

**Opticom™ Central
Management Software**

**Installation, Set-up, Maintenance &
Troubleshooting Manual**

1	DESCRIPTION AND REQUIREMENTS.....	5
1.1	Document purpose	5
1.2	Supported Opticom devices.....	5
1.3	Central Management Software Description	5
1.4	Server Machine Description and Requirements.....	6
1.5	Client Machine Description and Requirements	8
1.6	Communication Hardware Requirements	8
2	INSTALLATION PREPARATIONS	9
2.1	Needed information and materials.....	9
2.2	Set Managed Switches	9
2.3	Server Machine.....	9
2.4	SQL Database	9
2.5	Preparing the Intersection Equipment.....	9
2.5.1	Configuring the Phase Selectors.....	10
2.5.2	Connect Phase Selectors and COM devices to the network	11
	Table 2-1	11
2.5.3	Ping each Phase Selector	11
3	INSTALLING & CONFIGURING THE SOFTWARE ON THE SERVER.....	12
3.1	Install SQL Server.....	12
3.2	Install CMS on the server	12
3.2.1	.NET Framework.....	14
3.2.1.1	.NET Framework on Windows Server 2008.....	14
3.3	Verify the installation	16
3.3.1	Scheduling and Communication Services.....	16
3.4	Open Firewall.....	17
3.4.1	Port 8081	18
3.4.2	The Central Management Software	18
3.4.3	SQL	18
3.5	Open SQL for remote Access.....	18
3.5.1	Open remote access on SQL Server 2005.....	18
3.5.2	Open remote access SQL Server 2008.....	20
3.6	Add Users to the OpticomUsers Windows group.....	22
3.6.1	Add Additional System Users.....	22
3.7	Install firmware package	25
3.8	Install GIS Map database.....	25
4	CLIENT WORKSTATION	26
4.1	Install CMS on the Client machine.....	26
4.2	Install firmware package	28
4.3	Install GIS Map database.....	28
5	ADDITIONAL SETUP	29
5.1	Enter the product key	29
5.2	Set view options.....	29
5.3	Enter mail server info	29
5.4	Enter Region Name	30
5.5	Add users	30
5.5.1	Opticom Central Management Software Roles.....	31
5.5.2	Add Users.....	31
6	CONFIGURING THE OPTICOM CENTRAL MANAGEMENT SOFTWARE SYSTEM. 32	
6.1	Key Concepts.....	32
7	ADDING VEHICLES AND CONFIGURING SYSTEM SECURITY/CODES.....	34
7.1	Jurisdiction Security Level	35
7.2	Agency and Code Allocation	35
7.3	Allocate Opticom IR Agency Code Ranges	35
7.4	Configure GPS vehicle classes	36
7.5	Add Vehicles	37
7.5.1	Adding Vehicles Manually.....	37

7.5.2	Importing Vehicles.....	38
7.6	Mutual Aid.....	40
7.6.1	Configure Mutual Aid	40
7.7	Explicitly Blocked Vehicles.....	41
7.8	Adding vehicles that will be connected to CMS.....	41
7.8.1	Adding Vehicle Modules Manually.....	42
7.8.2	Adding Vehicle Modules through Active Monitoring	42
7.8.3	Updating Vehicle Module Firmware.....	42
8	ADDING INTERSECTIONS AND PHASE SELECTORS.....	43
8.1	Adding Intersections Manually.....	43
8.2	Importing Intersections.....	43
8.3	Adding Phase Selectors	44
8.3.1	Discovering Phase Selectors Manually.....	45
8.3.2	Adding Phase Selectors through a Job	45
8.3.3	Additional Phase selector setup	46
8.3.4	Updating Phase Selector Firmware	48
8.3.5	Updating Phase Selector Code Maps	48
8.3.6	Phase Selector Communication Job	49
9	ACTIVE MONITORING.....	50
9.1	Configure Active Monitoring.....	50
9.2	Start Active Monitoring	51
9.2.1	Stop Active Monitoring	52
9.2.2	Fine Tuning Polling Rate.....	52
9.2.3	Network Traffic.....	53
9.3	Alerts	53
9.3.1	Configuring Alerts	54
10	PROVISIONING, DECOMMISSIONING, REPLACING & DELETING A DEVICE .55	55
10.1	Provisioning a Replacement Device.....	55
10.2	Decommissioning a Device	55
10.3	Deleting a device.....	55
11	CENTRAL MANAGEMENT SOFTWARE ACCESS CONTROL	56
11.1	Service Accounts	56
11.1.1	Configure the Scheduling Service to use an alternative account	56
12	MAINTAINING THE CMS DATABASE	58
12.1	Pruning the Database.....	58
12.1.1	Creating a Database Archiving and Pruning Job	58
12.2	Backup database.....	59
13	TECHNICAL SUPPORT	60
13.1	Installation log	60
13.2	Code Site Logs	60
13.3	Setting Code Site Verbosity Level	61
14	OVERVIEW OF COMMUNICATIONS INFRASTRUCTURE	63
14.1	TCP/IP.....	63
14.2	Redirected Serial.....	63
15	TROUBLESHOOTING AND ERRORS MESSAGES	65
15.1	Error Screens.....	65
15.2	Errors and Warnings.....	70
15.3	Summary of Communication Flow	73
15.4	Communication Troubleshooting.....	74
15.4.1	General Guidelines in Diagnosing Communication Issues	74
15.4.2	Diagnosing TCP/IP Addressability Issues	74
15.4.3	Diagnosing the Model 750 series and Model 1000 at the Intersection.....	75
15.4.4	Diagnosing phase selector timeout issues.....	77
15.4.5	Diagnosing the Model 760 series at the Intersection.....	78
15.4.6	Diagnosing Redirected Serial Issues.....	79

15.5	Data Consistency Check	80
16	QUICK GUIDES.....	81
16.1	Pre-Installation.....	81
17	OPTICOM FIRMWARE PACKAGE.....	84
17.1	Firmware Package Installer	84
17.2	Determining the versions available on your machine	84
17.3	Download the latest version.....	84
17.4	Installing the Firmware Package.....	85
18	GIS MAPS	86
18.1	Delete old map data	86
18.2	Download Map Data (US):.....	86
18.3	Download map data (Canadian users):	87
18.4	Import Map Data into CMS:	87
19	MOVING AN EXISTING CMS DATABASE TO ANOTHER MACHINE	89
19.1	Steps to perform on the existing Server Machine.....	89
19.2	Steps to perform on the new Server Machine (Full SQL)	89
19.3	Steps to perform on the new Server Machine (SQL Express).....	90
19.4	Steps to perform on the existing Client Machine/s.....	91
20	CREATE EXCEPTIONS IN WINDOWS FIREWALL	94
20.1	Create an exception for SQL Server 2005 in Windows Firewall	94
20.2	Create an exception SQL Server Browser service in Windows Firewall.....	95
21	ADDITIONAL STEPS TO OPEN SQL FOR REMOTE ACCESS	95
21.1	SQL 2005.....	95
21.2	SQL 2008.....	97
22	UPGRADING TO A NEW VERSION	99

1 Description and Requirements

1.1 Document purpose

This document provides information on the following details of the Opticom Central Management Software (CMS).

- Hardware requirements
- Software requirements
- Software installation and configuration
- Initial system configuration and setup
- Adding Vehicles to the database
- Adding Intersections to the database
- Activating and configuring Monitoring
- Creating Alerts
- Troubleshooting
- Moving or upgrading the database

Please see the help file included with the software for details on the use and operation.

1.2 Supported Opticom devices

The CMS works with intersections and vehicles equipped with Opticom devices. The following Opticom models are supported:

- Model 752 Series Phase Selector
- Model 754 Series Phase Selector
- Model 1000 Phase Selector
- Model 762 Phase Selector
- Model 764 Phase Selector
- Model 2100 Radio/GPS Control Unit
- Model 2101 Radio/GPS Control Unit

1.3 Central Management Software Description

CMS helps the traffic engineer implement, manage, and maintain the Opticom priority control system.

- Manage your inventory of intersection and vehicle equipment.
- Manage Opticom system security.
- Actively monitor phase selector status and priority call activity.
- Generate alerts upon occurrence of user-selected system events and priority calls.
- Monitor system usage through preconfigured reports and real-time intersection and vehicle module views.
- Maintain your Opticom system using preconfigured reports, ad-hoc call history analysis, and real-time intersection and vehicle module views.
- Remotely provision replacement Opticom phase selector cards at the intersection.
- Remotely update firmware in Opticom devices.
- Schedule automatic generation and e-mail delivery of reports.

- Allow user access to the central management software according to users' role and responsibilities:
- Create and deploy evacuation plans, allowing transit vehicles to gain preemption (rather than transit signal priority) to efficiently vacate an area for an emergency or following a civic event. Evacuation Plans is a separately licensed module; contact your GTT representative for more information.

1.4 Server Machine Description and Requirements

The server machine hosts the database, services, and user interface.

Notes:

- **Opticom central management software should be deployed on a dedicated server, running no other substantial workload.**
- **The server machine is intended to be left running at all times.**
 - Necessary for background services to operate.
- **The specifications listed below, provide a scale for the components needed, comparable components may be used.**
- **Use of a SQL Server instance remote from the server is not supported.**
- **Server machines that do not meet the recommended requirements may perform unsatisfactorily if the CMS monitoring option is in use.**
- **It is recommended but not required that the server machine have internet access.**
- **It is recommended that an external time source be used to keep the server clock accurate.**
 - **The server clock is used as a reference to reset phase selectors clocks each night.**
 - **Not necessary in Opticom GPS operation since GPS time is used on the phase selector.**

Preferred Operating Systems:

- Windows® Server 2003 SP3
- Windows® Server 2008 R2

Optional Operating Systems

- Windows® XP Professional SP3 (no home editions)
- Windows® 7 SP1 Professional (no home editions)

Supported locales:

- English (United States)
- English (Canada)

Hardware requirements:

- Hardware requirements will vary depending on the number of configured phase selectors, priority call activity, desired active monitoring poll rate, and reporting requirements.

Up to 150 Intersections:

- Intel® Xeon® W3565 2.13 8MB/1066 QC CPU (HIGHPOWER)
- 8 GB DDR3-1333
- 1 TB SATA 7200
- High speed Ethernet connection
- Data backup methodology in place
- DVD Drive

Up to 500 Intersections:

- 2X AMD Opteron 6134 2.3GHz, 8C, 4M L2/12M L3, 1333Mhz
- 32 GB 1333 LV RDIMMs for 2 processors
- 2 TB (RAID 5 or other)
- 1GB Ethernet connection
- Data backup methodology in place
- DVD Drive

Contact GTT Technical Support for installations over 500 intersections.

Database requirements:

- SQL Server 2008 R2, Service Pack 2.
 - Standard or Express
- SQL Server 2005, Service Pack 4.
 - Standard or Express
- SQL Server 2005 Express is on the CMS installation CD.
 - SQL Server 2005 Express is limited to 4GB database size.
 - The database may be upgraded to full SQL Server edition
- Consult your SQL license for how many connections are allowed.

1.5 Client Machine Description and Requirements

The client workstation hosts the CMS user interface and allows you to access the CMS database and CMS services from a remote location. There is no limit on how many machines may run the client user interface.

Notes:

- **The client must be connected to the same network as the server and database.**
- **Port 8081 must be opened on the client machine.**
- **The client machine may be shutdown regularly.**

Supported Operating Systems:

- Windows® XP Professional, SP 3
- Windows® 7, SP 1
- Windows® Server 2003, SP 2
- Windows® Server 2008 R2, SP 1

Supported locales:

- English (United States)
- English (Canada)

Hardware requirements:

- 2 GHz or greater
- 2 GB memory
- 20 GB storage

1.6 Communication Hardware Requirements

Opticom Model 762/764 Phase Selectors include an integrated Ethernet port and can communicate with CMS directly using TCP/IP.

Opticom Model 1000 phase selectors and Model 752/754 phase selectors support only serial connectivity, which typically requires that a serial device server be installed in the traffic cabinet to bridge from Ethernet to serial. Alternatively, you might use a communications device that has built-in serial ports. Contact your GTT representative if you need more information on compatible communications devices or cabling.

Most serial device servers can be configured to optimize the transfer of information from the phase selector to the server. This can significantly reduce the processing overhead on the server, resulting in improved scalability when monitoring phase selector activity. Contact GTT technical support for assistance in this area.

If you have intersections with more than one phase selector, e.g., two 2-channel cards, it's best to use a separate port for each phase selector. You can also connect both cards to the same port and distinguish the cards by "device addresses", but using separate ports is easier to configure and allows you to use an automated phase selector discovery job, rather than configuring each phase selector manually.

2 Installation Preparations

This section describes all of the preparations and information needed to insure a smooth installation. It is recommended that the following items be available and configured prior to beginning your CMS installation.

2.1 Needed information and materials

- List of vehicles, IDs, code ranges, agencies and agency IDs, jurisdictions and IP addresses (See section 7)
- List of intersections, jurisdictions and IP addresses (See section 8)
- License key (on the CD jewel case)
- Mail server information (See section 5.3)
- User names (See section 5.5)
- Opticom Firmware package (See section 17)
- GIS map data (See section 18)

2.2 Set Managed Switches

On networks with high traffic such as networks with video, GTT recommends that managed switches be used. GTT recommends that the managed switches be set to allow only the bandwidth required for what each device needs. This is recommended for all devices on the network. You may experience intermittent communications with your Opticom devices on high traffic networks without managed switches or if the switches are not configured to limit traffic.

2.3 Server Machine

The server machine should be installed and connected to the network. Verify that the server has sufficient disk space to allow the growth of the SQL database.

2.4 SQL Database

If a full version of SQL is to be used, it should be installed on the server machine. The CMS installation disk includes a copy of SQL Express 2005. If you intend to use the SQL Express 2005 it will be installed during the CMS installation. SQL Express 2005 is limited to 4 GB.

2.5 Preparing the Intersection Equipment

Prepare the phase selectors for use with CMS by installing and configuring them in the traffic cabinet. Connect the phase selectors to the communication network. If you are using Model 750 Series or Model 1000 phase selectors you will also need to configure and install the communications equipment.

2.5.1 Configuring the Phase Selectors

Install and fully configure the phase selectors in the traffic cabinet.

Determine the approach direction for each phase selector channel. It is recommended that this information be entered into the appropriate field in the phase selector while configuring the phase selector in the field. Phase selectors have the ability to be configured to indicate the name of each channel. This information will be configured in the CMS software and is used to provide meaningful approach names in the CMS logs and reports. Channels that are not in use should be recorded and or marked as “Not used”. That information will then be readily available and may then be easily included in the Central Management Software.

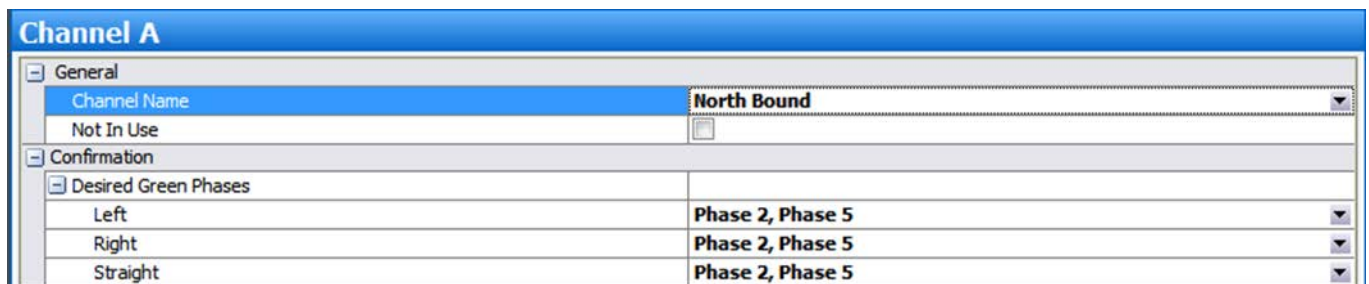
Opticom phase selectors have the ability to report “current greens” information when wired with an auxiliary harness or through the auxiliary interface panel. Contact your GTT representative for information on required equipment and wiring instructions.

When green sense is wired at the cabinet, central management software has these extra capabilities:

1. The software notes for each call whether the greens active at the end of the call match those configured for the approach. Consistent mismatch can indicate a wiring or configuration issue at the intersection.
2. The current activity screen displays active greens, whether preemption is currently active or not. It also monitors phase changes, so you can identify green extension / changes due to preemption or priority.

Record the phase assignments for each channel so this information can be configured in the software. Model 750 series and Model 760 series phase selectors have the ability to be configured to indicate which phases are associated with each channel. It is recommended that this information be included while configuring the phase selector in the field. That information will then be readily available and may then be easily included in the Central Management Software.

See Section 8.3.3 for more detail. See Figure 2-1.



The screenshot shows a configuration window titled "Channel A". It has two main sections: "General" and "Confirmation".

- General:**
 - Channel Name: North Bound
 - Not In Use:
- Confirmation:**
 - Desired Green Phases:
 - Left: Phase 2, Phase 5
 - Right: Phase 2, Phase 5
 - Straight: Phase 2, Phase 5

Figure 2-1

2.5.2 Connect Phase Selectors and COM devices to the network

Connect each phase selector to the appropriate network connection point in the traffic cabinet using the appropriate cable.

Record the Intersection name, IP address and port number for each phase selector.

If you are connecting Model 1000 or 750 series phase selectors, configure the serial device server's configuration as required by Opticom phase selectors:

	Model 750 Series Opticom infrared system phase selectors	Model 1000 Opticom GPS system phase selectors
Baud rate	9600	115,200
Parity	None	None
Data bits	8	8
Flow control	None	None

Table 2-1

2.5.3 Ping each Phase Selector

Once the phase selectors are connected to the network you will need to ping each one to verify connectivity. From the server machine launch a DOS/Command prompt and ping each device. See Figure 2-2.

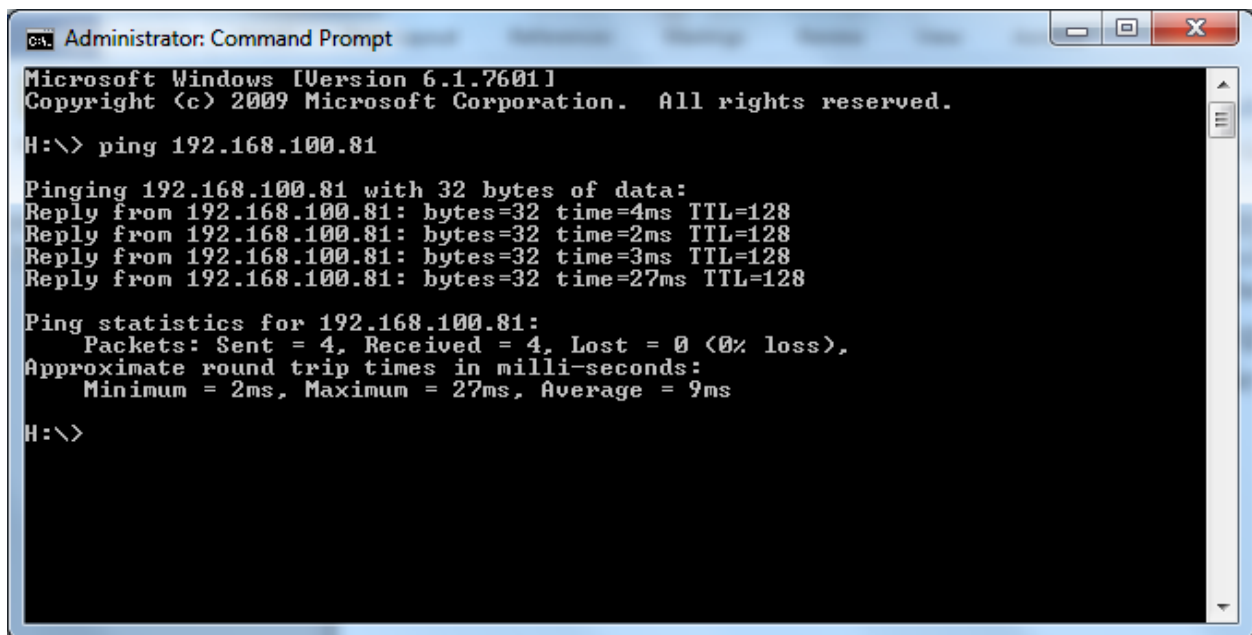


Figure 2-2

3 Installing & Configuring the Software on the Server

This section describes the steps to install and configure the CMS software on the server machine.

Notes:

- **Administrator privilege is required to install Opticom central management software on the server.**
- **The Windows® account used to install the server software is added to the Opticom central management software database as a user in an administrative role.**
- **Use of a SQL Server instance remote from the server is *not* supported.**
- **You can use the Opticom central management software client application on a remote workstation using either a Windows domain account or a mirrored local account (where the server and workstation have local accounts with the same name and password).**
- **Multiple copies of the central management software client application can be run concurrently on a single system. This allows you to run a “terminal services” environment where remote users access the application through individual remote desktop sessions to the server.**

3.1 Install SQL Server

The Central Management Software includes a copy of SQL Express 2005. SQL Express 2005 has a limit of 4 GB for the database. It is recommended that this version be used only in smaller installations. It is possible to start out with SQL Express and then migrate to a full version of SQL at a later date. The details of moving the database are included in Section 19.

If you will be using SQL Express 2005, skip this step of installing the full version of SQL.

If you will be using your own copy of SQL Server 2005 or 2008, install an instance on the server. You can use either the default, unnamed instance or a named instance. Refer to the documentation included with SQL for details.

Notes:

- **The SQL server instance must be on the same machine where the central management software will be installed.**
 - **Running the SQL instance and the Server software on different machines is not supported.**

3.2 Install CMS on the server

Install from the provided media and follow the directions on the installation wizard screens.

