, ensure that these connectivity devices will pass ICMP packets.

Restricting DCOM port assignments:
The dynamic ports are required for DCOM (negotiated by Microsoft DCE RPC end-point mapper for its DCOM services). Up to 5 DCOM ports may be required per concurrent client connection. The Client/Server establishes a connection initially using TCP port 135 which then negotiates DCOM port

GALLAGHER

assignments for further communications. The architecture of DCOM allows it to use dynamic port assignment for communication, however it is possible to restrict the range that it will use for particular cases e.g. firewalls/routers.

The method for restricting the dcom port range is as follows:

1. Select Start\Run and enter "dcomcnfg"
2. Windows XP only
   - Expand "Component Services"
   - Expand "Computers"
   - Right-Click on "My Computer" and select "Properties"
3. Select "Default Protocols" tab
4. Select "Connection-Oriented TCP/IP" and click on "Properties"
5. Select "Add Port Range" and add a range of port numbers to use e.g. 5001-5005 (ensure any other applications running on the PC are not using these ports and allow at least 5 ports per each client that will be required to connect to the server at any one time (concurrent connections)). For example if the site had 4 workstations 20 ports would be required, in this case these 20 ports would need to be added. e.g. 5000-5020.
6. Select OK and OK.
7. This is required on the Server PC and may be required on the Client PC's (as the Client can initiate callbacks), where this is the case the same port range should be added to the Workstations as the server, e.g. 5000-5020.
   More information is available from the Microsoft web site by searching for the Knowledge Base Article: 154596 - HOWTO: Configure RPC Dynamic Port Allocation to Work with Firewalls.

Additional Information:
The following applications and utilities may also assist with the configuration, networking or use of Gallagher Command Centre.

1. DNS (or HOSTS file if DNS unavailable)
2. Time Synchronisation - Intercom (Client PC must be within 30 seconds of Server for Intercom to work at Client PC e.g. NET TIME command (port 445?))
3. DHCP (If broadcast is disabled but directed broadcasts are allowed - BootP for FT Controllers (v2.xx Command Centre and above))
4. Terminal Services (thin client method for connecting to Command Centre)
5. VPN (secure method for connecting to Command Centre via a public network)
6. DCOMCNFG (Restricting DCOM port assignments)
7. IPCONFIG (networking)
8. PING (networking)
9. NBTSTAT (networking)
10. ARP (networking)
11. RDP5.1 (required if sound redirection is required to terminal services client - currently only supported on Windows XP)

be liable on any ground whatsoever to any party in respect of decisions or actions they may make as a result of using this information.

In accordance with the Gallagher policy of continuing development, design and specifications are subject to change without notice.

Developed and manufactured by Gallagher Group Ltd, an ISO 9001 Certified Supplier.
Cardax is a registered trademark of Gallagher Group Ltd.
Gallagher Security is a division of Gallagher Group Ltd.