1. If you see a dialog box about .NET framework (Figure 3-4) see section 3.2.1 for details on how to proceed.
2. Select the Server installation option when prompted See Figure 3-1
3. When prompted, select the instance of SQL that you will use.
 - a. Figure 3-2 shows an example of using a user installed full version of SQL.
 - b. Figure 3-3 shows an example of using SQL Express 2005.
4. Press the Finish button when complete.

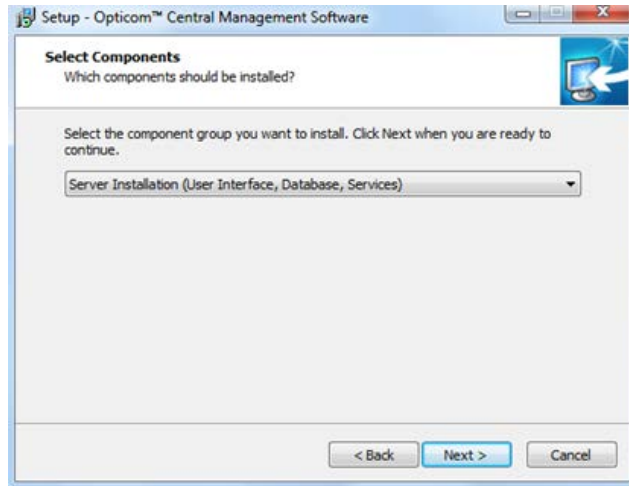


Figure 3-1

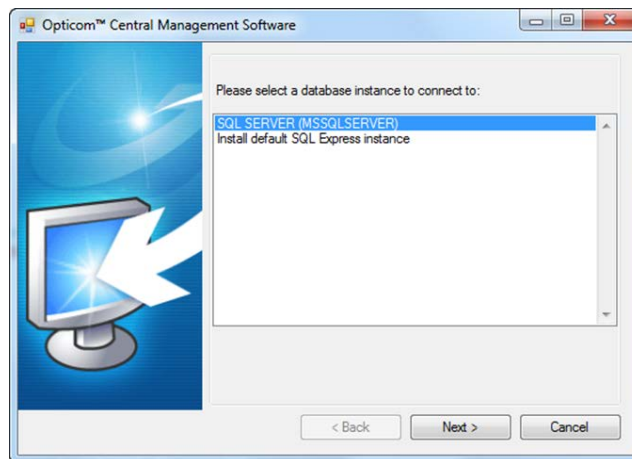


Figure 3-2

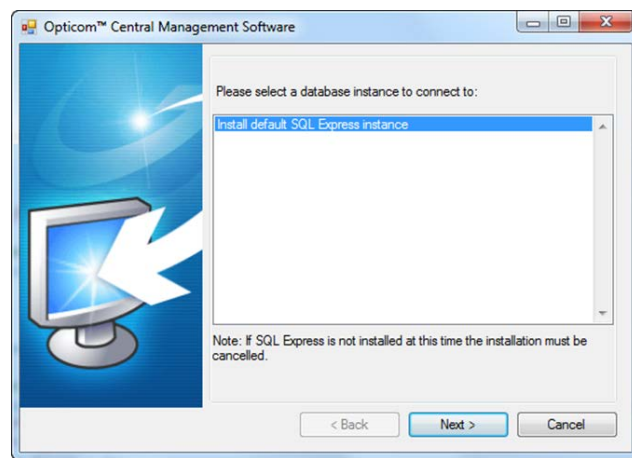


Figure 3-3

3.2.1 .NET Framework

The CMS software requires the Microsoft .NET framework software. Your machine may already have .NET framework installed. If your machine already has .NET framework the CMS installer will detect this and you may ignore this section.

If it is not already installed, CMS will prompt you that it is missing See Figure 3-4. A copy of .NET framework is included on the installation CD.

If prompted to install .NET framework press the Yes button. It may take some time before a dialog box appears saying that .NET framework is being installed. When complete go to step 2 in section 3.2.

If you are installing on Windows Server 2008 proceed to section 3.2.1.1.

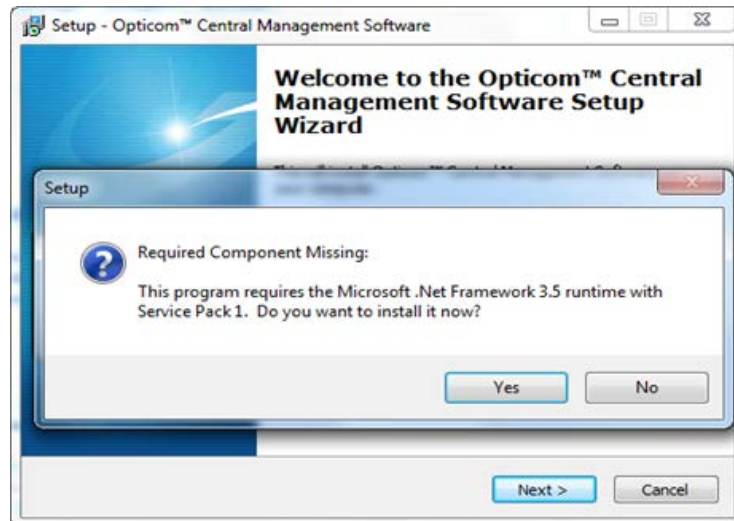


Figure 3-4

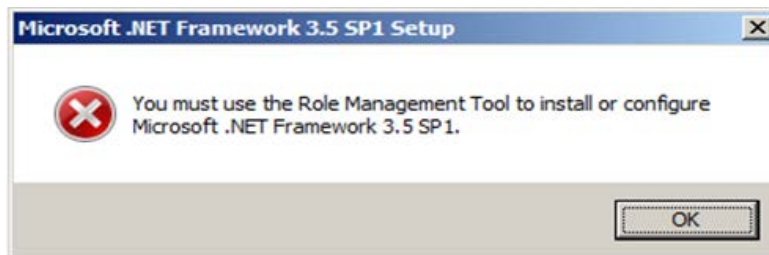


Figure 3-5

3.2.1.1 .NET Framework on Windows Server 2008

.NET framework will not automatically install on Windows Server 2008, it must be installed through the Role Management tool. See Figure 3-5.

1. Answer No to the “Do you want to install it?” message box and cancel the central management software installation.
2. On the desktop or in Windows Explorer, right-click My Computer and select Manage
3. Select the Features node, then Add Features.

4. In the Add Features Wizard, expand .NET Framework 3.5.1 Features, then check .NET Framework 3.5.1 (or the most current version)
5. Select Next, then Install.
6. Once the installation has completed, select Close.
7. Reboot the server if prompted
8. Restart the CMS installation then go to step 2 in section 3.2.

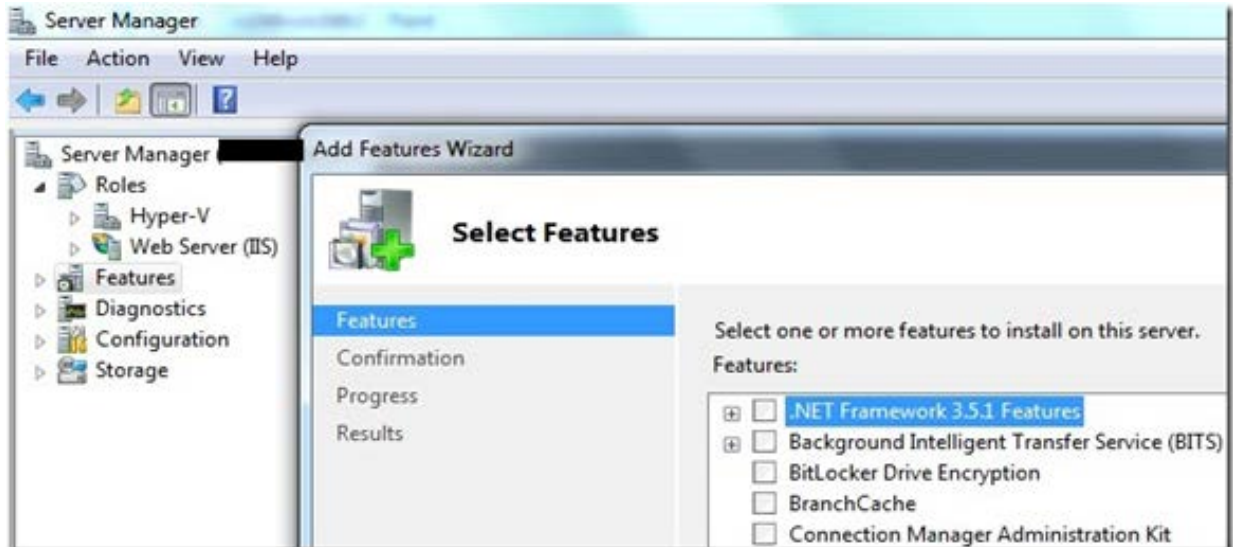


Figure 3-6

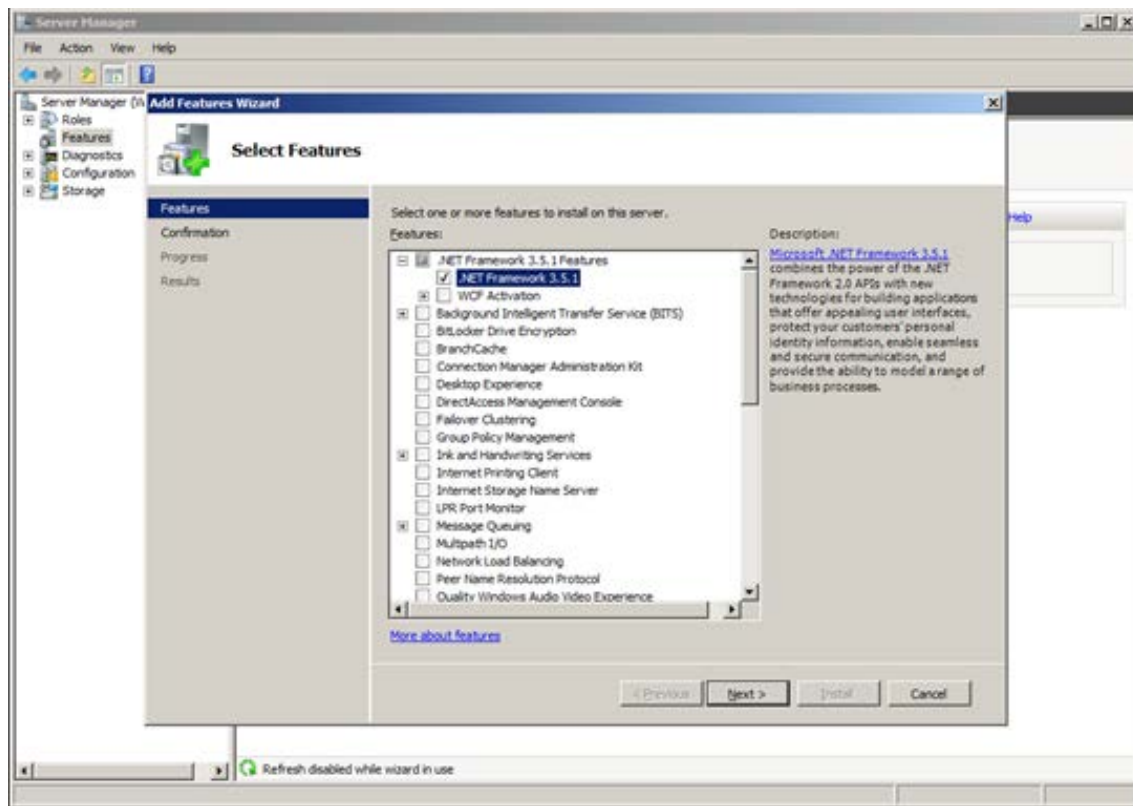


Figure 3-7

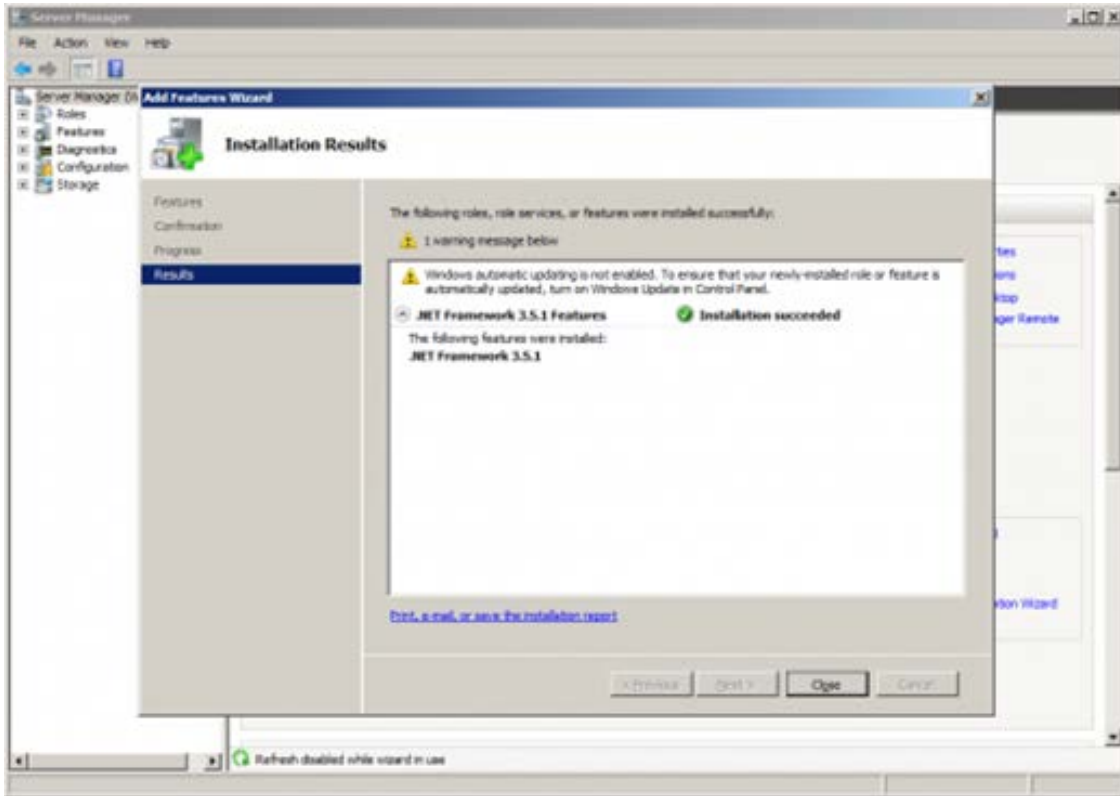


Figure 3-9

3.3 Verify the installation

Launch the application from Start / Programs / GTT / Opticom Central Management Software. Verify that the application starts up. You'll see the default Intersection Management screen. On the lower left, you'll see that you're signed into the application with your Windows account.

3.3.1 Scheduling and Communication Services

Verify that the GTT Communications and Scheduling Services are running. The CMS communications and scheduling services are installed on the server machine. The services are set to start and run automatically on startup of the server. If necessary these services may be manually started and stopped. These services can be accessed in the control panel's Administrative Tools section under the Services selection. The names of the services are "GTT Communications Service" and "GTT Scheduling Service". See Figure 3-10. See section 11- to run these services under a different account.

Notes:

- **Port 8081 on the firewall must be opened for the Communications Service to run.**
 - See the next section for details on opening Port 8081
- **These services must be running at all times on the server machine.**
- **If these services are not running CMS will not be able to communicate with the devices in the field nor will any scheduled jobs run.**

- If Port 8081 is not open, the Communications Services will not be able to start. (see section 3.4.1 and section 20 for more detail)
- Verify that the Startup Type is Automatic (Delayed Start) for the Communication Service.
- Verify that the Startup Type is Automatic for the Scheduling Service.
- Right click on the service and select Start to turn on the service.
- Right click on the service and select Stop to turn off the service.
- Right click and select Restart to reboot the service.
- The scheduling service is dependent on the communication service, which means the scheduling service will not run if the communications service is not running.
- The communications service is dependent on CodeSite Dispatcher.
- Scheduling service is also dependent on the specified SQL instance running.

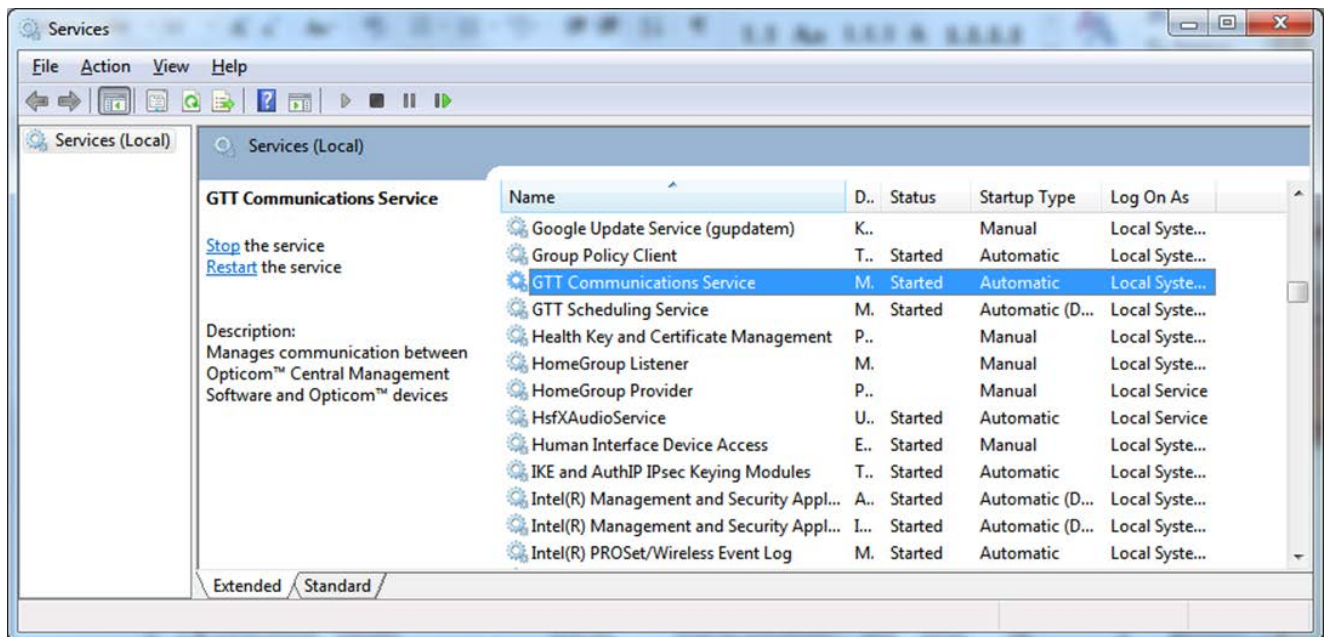


Figure 3-10

3.4 Open Firewall

Note:

- GTT recommends that any modifications to the firewall described in this section be performed only by your IT department.

If you are using a firewall on your network you will want to open the firewall for the following items:

- Port 8081
- The Central Management software
- SQL

3.4.1 Port 8081

In order for the communication service to connect to the phase selectors in the field it is necessary to open port 8081 on the server firewall and client firewall as well as any domain servers. If this port is not opened the communication service will not be able to start and CMS will not be able to communicate with the phase selectors in the field. Also since the scheduling service is dependent on the communication service it will not start if the communication service does not start. The firewall on any client machines must also have port 8081 opened. See section 20 for more details.

Contact GTT technical service if you wish to assign a different port for this access.

3.4.2 The Central Management Software

Add the Central management software to the list of allowed programs on the firewall on for the server and any client machines.

3.4.3 SQL

Add SQL to the list of allowed programs on the firewall for the server and any client machines. See section 20 for additional details.

3.5 Open SQL for remote Access

In order for the client machines to access the database it will be necessary to open SQL to allow remote access. By default SQL does not allow remote access/connections. The procedure to open SQL varies with the version of SQL that you are using. See the following sections for details on these procedures. This section contains the steps that will open SQL for remote access in most environments. In some environments, additional steps may be necessary. Those steps are in Section 21.

You may skip this section if you will not be installing CMS on any client machines.

3.5.1 Open remote access on SQL Server 2005

This section describes the steps for the SQL Express 2005 version included with the Central Management Software as well as the full version of SQL Server 2005.

The following is an excerpt from Microsoft Knowledge Base article 914277.

1. Under **Programs**, Open the **Microsoft SQL Server 2005** folder.
2. Open the **Configuration Tools** folder, and then click and open **SQL Server Surface Area Configuration**.
3. On the **SQL Server 2005 Surface Area Configuration** page, click **Surface Area Configuration for Services and Connections**. See Figure 3-11.
4. On the **Surface Area Configuration for Services and Connections** page, expand **Database Engine**. See Figure 3-12..
5. Click **Remote Connections**,
6. Select **Local and remote connections** and **Using both TCP/IP and named pipes**, then click **Apply**. See Figure 3-12.
7. Click **OK** when you receive the following message:

- Changes to Connection Settings will not take effect until you restart the Database Engine service.
8. On the **Surface Area Configuration for Services and Connections** page, expand **Database Engine**, click **Service**, click **Stop**, wait until the MSSQLSERVER service stops, and then click **Start** to restart the MSSQLSERVER service. See Figure 3-13.
 9. In most instances the preceding steps will have opened SQL to remote access. In some instances it may be necessary to perform the steps in section 21. If you receive errors when the client CMS is launched, refer to section 21.



Figure 3-11

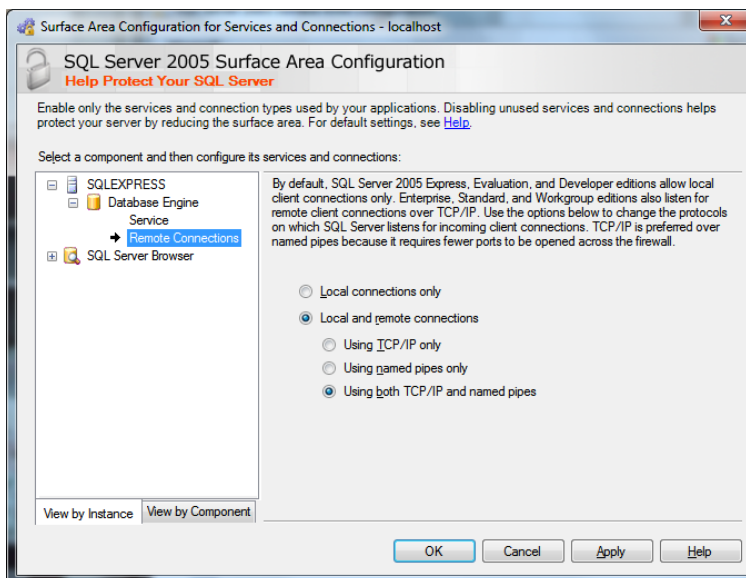


Figure 3-12

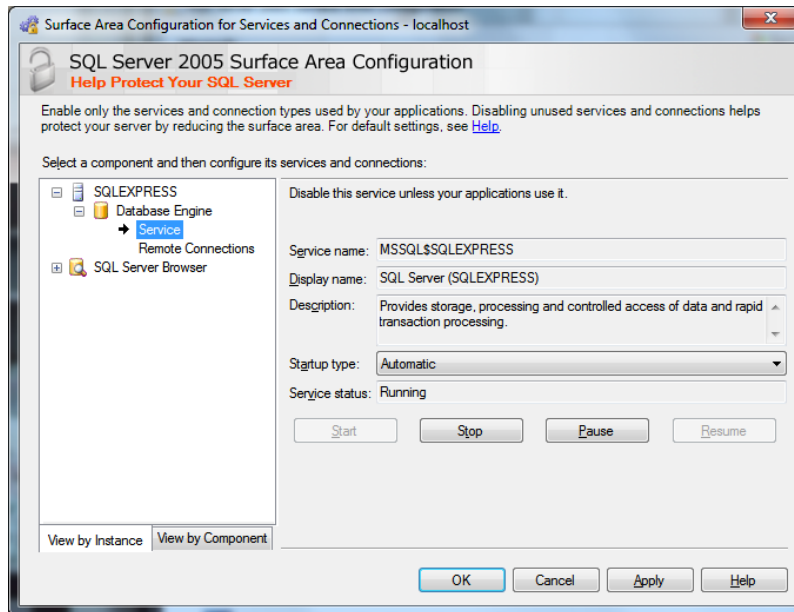


Figure 3-13

3.5.2 Open remote access SQL Server 2008

This section described the steps for the SQL Server 2008 and SQL Express 2008.

1. Under programs, open the **Microsoft SQL Server 2008(R2)** folder.
2. Open the **Configuration Tools** folder, and then click and open the program **SQL Server Configuration Manager**.
3. Open **SQL Server Network Configuration** and select **Protocols for MSSQLServer (Name may vary)**
4. Verify that **TCP/IP** and **Named Pipes** are enabled. See Figure 3-14.
 - a. Right click and enable them if not
5. Then select **SQL Server Services**.
6. Verify that **SQL Server Browser** is **running** and set to **Automatic** Start mode. See Figure 3-15.
 - a. If not select **SQL Server Browser**, right click and select **Properties**.
 - b. Click on the **Service** Tab and select **Automatic** as the start mode.
 - c. Click **Apply** and then close the screens.
 - d. Right click on **SQL Server Browser** and select **Start**.
7. Remote access should now be enabled.
8. In most instances the preceding steps will have opened SQL to remote access. In some instances it may be necessary to perform the steps in Section 21. If you receive errors when the client CMS is launched, refer to Section 21.

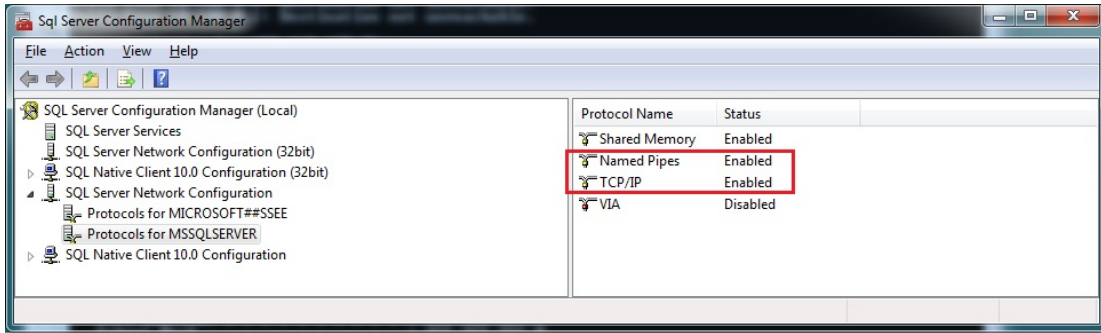


Figure 3-14

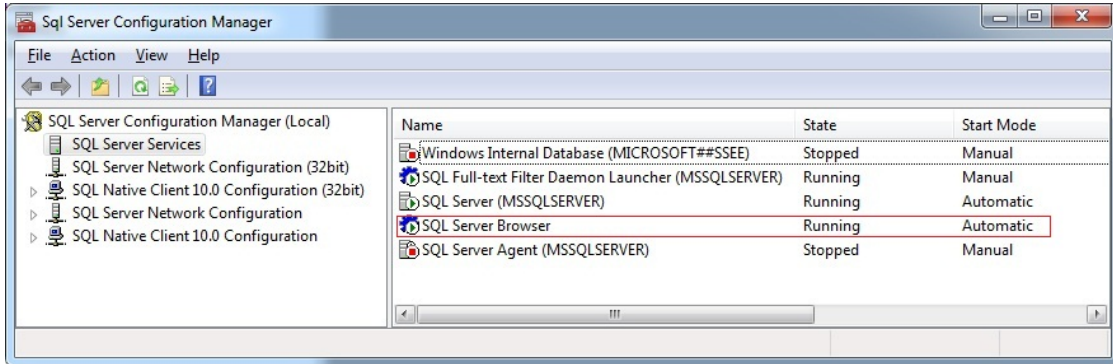


Figure 3-15

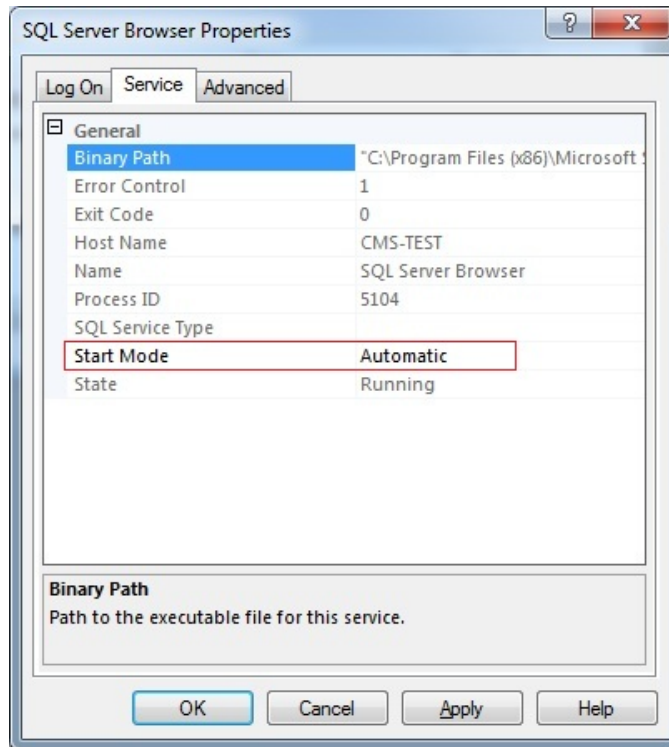


Figure 3-16

3.6 Add Users to the OpticomUsers Windows group

During CMS server installation, a user group is created called “OpticomUsers”. The person who was logged on when CMS was installed is automatically added to this group. This user is also added in the CMS users list in an administrator role. This user must be logged into CMS to add additional users.

Notes:

- **The OpticomUsers group is on the server machine only.**
- **All users of the CMS software will need to be added to this “OpticomUsers” group.**
- **You may add a domain user group containing many users to the “OpticomUsers” group rather than entering them individually.**
- **All users will also need to be added to the CMS software directly. See Section 5.5.**

3.6.1 Add Additional System Users

Access the OpticomUsers group properties screen on the server machine. This screen is accessed in different ways depending on the operating system you are using (Use the Windows Help if needed).

Typically it is under Control Panel\Administrative Tools\Computer Management\Local Users and Groups\Groups\OpticomUsers

1. Double click the **OpticomUsers** group. See Figure 3-17.
2. Press the **Add** button. See Figure 3-18.
3. Type the name of the user into the field provided.
 - 1) To make sure that the user selected has been entered correctly press the “Check Names” button.
 - 2) When adding members to the OpticomUsers group, the users names must be in the format that they use to log into your network.
 - 3) Domain\UserName or Domain\UserName@company.com (Where the domain and company information matches your specific information. See Figure 3-19.
4. Repeat to add additional users.

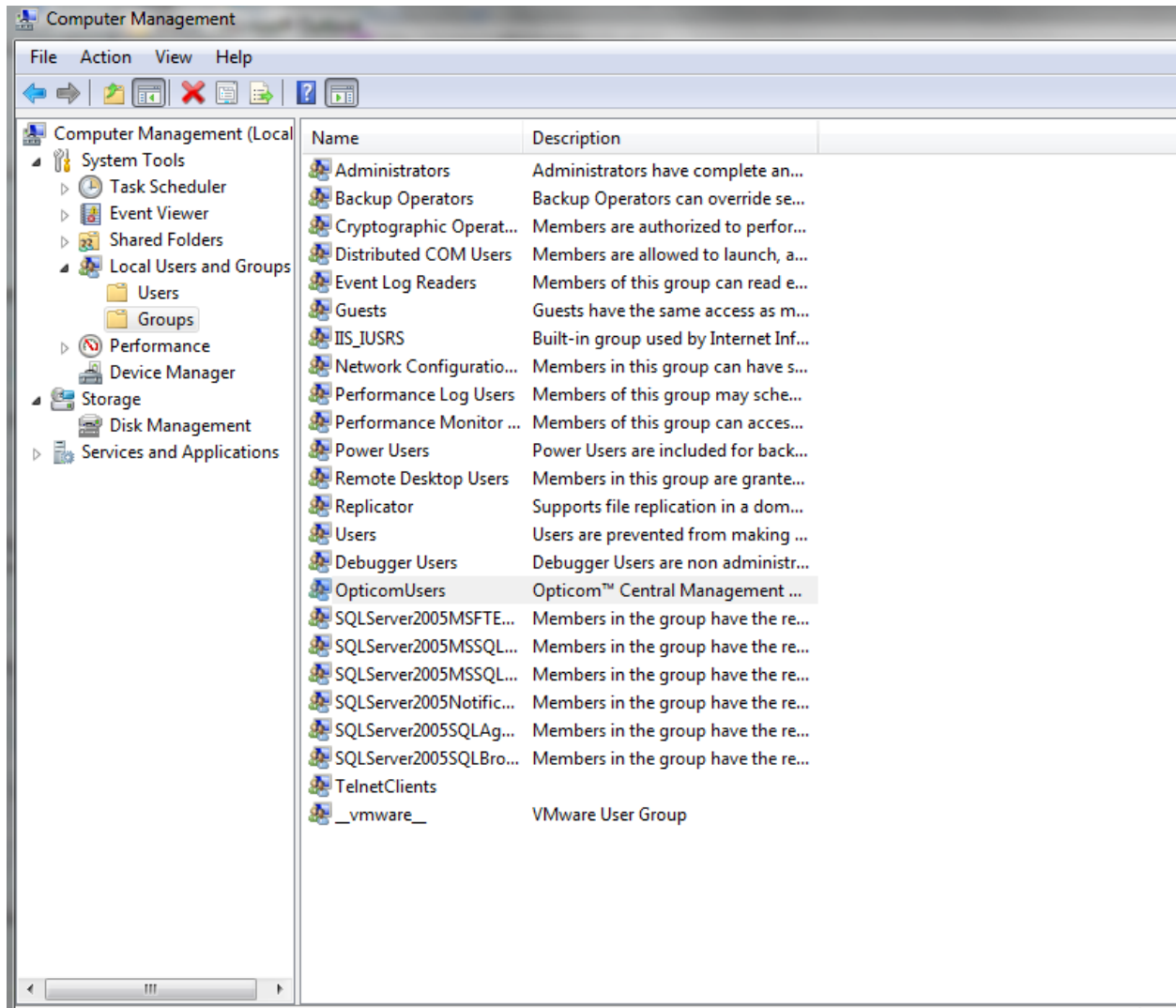


Figure 3-17

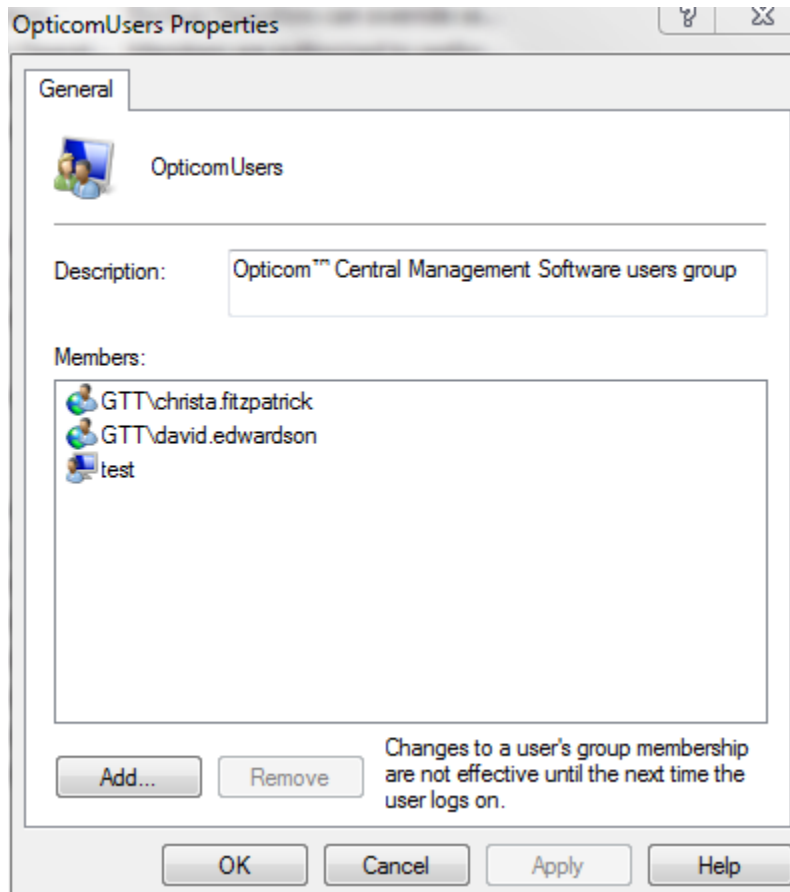


Figure 3-18

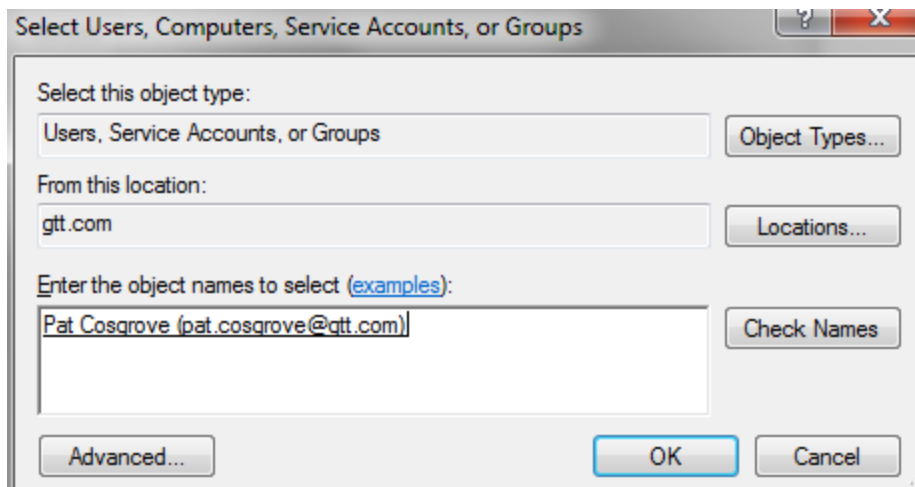


Figure 3-19

3.7 Install firmware package

If you are using M764, M762, or M1000 phase selectors and or Model 2100 or 2101 radio/GPS control units, install the Opticom Firmware Package on your server. See Section 17 for details.

3.8 Install GIS Map database

If you are using Opticom GPS, install the GIS map for your region on your server. Skip this section if your installation is Opticom Infrared only. See Section 18 for details.

4 Client Workstation

You may install the CMS software on as many client machines as you wish. Each of these machines will have the same user interface as the server machine. (The exception is some user levels will not have access to some of the function tabs). Each of the client machines will be configured to point to the SQL database on the server machine. You will need to install the firmware package and the GIS map database (if used) on each client machine.

4.1 Install CMS on the Client machine

1. Log on to the workstation as an administrator and as a user that has been added to the OpticomUsers Windows group and to CMS. See sections 3.6. and 5.5
2. Run the OpticomCentralManagementsetup.exe program.
3. When prompted on the Select Components screen, choose "Client Installation." See figure 4-1.

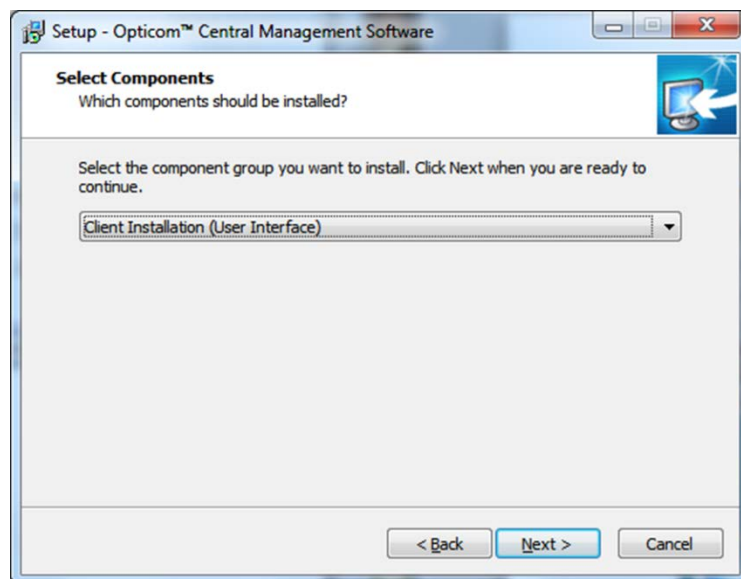


Figure 4-1

4. When prompted, type in the name of the SQL Server instance. See Figure 4-2.
 - a) The name and location of the SQL instance may be determined by looking along the bottom edge of the CMS user interface on the Server machine. See Figure 4-3.
 - b) **The SQL instance name is case sensitive; enter it exactly as it is displayed in CMS on the server machine.**

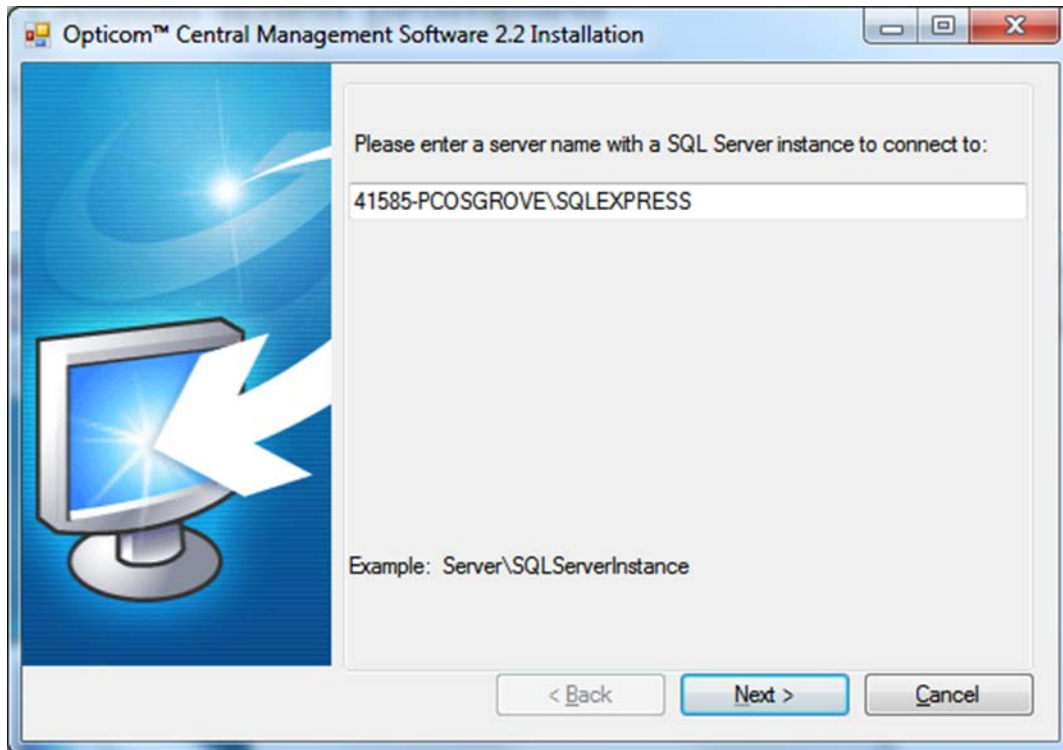


Figure 4- 2

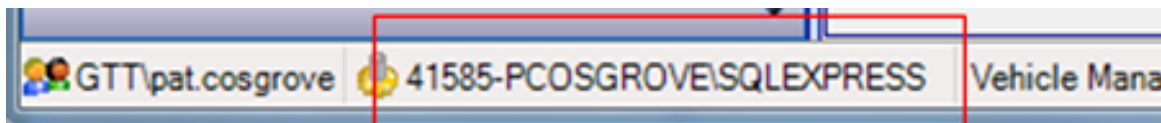
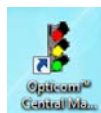


Figure 4-3

5. Launch the application from Start / Programs / GTT / Opticom Central Management Software or from the icon placed on the desktop.



6. Verify that the application starts up and is able to connect to the server machine.
 - a) If error screens appear refer to the appropriate sections of this manual for details on verifying that remote access is open, ports are open, the SQL instance is correct and your CMS user name matches your Windows login.
7. You will see the default Intersection Management screen. On the lower left, you'll see that you're signed into the application with your Windows account.

Note:

- **If the location of the SQL instance is ever moved it will be necessary to point all client machines to the new location.**
 - This may be done by uninstalling and reinstalling CMS on the client machines. Point to the new location when reinstalling.
 - You may also contact GTT Tech support for details on how to modify the settings on the client machine to point to the new SQL location.

4.2 Install firmware package

If you are using M764, M762, or M1000 phase selectors and or Model 2100 or 2101 radio/GPS control units, install the Opticom Firmware Package on each client machine. Since this information is not stored in the database, it must be installed on each client machine. See Section 17 for details.

4.3 Install GIS Map database

If you are using Opticom GPS, install the GIS map for your region on each client machine. Since this information is not stored in the database, it must be installed on each client machine. See Section 18 for details. Skip this section if your installation is Opticom Infrared only.

5 Additional Setup

The following items may be done on either the server machine or one of the client machines. It is only necessary to do these items one time since the information entered in this section is stored in the database.

5.1 Enter the product key

Your product key determines the number of intersections that you can configure. If you have purchased the optional Evacuation Plans module or Vehicle Communications module, you will be provided an additional product key for each purchased module/s. These keys are printed on a label on the CD jewel case

1. Open CMS and click on the **Tools** menu, select **Options**, then select **Product Information**.
2. Enter the product key, and press **Apply**.
 - a. After applying the base product key, the Product Information panel will be updated to show the number of intersections licensed, the number of intersections currently configured, and the number of remaining intersections.
 - b. After applying a product key for an optional module, that module will display as Licensed.

5.2 Set view options

The Central Management Software is used to communicate to devices that operate in Infrared only mode, GPS only mode or both modes simultaneously. The software may be set to display infrared only values and fields, GPS only values and fields or both simultaneously. Select the appropriate mode for the type of equipment that you are using.

1. Under the **Tools** menu, select **Options**, then select **Preferences**.
2. Set **View Information** to match the Opticom equipment in your region.

Valid Values:

- Opticom GPS and Opticom Infrared (Default)
- Opticom GPS
- Opticom Infrared

5.3 Enter mail server info

In order for CMS to generate e-mails it is necessary for CMS to access your mail server. This section allows you to tell CMS how to access the mail server.

Contact your mail administrator to determine if your mail server allows anonymous users. If not, request a user name and password for the CMS software to use and enter them in the appropriate fields.

1. Under the **Tools** menu, select **Options**, then select **Email Settings**.
2. Enter the following:
 - a. **Email From:** The "from" address used in report e-mails.

- i. Must be in an e-mail format.
- ii. i.e. opticomcms@anytown.com
- b. **Mail Server:** The computer name or IP address of your mail server.
- c. **User Name:** The user name for accessing the mail server.
 - i. Leave blank if your mail server allows anonymous users.
- d. **Password:** The password for accessing the mail server.
 - i. Leave blank if your mail server allows anonymous users.

5.4 Enter Region Name

The Region is an area that represents the scope of this central management software installation. It could be a county, metropolitan area, or city.

You may also enter address information and contact information. These fields are optional.

1. Under the **Tools** menu, select **Options**. Then select **Region** Information.
2. Change the word "Region" to your region.

5.5 Add users

Users must be added to the OpticomUsers Windows group. The details of this process are in section 3.6. If not the users will not be granted access to the database and will see the following error message in Figure 5-1 when they start CMS:

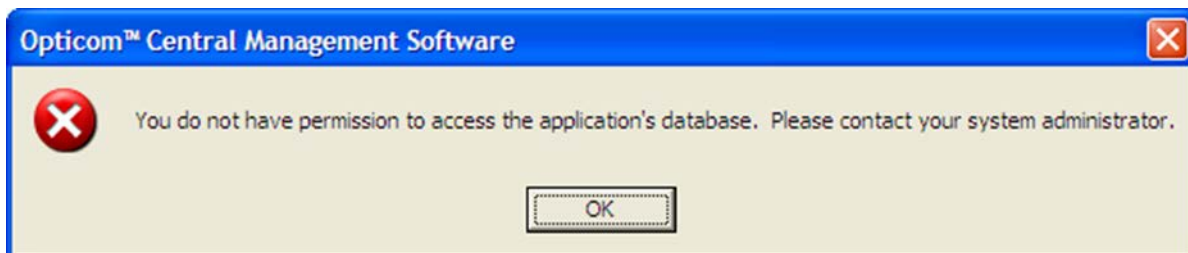


Figure 5-1

Once system users have been added to the OpticomUsers Windows group they will also need to be registered in the Central Management System via the Role Management Tab. Users who have not yet been registered with the application will see the error message in Figure 5-2 when they start CMS. Note that the message includes the user name in the format needed to be added to the database.



Figure 5-2

5.5.1 Opticom Central Management Software Roles

The following roles are supported by the application:

- The **Administrator** role can perform all operations.
- The **Intersection Management** role can configure and view jurisdictions, intersections, communication devices, and phase selectors, schedule jobs, and view monitoring information, Opticom logs and reports.
- The **Vehicle Management** role can configure and view jurisdictions, agencies, and vehicles, and view monitoring information, Opticom logs and reports.
- The **Monitoring** role can view monitoring information, Opticom logs and reports.
- The **Reporting** role can view Opticom logs and reports.

5.5.2 Add Users

1. The person adding additional users must already be entered in CMS as an administrator.
 - a. The person logged in when CMS was installed on the server is automatically added to both the OpticomUsers windows group and in CMS as an administrator.
2. Click on the **Role Management Tab** in CMS.
3. Select the desired level of the new user.
4. Click the **Add User** link.
5. Enter the user name in the format that they use to log into your network.
 - a. **This format must be correct and match the format that was added in the OpticomUsers windows group.**
 - b. **For network users, the format should be network\username.**
 - c. **For local computer users the format should be computer name\username.**
6. Add the users first and last name.
7. Add the users e-mail address (optional but recommended)
 - a. E-mails addresses added here will automatically be filled in in the reports scheduling e-mail to: screen.
8. Repeat to add additional users.

6 Configuring the Opticom Central Management Software System

6.1 Key Concepts

Opticom system central management software allows you to map your Opticom system equipment usage and ownership into your organizational framework. The key entities involved are:

Region: An area that represents the scope of an Opticom central management software installation. It could be a county, metropolitan area, or city.

Jurisdiction: A governmental unit or organization that controls intersections or agencies or both. It could be a city or a portion of a city system.

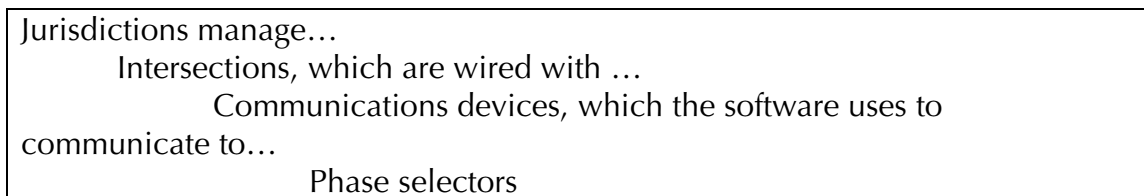
Intersection: A signalized intersection equipped with Opticom system phase selectors.

Communications Device: A COM device that lets CMS communicate to an Opticom device.

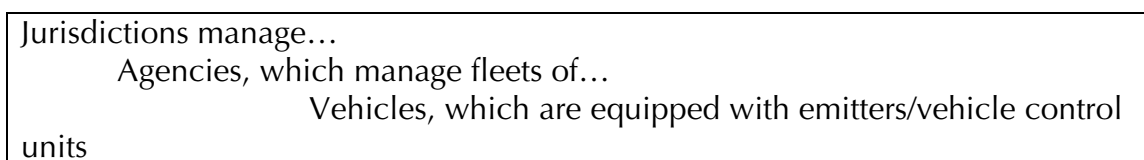
Agency: A governmental unit or organization that controls vehicles.

Vehicle: An emergency or transit vehicle equipped with Opticom system emitters and/or vehicle control units.

In Opticom central management software, “Intersection Management” is concerned with Jurisdictions, Intersections, Communications Devices, and Phase Selectors. The Intersection Management screen presents these entities in this hierarchy:



Likewise, “Vehicle Management” is concerned with Jurisdictions, Agencies and Vehicles (Optionally Vehicle communication devices and vehicle modules). The Vehicle Management screen presents these entities in this hierarchy:



Or

Jurisdictions manage...

Agencies, which manage fleets of...

Vehicles, which are equipped with emitters/vehicle control units

Communication devices which the software uses to communicate to Vehicle Modules

Any one jurisdiction manages either intersections, or agencies, or both. For example:

- One jurisdiction might be a particular city which manages both its intersections and its fire department. The fire department is an agency which owns vehicles (the fire trucks).
- Another jurisdiction might be a county which manages some intersections, but has no agencies.
- A third jurisdiction might be a metropolitan transit organization, with one or more agencies that operate buses.

With this information configured in its database, Opticom central management software can now help you understand how the Opticom system is being used, and by whom. Opticom central management software does this by combining the raw call history log tracked by the phase selectors with the organizational information. Within the software's database, the logs collected from phase selectors are categorized by intersection, and the jurisdiction that manages those intersections. Opticom central management software can also correlate the name of each vehicle making a call, as well as its owning agency. This lets you understand Opticom system usage across the region, for any one jurisdiction's intersections, at a specific intersection, by one agency's vehicles, or by a specific vehicle. You can see this activity within the past few minutes, or historically.

7 Adding Vehicles and configuring System Security/codes

If your Opticom vehicle equipment is not coded or all have the default code, there is no need to enter any vehicle information. Since the codes are all the same CMS will have no way to differentiate the vehicles. GTT recommends that all vehicles be programmed with a unique ID code.

Opticom central management software makes it easy to take full advantage of the benefits of Opticom system security in your region. There are several levels of security defined:

- Level 0: All vehicles are authorized.
- Level 1: All vehicles are authorized, except for those with uncoded emitters (infrared Class 0, ID 000). This level ensures that only GTT emitters are given access. This level applies only to Opticom infrared.
- Level 2: All vehicles are authorized, except for those with uncoded emitters (infrared Class 0, ID 000) and default-coded emitters (infrared Class 0, ID 001 and GPS 1:1:1). This level ensures that only vehicles that have been configured with a unique emitter code are given access.
- Level 3: Only vehicles from specifically allowed agencies are authorized. The agencies include those from the jurisdiction in which the intersection is located, plus any outside agencies that are granted access through mutual aid.

Security Level	Effective Code Map for Opticom GPS	Effective Code Map for Opticom Infrared
0	1:1:1 - 254:15:9999, minus explicitly blocked emitters	0 – 9999, minus explicitly blocked emitters
1	Not applicable	1 – 9999, minus explicitly blocked emitters
2	1:1:2 - 254:15:9999, minus explicitly blocked emitters	2 – 9999, minus explicitly blocked emitters
3	This jurisdiction’s agencies plus... any agencies granted mutual aid minus... explicitly blocked emitters	This jurisdiction’s agencies code allocation ranges plus... code ranges from any agencies granted mutual aid minus... explicitly blocked emitters

Opticom central management software lets you configure each of your (intersection owning) jurisdictions at one of these security levels, and evolve to more secure levels over time. Further, jurisdictions within the region can deploy different security levels. The code map pushed to the intersection depends on the security level set for the intersections’ jurisdiction, the mutual aid, and the explicitly blocked emitter list. See sections 8.3.2 and 8.3.5 for details on updating the security level/code maps in the phase selectors.

7.1 Jurisdiction Security Level

The jurisdiction's security level (0 through 3, as explained above) is set on the jurisdiction's properties form. While this can be accessed from either the Intersection Management activity or Vehicle Management activity, it's important to note that the security level applies to intersections, so it need only be set for intersection-owning jurisdictions. **Select the appropriate level when adding new jurisdictions.** See sections 8.3.2 and 8.3.5 for details on updating the security level/code maps in the phase selectors.

7.2 Agency and Code Allocation

An integral step in fully utilizing security is the development of a regional coding plan. Once developed, you can set this plan up in the Vehicle Management activity.

For Opticom GPS, a unique Agency ID is configured for each agency.

For Opticom infrared, it's necessary to allocate the available infrared code range among the region's agencies. Within the Vehicle Management module, select Allocate Opticom IR Agency Code Allocation, then enter the high and/or low priority code ranges for each agency. Once these allocations are configured, any vehicle whose emitter code is not within its agency's range is shown by a yellow highlight.

7.3 Allocate Opticom IR Agency Code Ranges

This section allows you to configure the range of IR codes that a particular agency will be using.

1. Add all Agencies either manually or using the import utility.
2. Click on **Allocate Opticom IR Agency Code Ranges**
3. Enter a start code number and an end code number for each agency in the appropriate priority level. See Figure 7-1.
 - a. There are separate fields for each agency for both high and low priority.
4. When complete press the button with two green check boxes to verify that overlapping code ranges have not been entered.
 - a. A validation successful message will appear if codes do not overlap.
 - b. Overlapping codes will be highlighted and a message will appear describing the overlapping codes
 - c. Change codes as needed to remove the overlap errors.

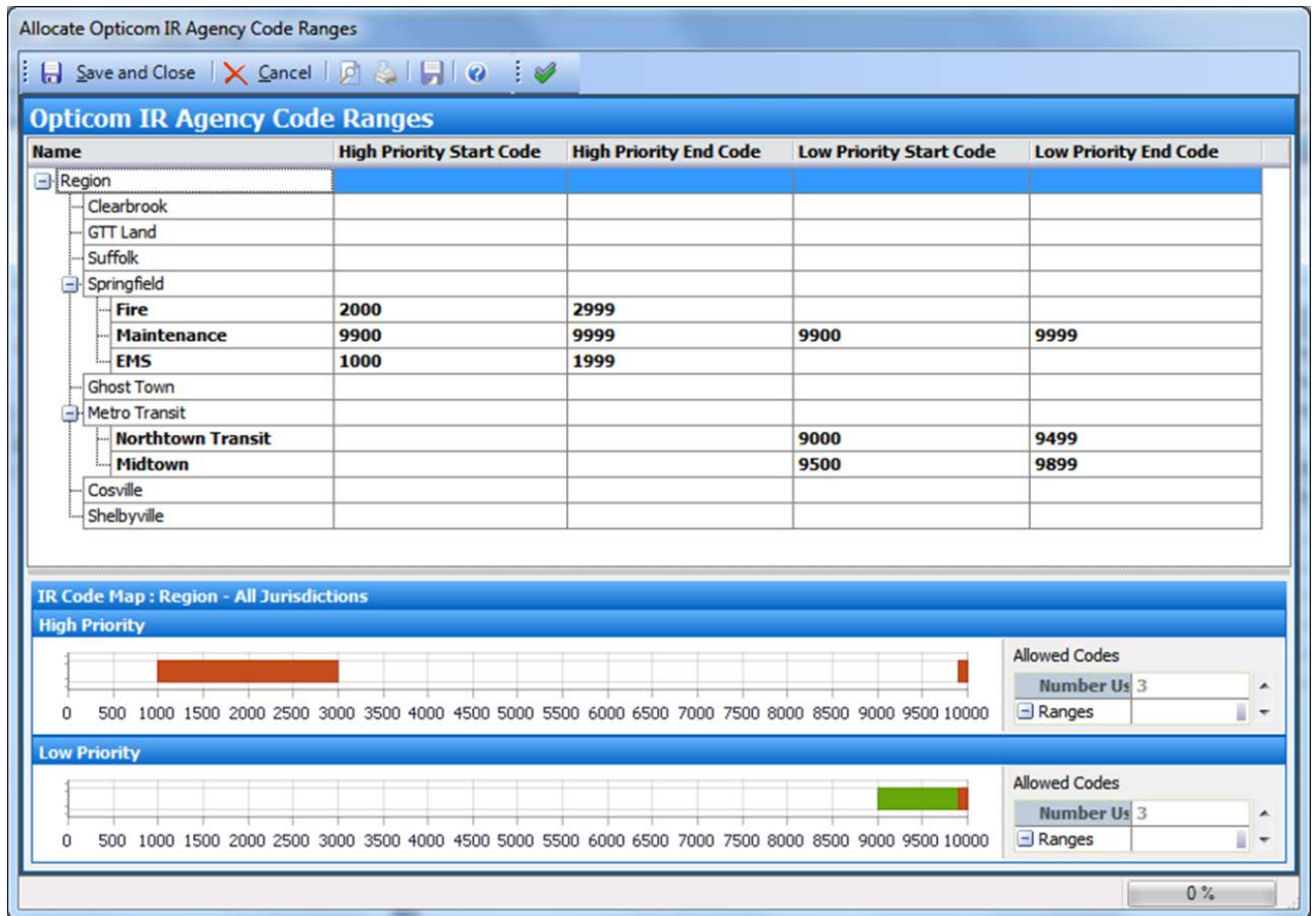


Figure 7-1

7.4 Configure GPS vehicle classes

This screen allows you to define what types of vehicles are assigned to a vehicle class. Default descriptions will be listed. This section only applies to Opticom GPS equipped vehicles. The default descriptions may be changed. See Figure 7-2.

1. Click on the Configure **Opticom GPS Vehicle Classes** link
2. Double click on the description to be changed and type a new description.
 - a) If a particular class is not in use, you may deselect the check box to deactivate it.
 - b) If the class is deactivated, it will not appear in the pull down lists in the vehicle configuration screens.
 - c) If a particular class is in use by a vehicle, it cannot be deactivated.
 - d) It is recommended that all classes be left active.

High Priority GPS Vehicle Classes			Low Priority GPS Vehicle Classes		
Class	Description	Active	Class	Description	Active
1	Fire Rescue/EMT/Ambulance	<input checked="" type="checkbox"/>	1	Regular Transit	<input checked="" type="checkbox"/>
2	Engine/Pumper	<input checked="" type="checkbox"/>	2	Express Transit	<input checked="" type="checkbox"/>
3	Ladder/Aerial/Snorkel	<input checked="" type="checkbox"/>	3	Paratransit	<input checked="" type="checkbox"/>
4	Brush	<input checked="" type="checkbox"/>	4	Light Rail	<input checked="" type="checkbox"/>
5	Miscellaneous	<input checked="" type="checkbox"/>	5	Trolley	<input checked="" type="checkbox"/>
6	Fire Chief/Captain	<input checked="" type="checkbox"/>	6	Snow Plows	<input checked="" type="checkbox"/>
7	Supervisor	<input checked="" type="checkbox"/>	7	Supervisor	<input checked="" type="checkbox"/>
8	Maintenance	<input checked="" type="checkbox"/>	8	Pavement Marking	<input checked="" type="checkbox"/>
9	Installer/Set-up	<input checked="" type="checkbox"/>	9	Installer/Set-up	<input checked="" type="checkbox"/>
10	Police/Sheriff Cars	<input checked="" type="checkbox"/>	10	Bus Rapid Transit	<input checked="" type="checkbox"/>
11	Miscellaneous Police/Sheriff	<input checked="" type="checkbox"/>	11	Not used	<input type="checkbox"/>
12	Police Chief/Supervisor	<input checked="" type="checkbox"/>	12	Not used	<input type="checkbox"/>
13	Private Ambulances	<input checked="" type="checkbox"/>	13	Not used	<input type="checkbox"/>
14	Not used	<input type="checkbox"/>	14	Not used	<input type="checkbox"/>
15	Base Station	<input checked="" type="checkbox"/>	15	Not used	<input type="checkbox"/>

Figure 7-2

7.5 Add Vehicles

With your agency and code information configured, you are now ready to add vehicles. If you are adding just a few vehicles, you can use a built-in wizard to manually step through the process of adding each vehicle and adding it to the database. If you have many to add, it's easiest to import them using the import utility.

7.5.1 Adding Vehicles Manually

If you are only adding a small number of vehicles it is probably easier to add them manually. You can then also manually allocate code ranges or GPS vehicle classes.

1. Click on the **Region** and then click on **Add Jurisdiction** (unless it has already been added.)
2. Enter the name of the Jurisdiction.
3. Select the security level of the Jurisdiction.
4. Click on **Add Agency** (unless it has already been added.)
5. Enter the name of the Agency
6. Select the priority level/s of the Opticom equipment on the vehicles in this Agency.
7. Select the type of equipment (IR and or GPS) on the vehicles in this Agency.
8. If GPS select the Agency ID.
9. Click on **Add Vehicle**.
10. Enter the name of the new vehicle
11. Enter the code of the Opticom equipment or press **Get Available Code** to pull a code from the assigned code range.

Note:

The Add Communication Device and Add vehicle module are only available and necessary on Opticom GPS Model 2100-2101 vehicle equipment that will be connecting to CMS. Contact GTT technical support for details.

7.5.2 Importing Vehicles

If you are adding many vehicles, it is easier to import them using the import utility. When you installed CMS an import utility and sample import spreadsheets were also installed. Go to program files and select the GTT program group and then to the Central Management Software folder. You will then see the Import utility program and a folder containing sample import spreadsheets. For vehicles there are three sample spread sheets, one for IR vehicles, one for GPS vehicles and one for dual equipped vehicles.

Notes:

- **Do not modify the headers or order of the columns in the import sample spreadsheet.**
- **The following columns are required:**
 - **Jurisdiction Name**
 - **Agency Name**
 - **Agency Priority Level (Required if using low priority)**
 - **Agency Equipment (GPS)**
 - **Agency ID (GPS only)**
 - **Code ranges (IR only)**
 - **Vehicle Name**
 - **Class ID (GPS)**
 - **Emitter Priority**
 - **Emitter Code**
 - **Not required but recommended**
 - **May be added later**
- **All other columns are optional**
- **Save the import spreadsheet in .csv format only**
- **You will be prompted with several save messages press OK or Yes for all.**
- **See the CMS and Import utility help file for more detail.**

1. Open the appropriate sample spread sheet for your vehicle type. See Figure 7-3
2. Select **Save As** and save the file under a new name in the .csv format
 - a. Press **Save** or **Yes** for all dialog boxes.
3. Enter the appropriate information in the spread sheet
4. **Delete any remaining sample information in the spreadsheet.**
5. Save the file in the .csv format
 - a. Press **Save** or **Yes** for all dialog boxes.
6. Open the **Import Utility** See Figure 7-4
7. Press the **Browse** button and point to the newly saved spreadsheet.
8. Press the **Populate** button
9. Upon successful import a dialog box will appear. The details of what was imported will also be listed.
10. Correct any issues in the import spread sheet if errors are encountered.
11. Press the **Refresh** button in CMS to update the screen after the import.

1	Jurisdiction Name	Agency Name	Agency Desc	Agency Priority	Agency Equip	Agency ID	Vehicle N	Vehicle D	Vehicle Id	Emitter Prior	GPS Class	GPS ID
2	Springfield	EMS	Springfield EMS	High	GPS	200						
3		Fire		High	GPS	201	Ladder 1248		1248	High	3	1248
4							Ladder 4569		4569	High	3	4569
5							Chief	Chief's car	1234567890a	High	6	344
6		Maintenance	Springfield traf	Low, High	GPS	1	Maintenance 1 High			High	9	1
7							Maintenance 1 Low			Low	9	1
8	Metro Transit	Northtown Trans	Covers the nort	Low	GPS	100	NT 7G801		7G801	Low	2	801
9							NT 7G802		7G802	Low	2	802
10							NT 7G803		7G803	Low	2	803
11							NT 7G804		7G804	Low	2	804
12							NT 7G805		7G805	Low	2	805
13							NT 7G806		7G806	Low	2	806
14		Midtown	Covers downto	Low	GPS	101	Arrow 123		1234567890a	Low	1	123
15							Arrow 124		234567890ab	Low	1	124
16							Arrow 125		34567890abc	Low	1	125
17							Arrow 126 No GPS Cl		4567890abcd	Low		

Figure 7-3

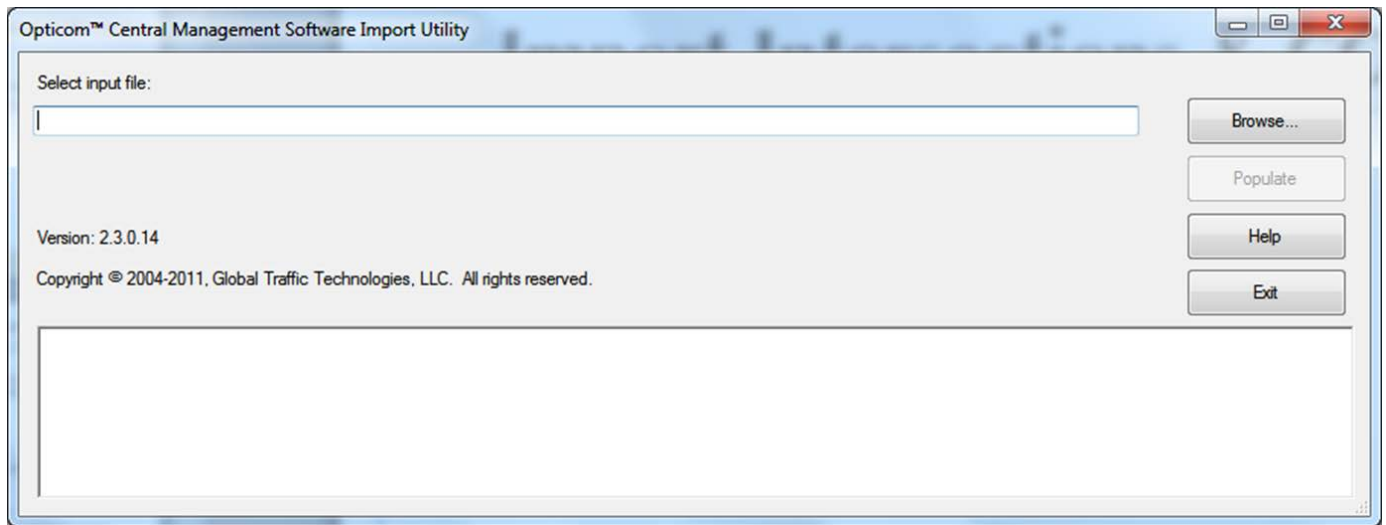


Figure 7-4

7.6 Mutual Aid

By default all jurisdictions will allow all vehicles from all other jurisdictions to activate the Opticom equipment in their jurisdiction. This is the case for security levels 0-2. Also by default, if Security Level 3 has been selected for a jurisdiction/s, the Opticom equipment in that jurisdiction's intersections will be configured to only allow that jurisdiction's agencies to use the Opticom system. By Configuring Mutual aid, you can extend access to agencies from other jurisdictions. Mutual aid can be one-way or reciprocal.

7.6.1 Configure Mutual Aid

1. Add all jurisdictions to CMS.
2. Set the Security level to 3 for jurisdictions that you wish to have mutual aid.
 - a) Mutual aid is only available for jurisdictions at Level 3. These configurable jurisdictions will be bold in the Configure Mutual Aid screen.
 - b) Jurisdictions not at level 3 will not be available to select configure mutual aid.
3. Click on **Configure Mutual Aid** in the **Vehicle Management** tab.
4. Expand a configurable jurisdiction, and there will be a list of all the other jurisdictions under it. See Figure 7-5
5. Expand these jurisdictions to see their agencies
6. For each jurisdiction, check the box next to the agencies whose vehicles you wish to allow access.
7. Update the code map for the changes to take effect.
 - a) See sections 8.3.2 and 8.3.5 for details on updating the code maps in the phase selectors.

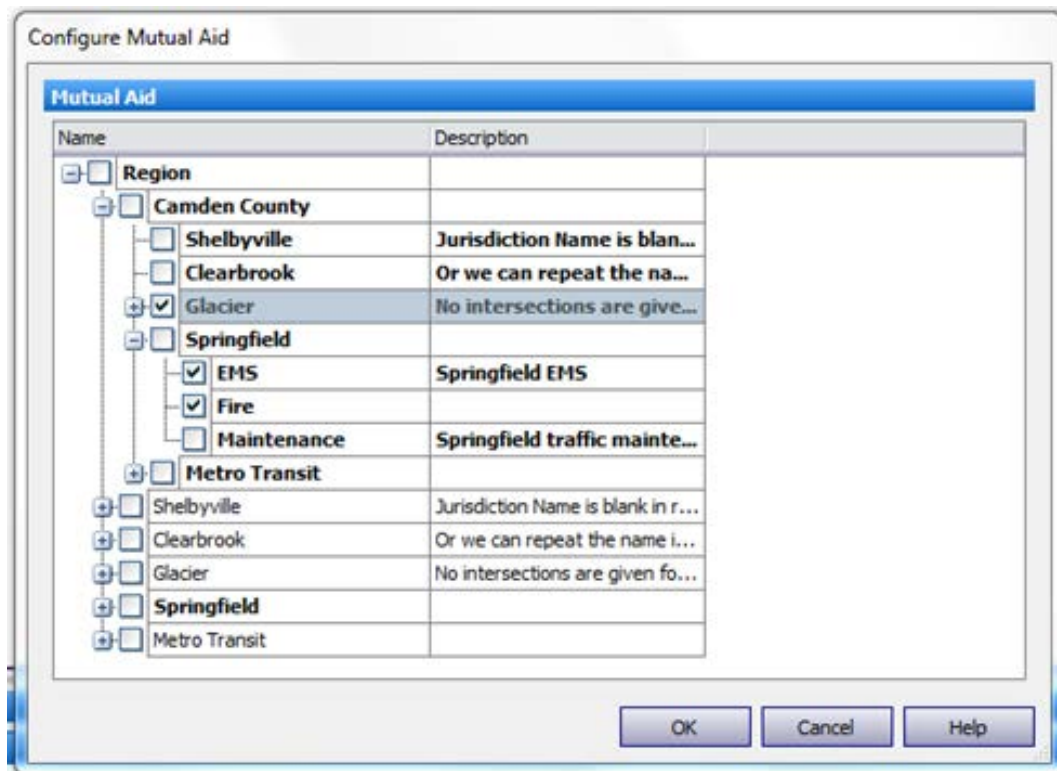


Figure 7-5

7.7 Explicitly Blocked Vehicles

You can further augment your use of Opticom system security by explicitly blocking codes via the Explicitly Blocked Vehicles Management dialog box in the Vehicle Management activity. You might want to block codes that you find in logs or reports and cannot be identified, or known missing or stolen emitters of vehicle control units, or even specific registered vehicles. The Explicitly Blocked Vehicle list applies across the entire region no matter the security level of a jurisdiction.

1. Click on **Manage Explicitly Blocked Vehicles** in the **Vehicle Management** tab.
2. Click on the **New** button
3. To block a single code or a range of codes select **Opticom IR** or **Opticom GPS** from the **Items to block** pull down menu.
 - i. Select the priority level
 - ii. Select the start and end codes that you wish to block for IR vehicles.
 - iii. Select the Agency, Class, and start and end vehicle IDs that you wish to block for GPS vehicles.
4. Select **Explicit Vehicle** from the pull down menu to block a specific registered vehicle.
 - i. Select desired vehicle from the **Select Vehicle** pull down list.
5. Click **OK** and click **Yes** to the confirmation message to save.
6. Update the code map for the changes to take effect.
 - i. See sections 8.3.2 and 8.3.5 for details on updating the code maps in the phase selectors.

7.8 Adding vehicles that will be connected to CMS

Model 2100 and 2101 vehicle radio/GPS control units may be connected to CMS via a third party radio. Model 2100-2101 devices connected to CMS may then download their logs and configuration to CMS and CMS can push firmware upgrades to the Model 2100-2101. This feature is only available with Models 2100 and 2101 devices. This feature also requires a separate CMS license. If you will be using this feature, contact GTT Technical Support for more details on installing and setting up your devices and CMS to use this feature.

If you are adding just a few vehicle modules, you can use a built-in wizard to manually step through the process of discovering each vehicle module and adding it to the database. If you have many vehicle modules to add, it's easiest to automatically add them via Active Monitoring.

When vehicle modules are added automatically through Active Monitoring, the vehicle module firmware is automatically updated if it is older than the version installed on your server and that version is selected in the Manage Firmware Updates task. It's necessary to first install the Opticom Firmware Package on your server and workstations as noted in Section 17.

7.8.1 Adding Vehicle Modules Manually

For each configured communications device in Vehicle Management, right-click the device, then select New | Vehicle Module. This begins a wizard with these three panels:

1. Device Settings / Communication Device Settings: Allows you to edit the settings of the communications device and device to be created.

Selecting Next causes the wizard to initiate communications with the vehicle module.

2. Device Information: If communications can be established with the vehicle module, this panel displays specifics about the device: Vehicle Name, Model Number, Serial Number, and Firmware Version. Confirm that these settings are as expected, then select Next.
3. The wizard reads further configuration information from the vehicle module, then writes this information to the database.

7.8.2 Adding Vehicle Modules through Active Monitoring

Using Active Monitoring eliminates much of the manual overhead in adding vehicle modules. Verify that an agency is created with the correct agency Id and priority in Vehicle Management, then under the Configure... task in Active Monitoring, check Monitor Vehicles to turn on vehicle monitoring. When a vehicle module with Central Management Software Connectivity enabled turns off its ignition while connected to the network, it will be automatically added to the database under the corresponding agency.

7.8.3 Updating Vehicle Module Firmware

The firmware in Model 2100 and 2101 vehicle radio/GPS control units may be updated. The firmware can be updated either manually or automatically through active monitoring. However, the radio and GPS receiver firmware connected to a Model 2100 or 2101 vehicle radio/GPS control unit cannot be updated.

To update a single vehicle module manually, select the Update Firmware operation for that device either in its properties screen or by right clicking on the device. The screen will inform you of the current version in the vehicle module and the latest available version in the installed Opticom Firmware Package, along with recommended update options.

To update vehicle modules in active monitoring, open the Manage Firmware Updates task which is only visible in Vehicle Status view. Select the firmware element(s) that you wish to update. While all monitored vehicle modules will be checked, only those with older firmware will be updated.

8 Adding Intersections and Phase Selectors

With your regional information configured, you are now ready to add intersections and phase selectors. If you are adding just a few phase selectors, you can use a built-in wizard to manually step through the process of adding each intersection and phase selector to the database. If you have many intersections and phase selectors to add, it's easiest to use the import utility and an automated Add Phase Selector job.

8.1 Adding Intersections Manually

If you are only adding a small number of intersections it is probably easier to add them manually.

1. Click on the **Region** and then click on **Add Jurisdiction** (unless it has already been added.)
2. Enter the name of the Jurisdiction.
3. Select the security level of the Jurisdiction.
4. Click on **Add Intersection**.
5. Enter the name of the Intersection.
6. Click on **Add Communication Device**.
7. Select **TCP/IP** and Enter the **IP address** and **Port number** of the phase selector or Communication server device.

8.2 Importing Intersections

If you are adding many intersections, it is easier to import them using the import utility. When you installed CMS an import utility and sample import spreadsheets were also installed.

Go to program files and select the GTT program group and then to the Central Management Software folder. You will then see the Import utility program and a folder containing sample import spreadsheets. Open the import sample intersections.csv file.

Notes:

- **Do not modify the headers or order of the columns in the import sample spreadsheet.**
 - **The following columns are required:**
 - **Jurisdiction Name**
 - **Intersection Name**
 - **COM device type**
 - **Port**
 - **IP Address**
 - **All other columns are optional.**
1. Open the Import Sample Intersections.csv spread sheet. See Figure 8-1
 2. Select **Save As** and save the file under a new name in the .csv format
 3. Press **Save** or **Yes** for all dialog boxes.
 4. Enter the appropriate information in the spread sheet
 5. Delete any remaining sample information in the spreadsheet.
 6. Save the file in the .csv format
 7. Press **Save** or **Yes** for all dialog boxes.
 8. Open the **Import Utility** See Figure 7-3

9. Press the **Browse** button and point to the saved spreadsheet.
10. Press the Populate button
11. Upon successful import a dialog box will appear. The details of what was imported will also be listed.
12. Correct any issues in the import spread sheet if errors are encountered.
13. Press the **Refresh** button in CMS to update the screen after the import.

	A	B	C	D	E	F	G	H	I
1	Jurisdiction Name	Jurisdiction Desc	Intersection Name	Intersection Id	Other Information	Comm Device Type	Port	IP Address	Device Address
2	Springfield	A nice place to live.	Afton Blvd S and St. Croix Trail S		This column demons	TCP/IP		2101 192.168.100.63	
3			Manning Ave S and Bailey Rd	MB9	Note that we left ou	TCP/IP		2101 192.168.100.64	
4			Manning Ave S and Hudson Rd S	MH10		TCP/IP		2101 192.168.100.65	
5			Manning Ave S and Valley Creek Rd	MV11		TCP/IP		2101 192.168.100.66	
6			Helmo and 47th	MV12		TCP/IP		2101 192.168.100.67	
7			Stagecoach Trail S and Hudson Rd S			TCP/IP		2101 192.168.100.68	
8	Shelbyville	Jurisdiction Name is bla	Lake Rd and Woodbury Dr			TCP/IP		2101 192.168.100.69	
9			Tamarack Rd and Radio Dr			TCP/IP		2101 192.168.100.70	
10			Tamarack Rd and Woodbury Dr			TCP/IP		2101 192.168.100.71	
11			Valley Creek Rd and Radio Dr			TCP/IP		2101 192.168.100.72	
12			Valley Creek Rd and Woodbury Dr			TCP/IP		2101 192.168.100.73	
13	Clearbrook	Or we can repeat the n	Century Ave S and Upper Afton Rd E			TCP/IP		2101 192.168.100.74	
14	Clearbrook		The Great River Rd and Carver Ave E	RiverGate20		TCP/IP		2101 192.168.100.75	
15	Clearbrook		The Great River Rd and Lower Afton Rd E	LowerRiverGate25		TCP/IP		2101 192.168.100.76	
16	Clearbrook		The Great River Rd and Upper Afton Rd	UpperRiverGate26		TCP/IP		2101 192.168.100.77	111
17	Clearbrook		Grodahl Dr and Upper Afton Rd			Serial	1		112
18	Clearbrook		White Bear Ave N and Upper Afton Rd E			Serial	1		113
19	Ghost Town	No intersections are given for this town so we'll just get a new jurisdiction with no intersections.							

Figure 8-1

8.3 Adding Phase Selectors

Once the intersection and COM devices have been added, the phase selectors can then be discovered and added to the database. Phase selectors may be discovered/added manually one at a time or through a phase selector discovery job. If you are only adding a few phase selectors it is probably easier to add them manually. If you are adding a large number, it is probably easier to run a phase selector discovery job.

When phase selectors are added, the phase selector's clock is automatically set to ensure that all future logs are properly time-stamped. If done through a job, the central management software server's clock is used as the source. If done manually, the clock from the computer on which you are running the user interface is used. Be sure that the computer clock uses an accurate time source, such as network time protocol (NTP).

When Model 1000 phase selectors are added, the phase selector firmware and radio module firmware are automatically updated if they are older than the minimum required versions. It's necessary to first install the Opticom Firmware Package on your server and workstations as noted in Section 17.

8.3.1 Discovering Phase Selectors Manually

1. Click on the **TCP/IP** communication of the intersection that you wish to add a phase selector. This will activate the **Add Phase Selector** button.
2. Click on **Add Phase Selector**. This will bring up a new window
3. Check the Discover Opticom GPS M1000 phase selectors box only if discovering Model 1000 devices.
 - a. **Note: Box will remain checked on subsequent add Phase selectors.**
4. Verify that the Wildcard check box is checked.
5. Click on the **Next** button. This will begin the initial discovery process. :
 - a. If communications can be established with the phase selector, this panel displays specifics about the device: Intersection Name, Model Number, Serial Number, and Firmware Version. Confirm that these settings are as expected.
6. Click on the **Next** button again when prompted.
 - a. Additional configuration information is then read from the phase selector, then saves this information to the database.
7. Click on the **Finish** button when prompted.

8.3.2 Adding Phase Selectors through a Job

Before running a phase selector communication job you will need to add the intersection and COM device as described in section 8.1 or 8.2. The phase selector discovery job will go out and attempt to locate and add a phase selector at the address that you specified.

1. Open the **Scheduling** tab.
2. Click on **Phase Selector Communication** link.
3. Enter a job name such as **Add new phase selectors**
4. By default the **Start Now** check box is checked.
 - a. Leave it checked to run the job immediately or uncheck the box and enter the desired start date and time.
5. Select **Add new phase selectors**.
6. Chose the location of the phase selector to be added in the **Choose intersections** section.
 - a. Choose **Select by jurisdiction** or
 - b. **Select by intersection** (then select the desired intersections)
7. If adding Model 1000, 752 or 754 phase selectors
 - a. Check the **Set Daylight Savings Time ... and Enable all logging.. check boxes.**
 - b. There is no need to do this with other model phase selectors.
8. Check the **Set Valid Code Map** check box if your Jurisdictions have their Opticom Security level set to anything other than Level 0 or you have explicitly blocked any codes or vehicles.
 - a. This will block the appropriate codes in all of the phase selectors.
 - b. See section 7 for more detail.
9. If you are discovering Model 1000, 762, 764 phase selectors and Model 768 AIPS and you know the firmware is out of date you may also check the appropriate check boxes under the firmware section to update the firmware. See section 8.3.4 for details.
10. Press **Save and Close** to start the job.
11. The job progress may be followed in the Scheduling screen.
12. When complete the new phase selectors will have been added to the database.

13. Press the refresh button on the Intersection Management screen to see the newly added phase selectors.

8.3.3 Additional Phase selector setup

After the phase selectors have been added to CMS, you'll want to enter or verify the following information in the phase selectors:

- Channel names have been entered
 - Channels not in use are marked as such.
- Green Sense information
- DST table updated (M1000 and 750 series only)
- All logging enabled (750 series only)
- Not set as emitter master (750 series only)
- Firmware on all devices is current (n/a on 750 series)
- Update phase selector code maps

Note:

- **The recommended method is to program this information into the phase selector while it is being installed in the field.**
- **It is very important to mark any channels that are not being used as "Not in Use" See Figure 8-2.**
 - **This will prevent unused channels from appearing to the inactive intersections report**
 - **In the case of infrared it will prevent the unused channels being reported as having a missing detector.**

1. Open the properties screen and go to Channel configuration.
 - Update channel names
 - These values are used in the central management software's logs and reports as approach descriptions, so it's very helpful to use meaningful identifiers, typically based on direction of travel (e.g., "Northbound" or "NB").
 - If there are no saved channel names in the database, channel names in logs from these units will be marked only with the channel letter.
 - Drop-down selections for channel names are provided to make it easier to set meaningful approach descriptions. You can customize the displayed channel names in Tools / Options / Preferences.
 - Mark channels not being used by checking the Not in Use check box
 - Model 752 and 754 phase selectors with firmware versions 1.x do not allow you to write channel names to the phase selectors, but CMS allows you to save channel names in the database.
 - See Figure 8-2.
 - Green sense information Desired Greens:
 - If green sense is connected, record the phase assignments for each channel in the phase selector's Desired Greens field. When desired greens are configured, the software notes for each call whether the greens that were active at the end of the call match those configured for the approach.

Consistent mismatch can indicate a wiring or configuration issue at the intersection.

- For Model 1000 and Model 764s operating in GPS mode you will want to record the desired greens for straight, left and right.
 - Record green phase assignment in the channel description section of Model 1000.
 - See Figure 8-2.
 - For any Model 752 or 754 phase selectors verify that none of them are configured as emitter masters. Emitter Master:
 - Phase selectors in this mode forward preemption requests to an attached emitter in order to relay the request to a second phase selector. Because this serial communication can interfere with Opticom central management software messages, GTT recommends that phase selectors in Emitter Master mode not be used with this software.
2. Repeat for each of the channels on the phase selector.
 - 3.

The following items may be updated by running a phase selector communication job and selecting the options.

If you used a discovery job you should have selected these items as part of the discovery job. If so it is not necessary to do the following steps.

- Enable Logging:
 - Phase selectors can be configured to log calls from valid emitters, calls from invalid emitters, and/or calls from probe emitters.
 - Valid and invalid refer to whether the emitter is allowed by the code map in the phase selector).
 - GTT recommends that you enable logging for all categories
 - By default Model 762,764 and 1000 phase selectors will log all types of calls.
 - By default Model 752 and 754 phase selectors will not log invalid id.
- Update the Daylight Savings Time (DST) tables in the phase selector:
 - Recommended for Model 1000, 752 and 754 phase selectors because these phase selector store the dates for the beginning and end of DST. These dates changed in 2007 and older phase selectors may still contain the old dates.
 - Not necessary for Model 762 and 764 phase selectors because these phase selectors do not store daylight savings time dates tables.
 - Verify that the time zone is set correctly on the server machine prior to updating.
- See section 8.3.6. for details on running a phase selector communication job.

Channel A	
General	
Channel Name	North Bound
Not In Use	<input type="checkbox"/>
Confirmation	
Desired Green Phases	
Left	Phase 2, Phase 5
Right	Phase 2, Phase 5
Straight	Phase 2, Phase 5

Figure 8-2

8.3.4 Updating Phase Selector Firmware

As part of the initial setup it is recommend that the firmware in your devices be updated to the latest version. The firmware in Model 762/764 and Model 1000 phase selectors may be updated. The firmware in Model 768 auxiliary interface panels may be updated. The radio and GPS receiver firmware connected to a Model 1000 phase selector may be updated.

The radio and GPS receiver firmware connected to a Model 764 phase selector cannot be updated.

The firmware cannot be updated in model 750 series phase selectors.

To update the firmware in the device/s in a single intersection, select the Update Firmware operation for that phase selector. The screen will inform you of the current versions and the latest available version in the installed Opticom Firmware Package along with recommended update options.

To update a number of devices in-bulk, create a Phase Selector Communication Job, then select the firmware element(s) that you wish to update and the intersections that you wish to update. While all selected intersections will be checked, only those with older firmware will be updated. See section 8.3.6. for details on running a phase selector communication job.

See section 17 for more details on downloading and installing the firmware package.

Note:

- **The preemption / priority system is inoperable while a firmware update is in progress. The duration is typically one to two minutes for phase selector, auxiliary interface panel, and radio firmware and 15 – 20 minutes for GPS receiver firmware, but could vary depending on your communications infrastructure.**
- **A firmware update will be prevented when a preemption / priority call is already active, but once the update is started, further calls are ignored until the update is completed.**

8.3.5 Updating Phase Selector Code Maps

If you have configured a security level other than zero for your jurisdictions, have added explicitly blocked vehicles and or setup mutual aid, it will be necessary to push a code map to your phase selectors. (See section 7.6, 7.7).

If you discovered the phase selectors through a job and selected update code map (section 8.3.2.) no further action is needed.

If you discovered phase selectors manually, you will need to schedule a Phase Selector Communication job to push code maps to your phase selectors. See section 8.3.6. for details on running a phase selector communication job.

8.3.6 Phase Selector Communication Job

This section describes how to update information in phase selectors already in the CMS database. The information and settings are described in sections 8.3.3-8.3.5.

1. Open the **Scheduling** tab.
2. Click on the **Phase Selector Communication** button.
3. Enter a job name such as Update new phase selectors
4. By default the **Start Now** check box is checked.
 - a. Leave it checked to run the job immediately or uncheck the box and enter the desired start date and time.
5. Select **Service configured phase selectors**.
6. Chose the location of the intersection/s to be updated in the **Choose intersections** section.
 - a. Choose Select by jurisdiction and all intersections in a selected jurisdiction will try to update information.
 - b. Choose Select by intersection (then select the desired intersections) and only those selected intersections will try to update information.
7. Select the following options as needed
 - a. **Set Daylight Savings Time ...**
 - b. **Enable all logging...**
 - c. **Set Valid Code Map...**
 - d. **Firmware update...**
8. Press **Save and Close** to start the job.
9. The job progress may be followed in the Scheduling screen.

9 Active Monitoring

With phase selectors (and optionally 2100-2101 vehicle modules) now added to the database, you're ready to set up active monitoring of device status and priority call activity. When enabled, active monitoring performs these steps in the phase selector:

- Regularly polls each monitored device to ascertain current device status and to retrieve any new priority call logs.
 - Log in the phase selector prior to discovery will not be uploaded because it is unknown if their clocks were correct.
 - Logs that are uploaded to CMS are not deleted from the phase selector.
- Displays active preemption and priority calls.
- Once a day, retrieves phase selector configuration and reports any change from the configuration stored in the central management software database. This happens at a random time throughout the day for each device.
- Sets the device clock (to server time) daily at 3:00 A.M.
 - This time reset is overwritten by phase selectors operating in GPS mode since these device clocks are updated continually by the GPS satellites.
- For phase selectors operating in infrared mode, CMS will analyze the optical detector health. Detectors that fall outside of normal parameters will be reported. This will happen daily at 1:00 A.M.

9.1 Configure Active Monitoring

Prior to starting the monitoring job, it's important to configure the monitoring job.

1. Click on **Configure** to expand the monitoring configuration screen
2. Verify that the **Monitor intersections** check box is checked to monitor the intersections.
3. Set the desired Poll rate.
 - a. The intersection poll interval is the *minimum* time between successive polls of each phase selector (but can be dynamically extended by the monitoring job based on job load).
 - b. Default rate is enabled once every 60 seconds.
 - c. Range 1-300 seconds(5 minutes)
 - d. Recommend 10 seconds
 - e. See sections 9.2.1. & 9.2.2 for more information on determining the appropriate poll rate.
4. Check the Track vehicles check box and select the rate if you wish to increase the poll rate when CMS sees that an intersection is actively in preempt.
 - a. The vehicle tracking interval is the *minimum* time between successive polls of the phase selector to obtain information about vehicles requesting preemption. This extra polling is optional and only performed when the intersection is known to be in preemption.
 - b. Default is disabled (set to 5 seconds).
 - c. Range 1-60 seconds.
 - d. Recommend 2 seconds.
5. Analyze Infrared detectors
 - a. Check this check box if operating in infrared mode,

- b. Do not check this box if operating in GPS mode.
- c. Default is enabled.
- 6. Monitor Vehicles
 - a. Check this box if you have Model 2100 or 2101 Opticom GPS vehicle units that are connected to and monitored by CMS. Its default is disabled. This option cannot be enabled until a Vehicle Communications license is entered.
 - b. When enabled, vehicle module configurations are retrieved and any change from the saved configuration is reported for all monitored vehicle modules.
 - c. When enabled, vehicle module firmware is updated with the firmware version selected in Manage Firmware Updates, if needed, for all monitored vehicle modules.
 - d. Vehicle modules will be discovered automatically through active monitoring if a vehicle module's priority and agency Id matches an existing agency.
- 7. Generate Alerts
 - a. Check this box if you wish to generate alerts.
 - b. Default is enabled
 - c. Configure the alerts that you wish to receive.
 - d. See section 9.3 for details.
- 8. Press the **Update** button to apply the changes.

9.2 Start Active Monitoring

1. Click on the **Start Monitoring Job** button to start the monitoring job.
 - a. It may take some time for the job to start.
 - b. Once it has started you will see a green dot and it will say "Monitoring". See Figure 9-1.
2. To monitor phase selectors, go to the Intersection Status view Right click individual phase selectors, or groups of phase selectors, and select **Start Monitoring**.
 - a. As each phase selector is brought into the monitoring state, you'll see its current device status change to monitoring.
 - i. Their status will be listed as Normal with a green dot. See figure 9-2.
3. To monitor vehicle modules, go to the Vehicle Status view, right click individual vehicle modules, or groups of vehicle modules, and select Start Monitoring. As each vehicle module is brought into the monitoring state, you'll see its current device status change to Not in Communication.

Note:

- **Newly discovered devices will default to Not Monitored.**
 - **Right click individual phase selectors, or groups of phase selectors, and select Start Monitoring.**



Figure 9-1

Status: ● Normal (2)				
GTT Land	Ideal Ave & Third Street	Opticom M764	1/23/2012 1:36:56 PM	
GTT Land	Ideal and GTT Exit	Opticom M764	1/20/2012 3:29:55 PM	

Figure 9-2

9.2.1 Stop Active Monitoring

1. Click on **Stop Monitoring Job** button to stop the monitoring job.
 - a. It will take some time for the job to stop.
 - b. It will say Stopping Monitoring Job.
 - c. Once it has stopped you will see a red dot and it will say “Not Monitoring”. See Figure 9-3.

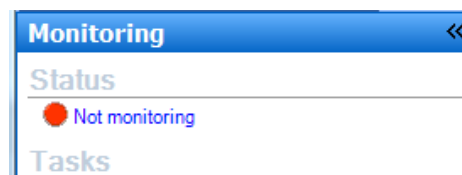


Figure 9-3

9.2.2 Fine Tuning Polling Rate

The following process is recommended for tuning the monitoring job settings. It uses server processor utilization to help select a sustainable polling level (note that the monitoring job does not consume a significant amount of server memory). You can observe server processor usage through Task Manager or the Windows® Performance utility under Administrative Tools.

1. Begin the tuning process with the default monitoring job settings (intersection poll interval of 60 seconds and vehicle tracking disabled), and the monitoring job stopped. Note the baseline processor utilization without monitoring.
2. Start the monitoring job. The monitoring job is active when Status is displayed as Monitoring.
3. Once the monitoring job is active, start monitoring a few intersections (right-click the set of desired intersections and select Start Monitoring).
4. Verify that this first set of intersections is polled by observing an update to the Last Update column of the Intersection Status view). At this point, server processor utilization should be only nominally above the baseline without monitoring.
5. Start monitoring all intersections and wait for the first poll to complete on the additional intersections. Note that this first poll fetches the full phase selector configuration, so processor utilization will level off once the first poll has completed on all phase selectors.
6. At this point, note the processor utilization with the default (60 second) intersection poll interval.

7. Lower the poll interval until you achieve an optimal balance between processor utilization and response time. It's best to keep processor utilization at 50% or less so that server resources are available for other work such as generating Opticom system reports. Be sure to give a few minutes for the utilization to level off with each change to the poll interval.
8. Enable vehicle tracking. If you are operating with emergency vehicle preemption only, you will likely be able to sustain a 5-second poll rate or lower, since the vast majority of intersections are not in preemption at any one time. If you are running substantial transit signal priority activity, you should select the poll interval by observing processor utilization during peak periods of transit activity.

9.2.3 Network Traffic

The network traffic for central management software varies with the configured monitoring poll rate). The following tables provide the approximate network traffic per monitored intersection.

Network traffic (KBytes / second) for Model1000,762 &, 764 phase selectors:

Intersections	50	100	300	500
Poll rate (sec)	25.0	50.0	150.0	250.0
1				
5	5.0	10.0	30.0	50.0
10	2.5	5.0	15.0	25.0
20	1.3	2.5	7.5	12.5

Network traffic (KBytes / second) for Model 750 phase selectors

Intersections	50	100	300	500
Poll rate (sec)	10.0	20.0	60.0	100.0
1				
5	2.0	4.0	12.0	20.0
10	1.0	2.0	6.0	10.0
20	0.5	1.0	3.0	5.0

9.3 Alerts

You can configure the system to produce alerts on specific priority calls or system events. Add an alert rule for a specific type of priority call or system event of interest.

The alert rule includes a pattern to be matched to specific call or event fields to detect the event. For example, you can detect a long priority call with a simple alert rule that looks for calls with *duration > 120 seconds*. Or you can generate an alert for any device status error by selecting *operation = device status* and *severity = error*.

You can also create a custom message of the alert text. The custom message is any combination of free-form text and fields from the detected call or event.

All alerts are displayed in the Alerts pane in the Monitoring screen. You can also add one or more e-mail recipients to receive the alert. Alerts can be sent as text messages by configuring the destination e-mail address to use the text message service provided by your phone company.

9.3.1 Configuring Alerts

It is recommended that you experiment with the alerts to determine the configuration that meets your needs.

1. Click on **Add Alert Rule**.
2. Enter a name for the alert.
3. Enter a description of this alert if desired.
4. select the alert type
 - a. **Opticom Log** alerts pull information from call history logs or preemption activity.
 - b. **Event Log** alerts pull information from the event logs generated manually by users, during scheduled jobs, and during monitoring.
5. Deselect the **Active** check box if you wish to create the alert but do not wish to activate it.
6. Click on **Alert filter**
7. Select the **Field** that you want to base the alert on.
8. Select the **Operator** to apply to that field
9. Select the **Value** that you want the alert to look for.
10. Add additional **Conditions** and **Groups** of Conditions as desired.
11. Click on **Alert Message**
12. Check the **Send E-mail** check box to have the alert send an e-mail.
13. You may enter a maximum number of e-mails in a specific time frame to prevent your inbox from being flooded by alerts that may generate a larger than expected number of messages.
14. Enter the e-mail address that you wish the alert to go to.
 - a. Separate e-mail addresses by a comma, semicolon, space or new line.
 - b. Pressing the **Validate Addresses** button will check the format of the e-mail addresses. It will not verify that the addresses are correct
15. The alert text box contains an example of the recommend method for creating the alert message.
 - a. Remove any fields or text that you do not wish to send.
 - b. Place your cursor in the text box at the location that you wish to enter text or a field
 - i. Double click on the desired field to add it to the Alert text.
 - ii. Enter desired text in between the fields.
16. Press **Save and Close**.
17. You can see the alert rules by selecting **Alert Rules** in the view section of the Monitoring screen.
18. To edit a particular alert, right click on the alert and select **Properties**.

10 Provisioning, decommissioning, replacing & deleting a device

10.1 Provisioning a Replacement Device

You can use central management software to provision a phase selector or vehicle module replaced in the field. This allows you to dispatch a technician to swap a device, then populate the configuration from central, rather than having to configure the device at its location using the ITS Link or On-site software. This pushes the previous device's configuration from the database to the new device, saving the time required to do the same operation manually using ITS Link or Opticom On-site.

For Model 762, 764, 2100 and 2101 devices you must first program in the IP address, port number, subnet mask, gateway etc into the device using On-site before installing it in the field.

To provision the device, simply select the Write To Device operation for the device. The software notes that the device's serial number has changed and asks if you wish to provision the replacement device. Optionally, if you've already set up the configuration in the replacement device, you can choose to read the replacement device's configuration into the database.

You may optionally write an older version of the configuration to the device. Select the desired older configuration file from the revision section of the properties screen of the device, right click and select, Write this revision to device

This capability is available for all phase selector models, but can only be used when swapping a phase selector for one of the same model.

10.2 Decommissioning a Device

There are some situations where a phase selector or vehicle module is no longer in use in the field, but you wish to keep it visible within the software. You can keep such a device visible by "decommissioning" it.

When decommissioned, the device and its Opticom logs remain visible within the central management software, but no communication is possible with the device. This capability is used when replacing a phase selector with one of a different model (add a new phase selector in the software for the newer model device, and decommission the old phase selector) or when replacing two 2-channel phase selectors with a single 4-channel phase selector (replace one of the 2-channel devices with the new one and decommission the other 2-channel).

To decommission a device, Right click on the device to be decommissioned and select Decommission.

10.3 Deleting a device

If you select delete rather than decommission. All logs and configuration files for that device will be permanently deleted.

To permanently delete a device, Right click on the device to be deleted and select Delete.

11 Central Management Software Access Control

11.1 Service Accounts

The GTT Communication Service and GTT Scheduling Service are installed to run under the System account. You may want to reconfigure the Scheduling Service to run under another account for one or both of these reasons:

- The Scheduling Service is allowed access to the Opticom Management database through SQL Server's default NT AUTHORITY\SYSTEM login. If your site has removed the NT AUTHORITY\SYSTEM login for security reasons, then you will need to configure the Scheduling Service to run under another account.
- You might want to schedule jobs to use a network share to save files. Because the SYSTEM account does not have permission to access network resources, you will need to use a domain account with write access to the share.
- Examples of items to save on a network share:
 - Import offline files
 - Save archived files during a pruning job
 - Save sent e-mails
 - Save sent reports

11.1.1 Configure the Scheduling Service to use an alternative account

1. You may use either a local account or a domain account, but will want to use a domain account if you want to write reports to a network share.
2. Add the selected account to the "Opticom Users" Windows group to allow it to access the Opticom database. See Section 3-6.
3. Using the "Services" utility under Administrative Tools, stop the GTT Scheduling Service, double click on the service to bring up its properties screen then configure the selected account's User ID and password in the "Log On" tab, then restart the service. Note that it will be necessary to update the password using the Services utility if the password expires. See Figure 11-1.

Note:

- **When configuring a job to write reports to a network share, you must use the share's Universal Naming Convention (UNC) name and not a mapped drive. Windows services cannot access mapped drives.**

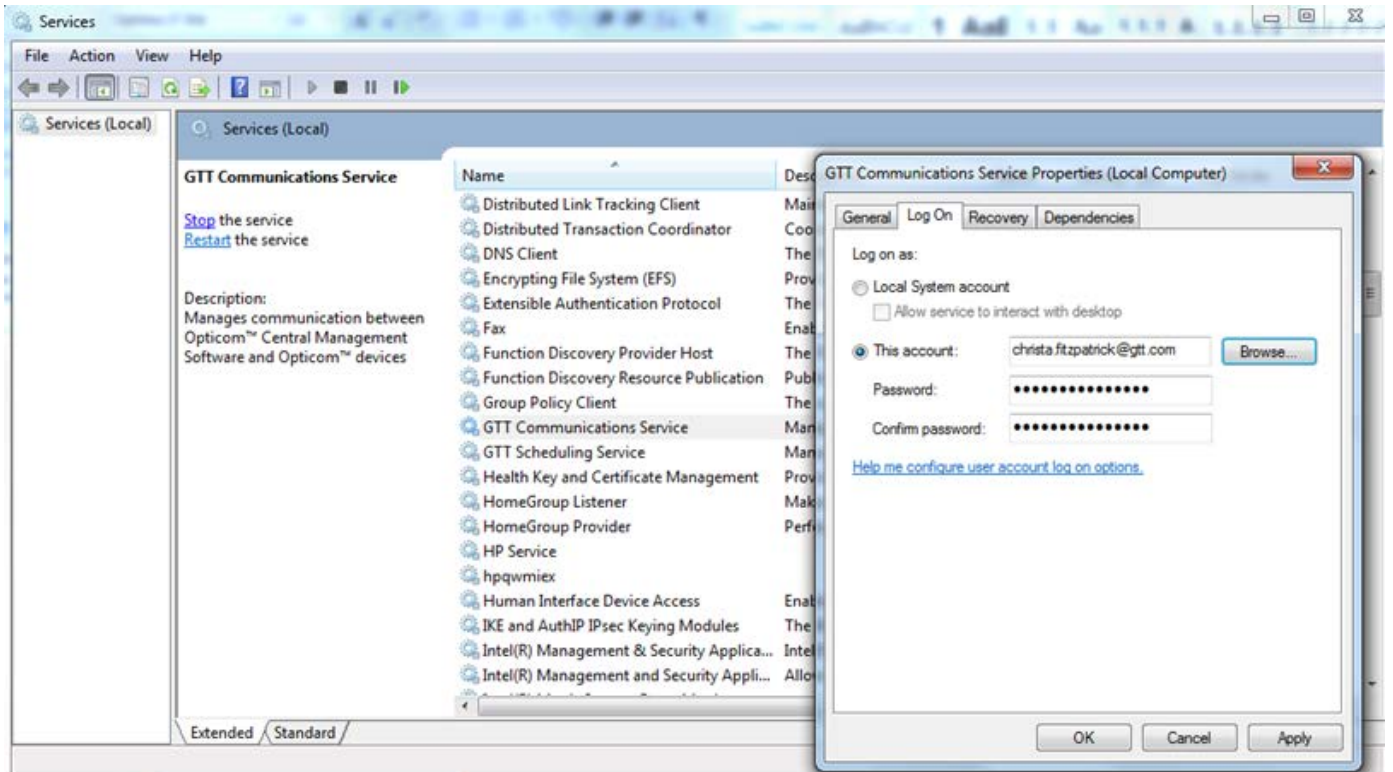


Figure 11-1

12 Maintaining the CMS Database

This section describes details about pruning and backing up the database.

12.1 Pruning the Database

An application maintenance job can be configured in the software to provide automated archiving and pruning (data trimming) of the database. Archiving and pruning can be selected based on either age of the data or record count. Data that can be selected includes Opticom logs, event logs, and device configuration files. The pruning job can be configured to completely delete the selected records from the database or to delete them but save an archive copy in the .csv format. Archived files cannot be imported back into CMS. They must be viewed with a program like Microsoft Excel.

Note that the archiving process is implemented using SQL Server's OLE Automation Procedures. By default, OLE Automation Procedures are disabled in SQL Server. When performing the archiving step when OLE Automation Procedures are disabled, the GTT Scheduling Service temporarily enables use of OLE Automation Procedures, performs the archive, then returns OLE Automation Procedures to disabled. The Scheduling Service is able to perform this operation as long as Opticom central management software and SQL Server are in their default configuration. See Section 11 for information on modifying the Scheduling Service to run under a different account if needed in your environment.

12.1.1 Creating a Database Archiving and Pruning Job

1. Open the **Scheduling** tab
2. Click on **Application Maintenance Job**
3. Select **Database Archiving and Pruning from the Maintenance Job** pull down list.
4. Place a check box next to the **Database Items** that you wish to prune/archive.
5. Select **Prune by age** or **Prune by record count**.
6. Select the number of days (age) or count of records for each database item checked.
 - a) Age range is 10-3650 days.
 - b) Record count range is 10,000-100,000,000 records
7. Select the **Archiving/Pruning Interval** and **Record Retention Delay** period.
 - a) The **Archiving/Pruning Interval** is the number of days between checks to see if any records meet the pruning criteria.
 1. The range is 1 – 365 days.
 - b) The **Record Retention Delay** is the number of days after a record is marked for deletion that it actually gets deleted.
 1. Zero means the records are deleted immediately or immediately after being archived.
 2. The range is 0 – 364.
 3. The **Record Retention Delay** can never be larger than the **Archive/Pruning Interval**.
8. If you wish to Archive the pruned items, check the Archive to file check box and select a location to save the archived files.

Notes:

- See the CMS help file for more details.
- This job will now run on a recurring basis.
 - The job will check based on the Archiving/Pruning Interval to see if any records meet the pruning criteria that you set.
- See section11 to save the archive file on a network share drive.

12.2 Backup database

GTT recommends that you back up your SQL Server database on a regular schedule, and periodically test your backups. Information on database backup can be found in Microsoft SQL Server Books Online.

The location of the database file varies depending on the version of SQL that you are using as well as the operating system that you are using.

An example of the location on Windows 7 with SQL 2005:

- C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data

The database files are called:

- OpticomManagement.mdf
- OpticomManagement_log.ldf

13 Technical Support

GTT Technical Service in the U.S. can be reached at 1-800-258-4610. Select Option 3, then Option 1.

Worldwide Technical Service (outside the U.S and Canada) can be reached at +1 651-789-7333.

Please provide the following information when reporting issues to GTT:

- A full description of the symptoms and actions that led to them.
- Any relevant screen shots.
- The version of CMS that you are running
- Opticom central management software code site log (section 13.2)
 - The log files have names such as log_01.csl. Log files should be captured as soon as possible to reduce the probability of pertinent events being overwritten.
- Installation log file (section 13.1)
- GTT might ask for additional information if necessary to diagnose the issue.

13.1 Installation log

A log file is created during installation that might provide information to diagnose any installation issues. Send this file if requested. This log named **OpticomCMSInstallation.log** is located at:

C:\ProgramData\GTT\Opticom™ Central Management Software x.x Installation\x.x.x

- x.x is the version number

13.2 Code Site Logs

The CMS software maintains logs files that may be used for helping debug the software installation and operation. The logs are created by a software application/service called Code Site. This service and the related applications are automatically installed during the CMS installation.

The log files created by Code Site are stored at:

- Windows XP, Windows Server 2003:
 - C:\Documents and Settings\All Users\Application Data\GTT\ Opticom Central Management Software*CurrentVersion*
- Windows 7, Windows Server 2008:
 - C:\ProgramData\GTT\ Opticom Central Management Software*CurrentVersion*

The files are named Log_#.csl. See Figure 13-1.

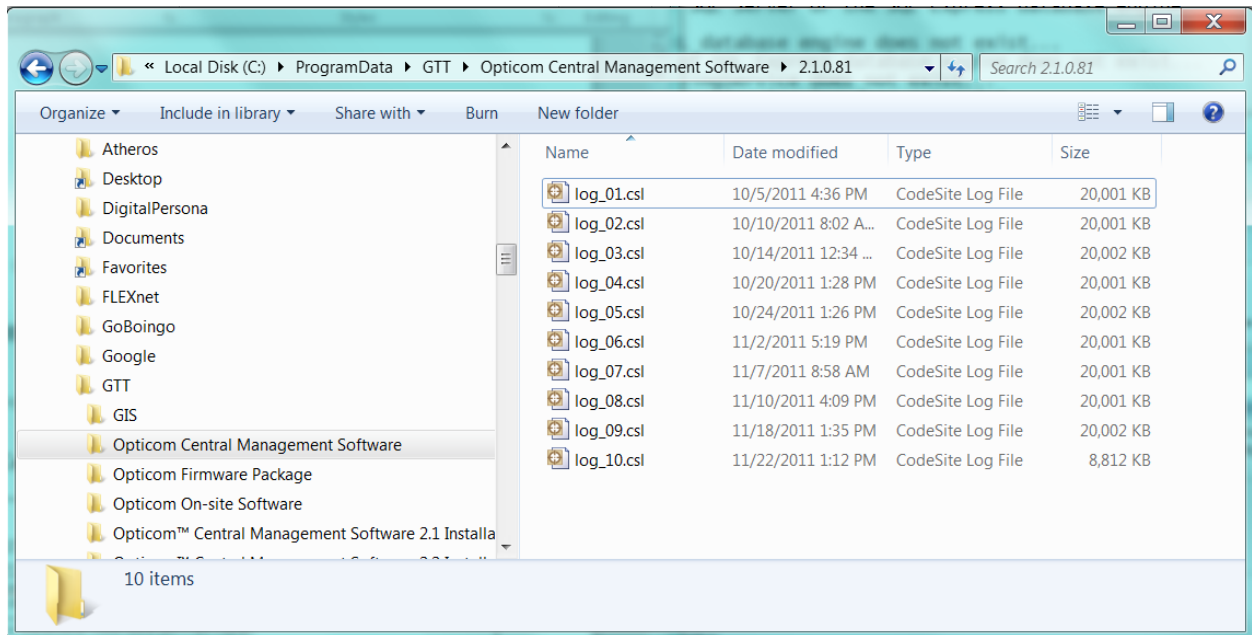


Figure 13-1

Double click on a log file to open it.

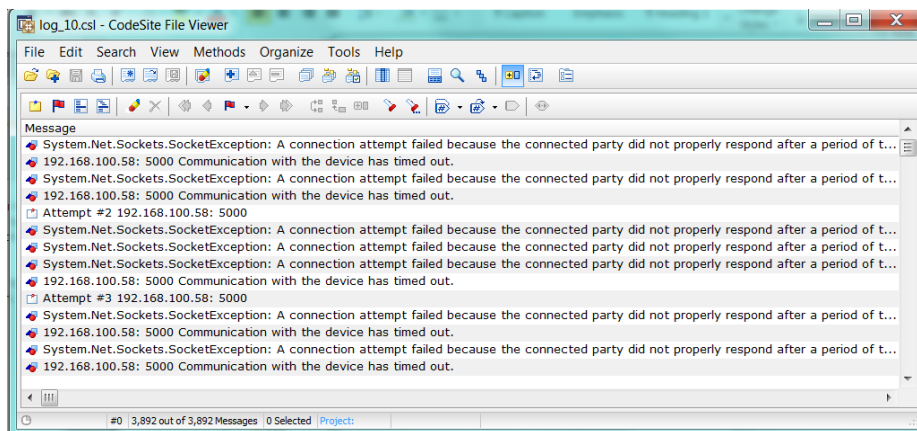


Figure 13-2

13.3 Setting Code Site Verbosity Level

The type and amount of data that is written to the logs may be set by changing the verbosity level in the client.config file on both the client and server machines. In the Client.config file can be found at:

- Windows XP, Windows Server 2003:
 - C:\Documents and Settings\All Users\Application Data\GTT\ Opticom Central Management Software\ Configs\client.config
- Windows 7, Windows Server 2008:
 - C:\ProgramData\GTT\ Opticom Central Management Software\ Configs\client.config

Notes:

- **Do not change this setting unless instructed by GTT technical support.**
 - **It is only recommended to increase the verbosity during testing or debug operations; the functioning of the logs can slow the system for other operations.**
1. Open the Client.config file
 2. Find the AppSettings section.
 3. Go to the line "addkey="verbosityLevel" value ="0"
 4. Change the value from 0 to a number from 0 to 3.
 - a) 0 shows the least logs and 3 shows the most).
 5. Restart the Communications service to have the changes take effect. See section 3.3.1.

```
<appSettings>
  <!--Its.Common.Data //-->
  <add key="ConnectionString" value="Data Source=406

  <!--Its.Diagnostics settings-->
  <!--OVERALL ENABLE, specific categories and destin.
  <add key="profilingEnabled" value="true" />
  <!--VERBOSITY LEVEL. 0 is least verbose-->
  <add key="verbosityLevel" value="0" />
  <add key="profilerImplementationFactoryAssemblyName" v.
  <add key="profilerImplementationFactoryTypeName" v.
```

Figure 13-3

14 Overview of Communications Infrastructure

Opticom central management software supports TCP/IP and redirected serial.

- **TCP/IP is the recommended method of communication**
- **Model 762 and 764 phase selectors have built-in Ethernet ports and may be addressed with TCP/IP.**
- **Model 1000 and 750 series may be addressed with TCP/IP if they are connected to a device such as a Serial to Ethernet converter. Contact GTT technical for information on these devices.**

14.1 TCP/IP

TCP/IP is used when the communication device at the remote site is directly IP-addressable. When TCP/IP is used, the communication device in the software is configured with the communication device's IP Address and Port (192.168.100.63 and 2101 in Figure 14-1). Note that in this context, *port* refers to the socket port on which the communication device is listening for TCP connections.

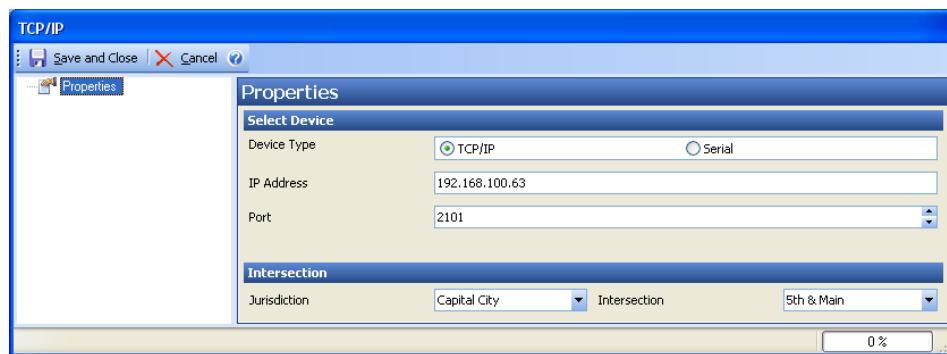


Figure 14-1

14.2 Redirected Serial

Redirected Serial is used when the communication device at the remote site is not directly IP-addressable. In this scenario, serial redirection software is installed on the server and a virtual serial port is configured to map to the communication device. When redirected serial is used, the communication device in the software is configured with the number of the virtual serial port (COM157 in Figure 14-2).

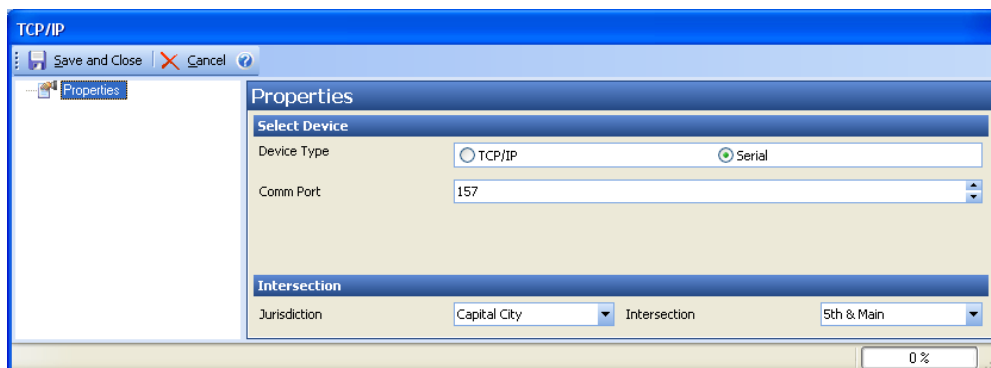


Figure 14-2

Between the central site and the intersection, and across the communications backbone, there may be any number of intermediate devices and types of physical media deployed.

At the intersection, a communication device is connected directly to the phase selector. The communication device must be capable of communication with the phase selector using serial protocol. The communication device is attached to the phase selector using a cable appropriate for the specific phase selector model used.

The networking configuration of the communication device must match that of the Opticom central management software. For TCP/IP, this is the IP address and port. For redirected serial, the configuration must match that of the serial redirection software.

The serial port configuration of the communication device must be set to match that required by Opticom phase selectors.

15 Troubleshooting and Errors Messages

This section includes information on error messages and troubleshooting.

In this section the term **COM device or communication device** refers to a third party serial to Ethernet converter used to connect the Model 750 series or Model 1000 phase selector to your communication network.

15.1 Error Screens

The following are possible error messages. Some of these errors may also appear in the Recent Event tab of the Monitoring screen, the lower half of the Scheduling screen and in the Event log report.

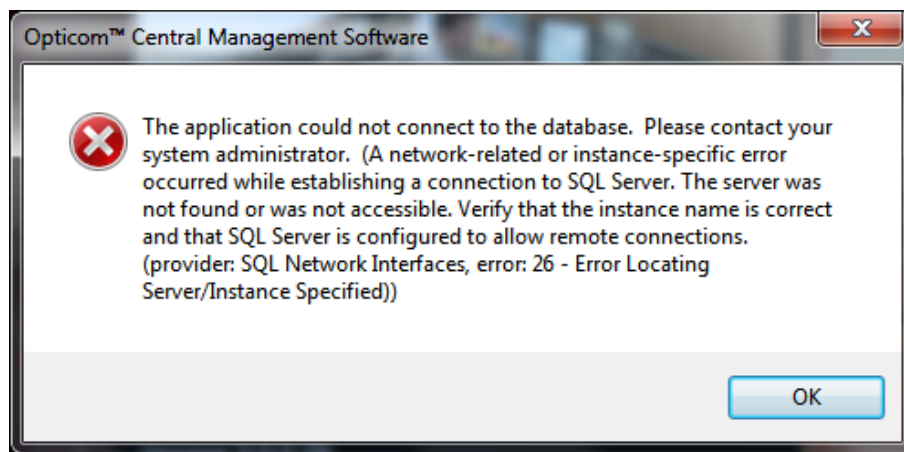


Figure 15-1

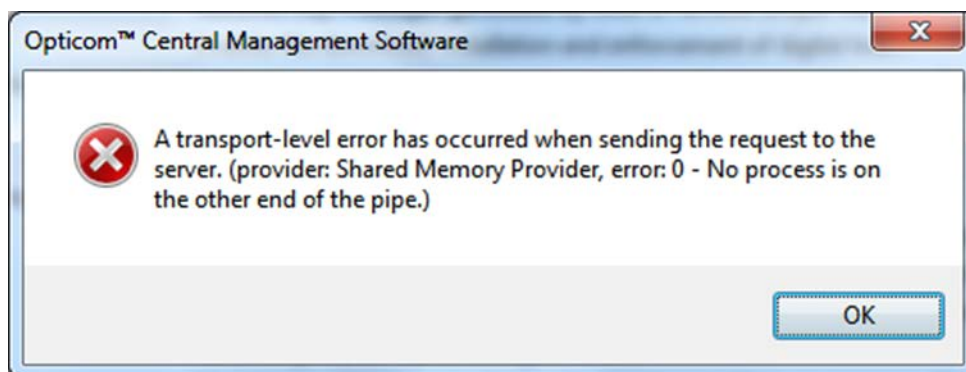


Figure 15-2

The errors in figures 15-1 or 15-2 occur when CMS (usually the client) cannot connect to the SQL database on the server.

To resolve verify the following:

- Server machine is running.
- SQL is configured to allowed remote access. See section 3.5.
- SQL is running on the server

- The firewall setting on the client machine allows access to the network. See section 3.4
- The firewall setting on the server machine allows access to the network. See section 3.4
- Port 8081 is opened See section 3.4.
- A firewall setting on the server machine is not blocking access to CMS.
- The CMS version on the server machine matches the CMS version on the client.
- Client machine is pointing to the correct SQL instance name. See section 4.
 - The case of the instance name is important i.e. SqlExpress rather than SQLEXPRESS will cause the error.
 - You can modify the SQL instance name on the client machine by opening the client.config file located at C:\ProgramData\GTT\Opticom Central Management Software\Configs. Look for the instance name and correct it.
 - i.e.... "ConnectionString" value="Data Source=**41585-CMSSERVER\SQLEXPRESS...**
 - Reinstalling CMS on the client and then pointing to the correct instance is another way of fixing an incorrect name.
- Rebooting the server machine may also resolve this issue.

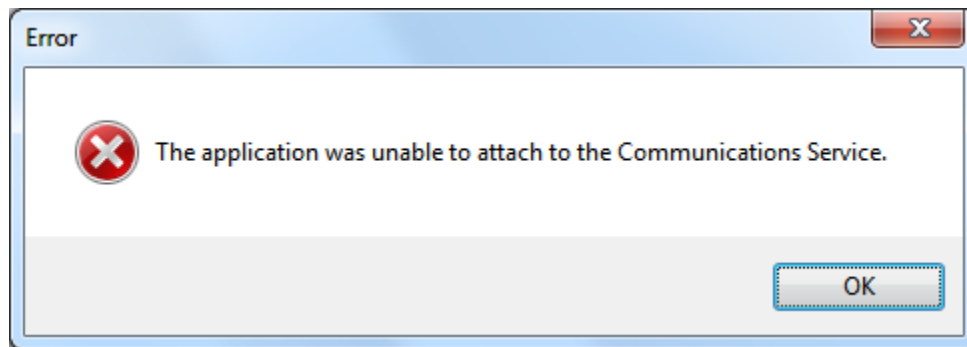


Figure 15-3

The error in figure 15-3 will occur if the communications service on the server is not running.

- Go to services on the server machine and restart the communication service.
 - See section 10.2 for more details
- Verify that Port 8081 is opened See section 3.4
- Rebooting the server machine should also restart the communication service.

You may also see this on the client machine.

To resolve verify the following:

- The firewall setting on the client machine allows access to the network.
- The firewall setting on the server machine allows access to the network.
- Port 8081 is opened.

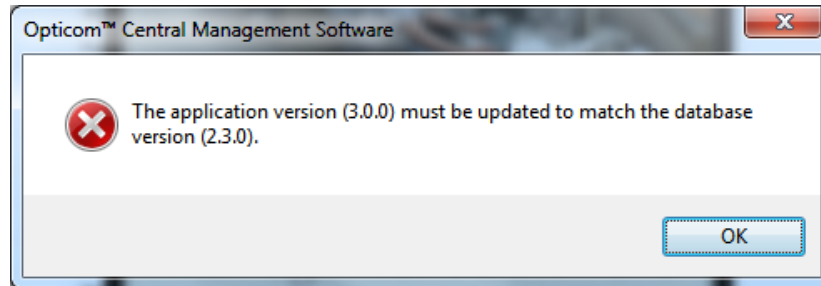


Figure 15-4

The error in figure 15-4 occurs if the central management software version running on the client machine does not match the version running on the server machine

- Update the CMS version on the client to match the version on the server.

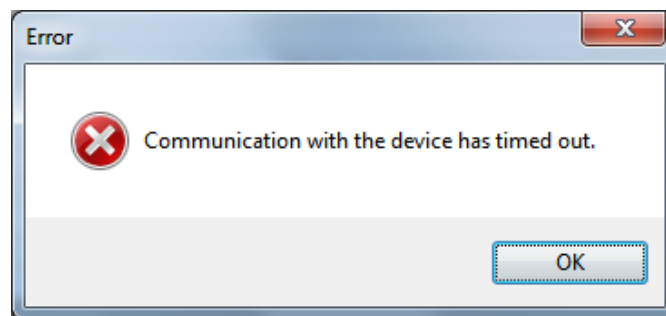


Figure 15-5

The error in figure 15-5 indicates that CMS is not able to communicate with the specified phase selector or COM device.

- There are a number of possible causes of this:
 - Network issues
 - Switch/hub issue in the traffic cabinet.
 - An issue with the Cable connecting the phase selector of COM device to the switch/hub.
 - An issue with phase selector or COM device.
 - Verify that the COM device has been configured properly.
 - High network traffic

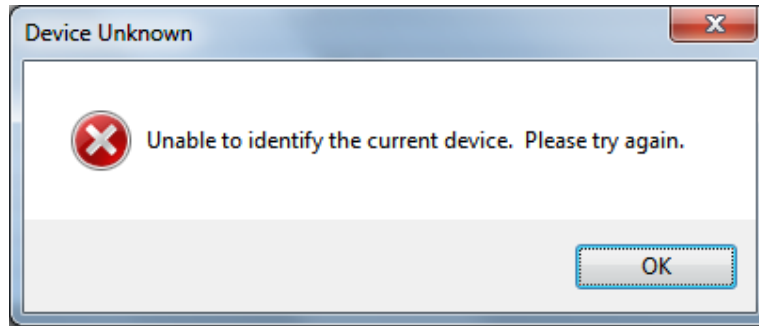


Figure 15-6

The error in figure 15-6 indicates that CMS is not able to identify the device likely because it can not communicate with it. The error screen typically appears after the error screen in figure 15-5. Resolving the communication issue will likely resolve this error as well.

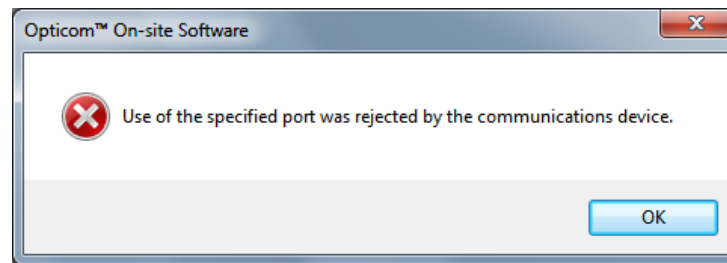


Figure 15-7

The error in figure 15-7 indicates that a device was found at the provided IP Address, but a connection cannot be established over the specified port.

- Verify that the port number programmed into the phase selector or COM device matches the port number programmed into CMS.
- Verify that another application such as On-site is not using the communication device.
 - Shut down On-site
- Verify that the port number specified in CMS is the correct port for the communication device. (Serial to Ethernet converters).
- Verify that the COM device has been configured properly.

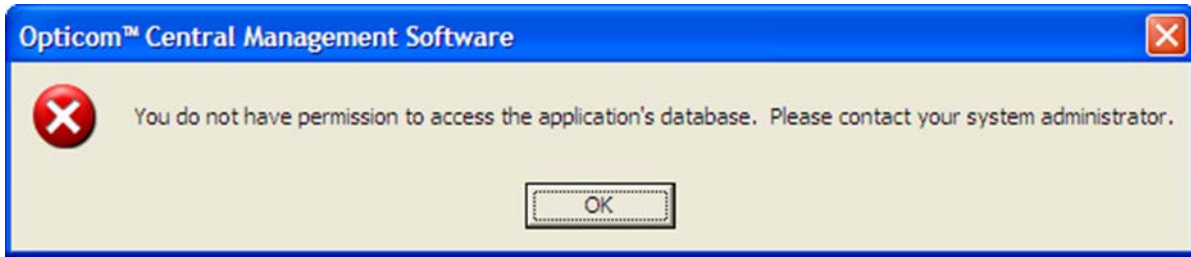


Figure 15-6

The error in figure 15-6 will appear if the user has not been entered into the OpticomUsers Windows group on the server machine. See section 3.6 for details.



Figure 15-7

The error in figure 15-7 will appear if the user has not been registered in to the Central Management System via the Role Management Tab. See section 5.5 for details.

15.2 Errors and Warnings

The following is a description of the Errors and Warnings that may appear in the Recent Event tab of the Monitoring screen, the lower half of the Scheduling screen and in the Event log report.

These errors may also appear in a pop-up error box.

Message	Meaning	Resolution
The devices communication channel is currently in use	The communication device is currently in use by another central management software user or job. Another application such as On-site is communicating with the Opticom device.	Wait until the other user or job is finished. If the problem persists, restart the GTT Communications Service. Shut down On-site.
Connecting to the communication device has timed out. Communication with the device has timed out. Communication with the phase selector has timed out.	CMS is not able to communicate with the specified phase selector or COM device.	May be a network issue or an issue with the phase selector/ COM device, switch/hub and or cable in the traffic cabinet. Verify that the COM device has been configured properly.
The device is not accessible (A socket operation was attempted to an unreachable host x.x.x)	CMS is not able to communicate with the specified phase selector or COM device.	May be a network issue or an issue with the phase selector/ COM device, switch/hub and or cable in the traffic cabinet.
No response was received from the device	Another application could be using the communication device.	Stop the other application.
Device is off line	The device is in CMS as an offline device	Connect device to CMS or deselect that device when sending jobs
There was an error generating the XML document	The configuration file in the 760 series phase selector has been corrupted.	Upgrade firmware to v4.xx or later and reprogram phase selector as needed

Unable to update firmware. Requested service not found	The communication service was not found or was not running.	Verify that the communication service is running.
Unable to update firmware. The device did not transition to the expected operating mode. Cycle device power and retry firmware update.	Connection issues	Cycle device power and retry firmware update. Use reboot command to reboot the device (762/4 only) Contact GTT technical support if the issue continues.
The connection to the device must be established	COM Connection issues	See above solutions for COM issues
Requested service not found	The communication service was not found or was not running.	Verify that the communication service is running.
Faulty or missing detector on channel (s) X, X: xbound (high noise level) X: xbound (low noise level)	CMS has detected a detector whose noise level is outside of the normal range	Open that phase selector current activity screen and verify noise level (s/b approx. 10-35). Replace any detectors that fall outside of normal range. Turn off Analyze Infrared detectors in GPS applications. Mark channels as not is use to prevent CMS from flagging non-existent detectors.
The current devices' serial number does not match the serial number for the device in the database. If the previous phase selector has been replaced, use phase selector manual operation to either provision it from the database or read the configuration from the new device.	Phase selector has been replaced.	Follow directions in the message as needed.
Different serial number detected on the device	Device has been replaced.	Press read from device to update database

Configuration changed	Notification that the configuration has changed	Look at revisions to see what has changed , See the CMS help file for details
The phase selector is busy and unable to process the request	The phase selector is processing a preemption/priority request.	Try again when preemption/priority request is finished.
Failure sending mail	Scheduled mail was not sent	Verify mail server settings. Verify that CMS has access to mail server. E-mail is too large. Select a shorter range of dates to make report smaller.
Email settings have not yet been configured under Tools-Options	E-mail not configured	Setup email under Tools/Options/Email Settings
Operational Status, Radio Module Offline, GPS Receiver Offline, GPS receiver data invalid	The phase selector is not seeing the radio/GPS unit.	If issue persists dispatch service technician.
Operational Status, GPS receiver data invalid	The phase selector is not receiving valid GPS data from the radio/GPS unit or GPS lock has been lost.	If issue persists dispatch service technician.
Unable to find Device Followed by another more specific message	Usually on a Phase selector discovery job	Verify that your IP address is correct. Follow the additional information.
A call to SSPI failed, see inner exception	SSPI(Security Support Provider Interface) is an issue with TCP connection to remote server or the security certificate of the network blocking CMS	Contact your network administrator

The device is not accessible, (An established connection was aborted by the software in your host machine 10.xx.xx.xxx:5000 (IP address and port number)	A issue with the serial to Ethernet converter	Verify configuration of the serial to Ethernet converter
The execution of the command requires a password but no password has been provided or The password is not correct	A password has been configured in the phase selector, but not in central management software. <u>750 series only</u>	Configure the phase selector's password in central management software.
Access to the path '\\gtt.com\dfs\Users\john.smith\Desktop\Agency Usage Report [6-6-2012 at 2-17 PM].pdf' is denied.	Software does not have access to the specific drive.	Save document to a different drive that CMS has access. Reconfigure the scheduling service to run under an account that has access to the drive.

Table 15-1

15.3 Summary of Communication Flow

Understanding the flow of communications messages through the system will help you diagnose and correct communication issues:

1. The Central Management Software (CMS) issues a communication request to the GTT Communications Service.
2. GTT Communications Service checks whether the communication device is already in use by another CMS user, job or another application.
3. GTT Communications Service connects to the communication device.
4. GTT Communications Service sends a request to the communication device.
5. Communication device forwards the request to the Opticom device.
6. The Opticom device processes the request.
7. The Opticom device returns a response to the communication device.
8. The communication device forwards the response to the GTT Communications Service.
9. GTT Communications Service forwards the response to CMS.
10. Steps 4 through 9 are repeated until CMS requires no further communication with the Opticom device.
11. GTT Communications Service disconnects from the communication device.

15.4 Communication Troubleshooting

Use the messages displayed by central management software as a first step in isolating where the communication issue lies:

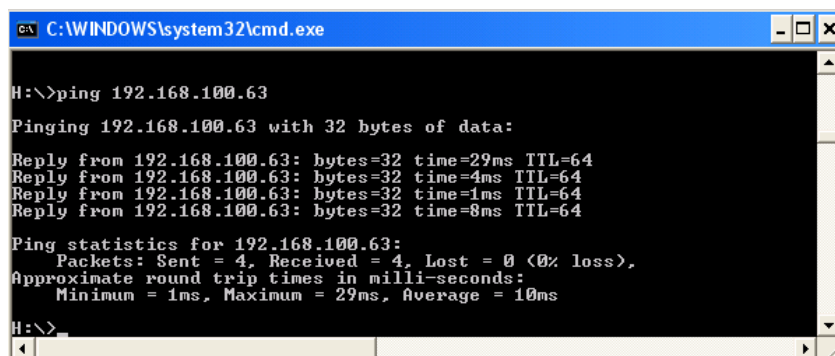
15.4.1 General Guidelines in Diagnosing Communication Issues

1. For new installations, problems are probably power, connections or configuration. Failed equipment is less likely if new equipment is being used, but should not be ruled out.
2. If communication previously worked, but now fails, problems are most likely to be failed equipment or power issues. However, it's also possible that configuration settings were inadvertently reset or connections have become unreliable.
3. Firewalls on the CMS server or between the server and the traffic control network can block communications traffic. During installation and subsequent troubleshooting, verify that any installed firewall (software and or hardware) allows access to the communication device IP addresses and ports. Depending on the type of firewall in use, you may need to add each IP address to the allowed list of the firewall. Shutting off the firewall to see if the communication issues are resolved may also point to the firewall as the issue. Some firewall software may not be easily shutdown; it may need to be prevented from starting on system restart.

15.4.2 Diagnosing TCP/IP Addressability Issues

In this section the term **COM device or communication device** refers to a third party serial to Ethernet converter used to connect the Model 750 series or Model 1000 phase selector to your communication network.

1. Can the device be reached from the server?
 - Start a command line window.
 - Type "ping xxx.xxx.xxx.xxx" where xxx.xxx.xxx.xxx is the IP Address of the Opticom device or the serial to Ethernet converter that is connected to the Opticom device.
 - This output indicates that the device can be addressed:



```
C:\WINDOWS\system32\cmd.exe

H:\>ping 192.168.100.63

Pinging 192.168.100.63 with 32 bytes of data:

Reply from 192.168.100.63: bytes=32 time=29ms TTL=64
Reply from 192.168.100.63: bytes=32 time=4ms TTL=64
Reply from 192.168.100.63: bytes=32 time=1ms TTL=64
Reply from 192.168.100.63: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.100.63:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 29ms, Average = 10ms

H:\>
```

Figure 15-8

- This output indicates that the communication device cannot be addressed with ping's default timeout. You can try pinging with a higher timeout value (type "ping" to see the options). If you find that your communication device can be seen only with larger timeout values, you may need to extend the timeout in the Opticom central management software; contact GTT technical support for assistance.

```

C:\WINDOWS\system32\cmd.exe
H:\>ping 92.168.100.63
Pinging 92.168.100.63 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 92.168.100.63:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
H:\>

```

Figure 15-9

- If the device is still unreachable after increasing the timeout, suspect a network issue.
- If the intersection checks out, then the issue lies in the networking equipment between the server and the communication device.
 1. Is the communication device listening port set correctly? If the communication device can be pinged, next verify that the port settings are properly configured.
 - Check that the Port number configured in Opticom central management software matches that in the communication device. Consult the installation and configuration instructions for your communication device for more information.
 2. Verify that the IP address has not been assigned to multiple devices.
 3. Many communication devices use internal web pages and may be reached by typing the IP address of the device into the address line of a web browser. If communication is successful the device's web page will appear and many device settings can be edited. If it is not successful an error message will appear.

15.4.3 Diagnosing the Model 750 series and Model 1000 at the Intersection

In this section the term **COM device or communication device** refers to a third party serial to Ethernet converter used to connect the Model 750 series or Model 1000 phase selector to your communication network. See section 15.4.5 for diagnosing issues with Model 760 series phase selectors.

1. Verify and resolve any cable connections issues:
 - Between the communication device and the upstream box/switch
 - Between the upstream box and the network

2. Verify that power is supplied and the device is switched on.
3. Verify that the settings on the COM device are correct, refer to the manufacturers documentation for details
4. For communication devices that have hardware switches on them to activate serial ports, verify the correct settings are in place.
5. Check Ethernet status LEDs (if supplied) to determine if Ethernet connection is live. Link activity should be indicated. Good link LED should be solid. If LEDs don't light up, suspect the communication device.
6. If link activity is not shown or the good link LED is not on, connect a laptop to the Ethernet side of the communication device using a cross connect Ethernet cable. This will take the communication device off the network and the laptop becomes the network. The laptop must have static IP configured in order to talk to the communication device. While connected through the laptop:
 - a) If LEDs light up when connected to the laptop, suspect a network problem.
 - b) If LEDs are lit, ping the communication device's IP address directly from the laptop (see "Diagnosing TCP/IP Addressability Issues" for instructions).
 - c) If the ping fails, suspect the configuration setup. Try to ping the device at its factory default address.
 - d) Try a hardware reset of the communication device. Most communication devices have a reset button that you depress and hold for 10 seconds while the device is power cycled. This will bring the device back to a factory default address (typically 192.168.0.1.) Re-ping the communication device. If the ping fails, suspect the communication device.
 - e) If you can ping the communication device, and it supports an internal web server for configuration and maintenance, access its home page by opening a browser and entering the IP address into the link bar. Verify settings and make corrections as needed and save.
 - f) If you're using redirected serial and have configured a virtual serial port on the laptop, try connecting to the serial port using ITS Link or ITS Explorer from the laptop.
 - g) If a duplicate IP address is suspected, then disconnect the laptop from the communications device and connect it to the communications network using a standard Ethernet cable, not the cross connected cable. Verify that the connection is good (Link good and activity LEDs are lit). Ping the IP address. If a response is received, then there is a duplicate address somewhere in the network. Resolve the IP conflict and reconnect the communications device.
 - h) Lastly, a quick test to verify the network is to connect the laptop directly to the network and attempt to ping a known IP address somewhere else on the network or perhaps the communications server if the address is known. Verify that the connection is good by observing the link good and link activity LEDs. A ping failure indicates a network problem.
7. Retry communications from the central location. If the communication device is still not reachable, suspect a network problem.

15.4.4 Diagnosing phase selector timeout issues

In this section the term **COM device or communication device** refers to a third party serial to Ethernet converter used to connect the Model 750 series or Model 1000 phase selector to your communication network.

Phase selector timeouts will be seen if there's a problem getting the request from the communication device to the phase selector, or the phase selector does not return a response, or the communication device does not return the response to the server.

From the central site:

1. If this issue is seen when discovering a device:
 - a. Check that the proper baud rate is selected (9600 for Model 750 Opticom infrared phase selectors and 115,200 for Model 1000 Opticom GPS phase selectors)
 - b. Check that the "Discover Opticom GPS M1000 phase selectors" option on the Add Phase Selectors form is properly set. This option should be checked if discovering Model 1000 phase selectors and not checked when discovering Model 750 or 760 phase selectors.
2. If the communication device has remote maintenance access (e.g., through an embedded web server), verify that the communication device's serial port settings match that required for the phase selector. See "Overview of Communications Infrastructure" above.

At the intersection:

1. Verify and resolve any cable connections issues:
 - a. Between phase selector and communication device
 - b. If the serial port on the communication device type is DTE (female), verify that a null modem is installed between the communication device and the serial cable
2. Verify that power is supplied and the phase selector is switched on.
3. If this issue started after replacing a phase selector at the intersection:
 - a. Check that phase selector has not been replaced with one in a different family (i.e. M1000 for M750 or vice versa).
 - b. Check that the new phase selector uses the default baud rate on the serial port used by central management software (9600 for M750 and 115,200 for M1000).
 - c. If using device addressing, check that the new phase selector has the same device address as the previous phase selector. Note that provisioning through central management software when using device addressing requires that the new phase selector be preconfigured in the field with the same device address as the previous card.
4. Connect the phase selector to the serial port of a PC using the cable in the cabinet, and verify communications using ITS Link or On-site. If unable to communicate, suspect the phase selector or cable.

If you were unable to verify the communication device's serial port settings remotely, check these directly at the communication device.

15.4.5 Diagnosing the Model 760 series at the Intersection

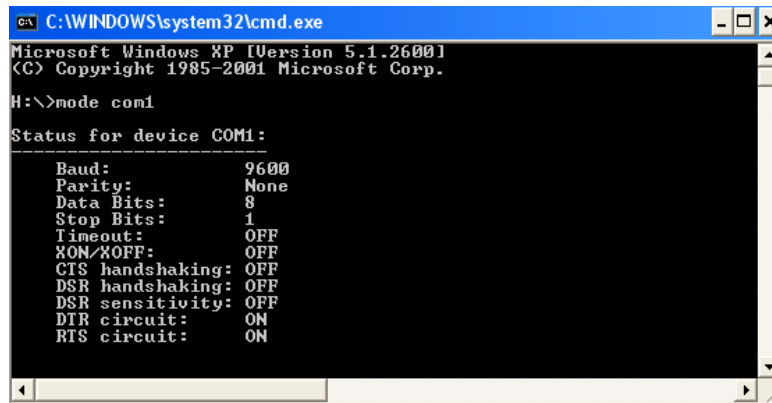
1. Verify and resolve any cable connections issues:
 - a. Between the Model 760 and the upstream box/switch
 - b. Between the upstream box and the network
2. Verify that power is supplied and the model 760 status light is on.
3. Check Ethernet status LEDs on the Model 760 and the upstream switch/box to determine if Ethernet connection is live. Link activity should be indicated. Good link LED should be solid. If LEDs don't light up, suspect the communication device. See table 15-2 for Model 760 Ethernet indicator meaning.
4. If link activity is not shown or the good link LED is not on, connect a laptop to the Ethernet port of the Model 760 using a cross connect Ethernet cable. This will take the Model 760 off the network and the laptop becomes the network. The laptop must have static IP configured in order to talk to the Model 760. While connected through the laptop:
 - a. If LEDs light up when connected to the laptop, suspect a network problem.
 - b. If LEDs are lit, ping the IP address of the Model 760 directly from the laptop
 - c. If the ping fails, suspect the configuration setup. Connect to the Model 760 with On-site through the serial port and verify Network settings are as expected.
 - d. Ping the IP address of the hub/switch that the Model 760 is connected to.
 - e. Try a hardware reset of the hub/switch that the Model 760 is connected to. Most of these devices have a reset button that you depress and hold for 10 seconds while the device is power cycled. This will bring the device back to a factory default address (typically 192.168.0.1.) Re-ping the hub/switch. If the ping fails, suspect the hub/switch.
 - f. If you can ping the hub/switch, and it supports an internal web server for configuration and maintenance, access its home page by opening a browser and entering the IP address into the link bar. Verify settings and make corrections as needed and save.
 - g. If a duplicate IP address is suspected, connect the laptop to the communications network using a standard Ethernet cable, not the cross connected cable. Verify that the connection is good (Link good and activity LEDs are lit). Ping the IP address. If a response is received, then there is a duplicate address somewhere in the network. Resolve the IP conflict and reconnect the communications device.
 - h. Lastly, a quick test to verify the network is to connect the laptop directly to the network and attempt to ping a known IP address somewhere else on the network or perhaps the communications server if the address is known. Verify that the connection is good by observing the link good and link activity LEDs. A ping failure indicates a network problem.
5. Retry communications from the central location. If the communication device is still not reachable, suspect a network problem.
- 6.

Indicator	Off	Solid	Flashing
Yellow	No Ethernet connection	Ethernet port connected	Active communication
Green	Speed set to 10Mb/s	Speed set to 100Mb/s	n/a

Table 15-2 Model 762 and 764 Ethernet port indicator meaning

15.4.6 Diagnosing Redirected Serial Issues

1. Is the redirected serial port visible to the operating system and available? If the serial port is not visible and available, then the GTT Communications Service will not be able to access it. Check as follows:
 - Start a command line window.
 - Type “mode comx” where x is the redirected serial COM port number.
 - Figure 15-10 indicates that the serial port is visible and available. Continue to the next step.



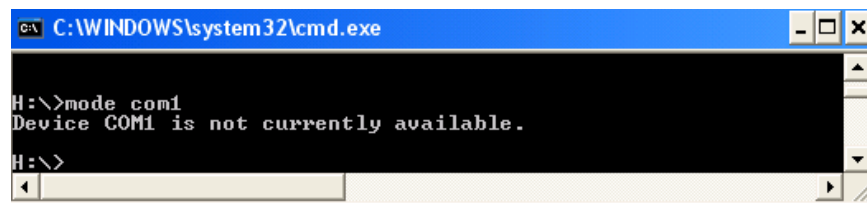
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>mode com1

Status for device COM1:
-----
Baud:          9600
Parity:        None
Data Bits:     8
Stop Bits:    1
Timeout:      OFF
XON/XOFF:     OFF
CTS handshaking: OFF
DSR handshaking: OFF
DSR sensitivity: OFF
DTR circuit:  ON
RTS circuit:  ON
```

Figure 15-10

- Figure 15-11 indicates that the COM port is visible, but in use by another application. Stop the other application and retry.



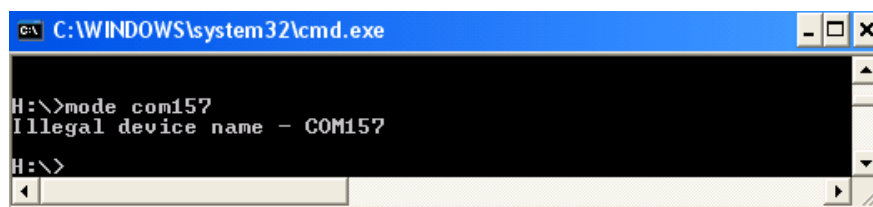
```
C:\WINDOWS\system32\cmd.exe

H:\>mode com1
Device COM1 is not currently available.

H:\>
```

Figure 15-11

- Figure 15-12 indicates that the COM port is not visible to the operating system. Consult the installation and configuration instructions for your serial redirection software.



```
C:\WINDOWS\system32\cmd.exe

H:\>mode com157
Illegal device name - COM157

H:\>
```

Figure 15-12

2. Is the virtual serial port properly configured for the communication device?

- Verify that the IP address (or MAC address) and TCP listening port match those of the communication device. Consult the installation and configuration instructions for your serial redirection software for more information.
- If the redirected serial port is visible and available, and the virtual serial port is properly configured for the communication device, see “Diagnosing TCP/IP addressability issues.”

15.5 Data Consistency Check

The data consistency check scans the database to see if there are any database errors.

To run a data consistency check select the **Data Consistency Check...** command from the **Tools** menu. Press the **Check Data** button. Contact GTT technical support if the check finds any issues. See Figure 15-13.

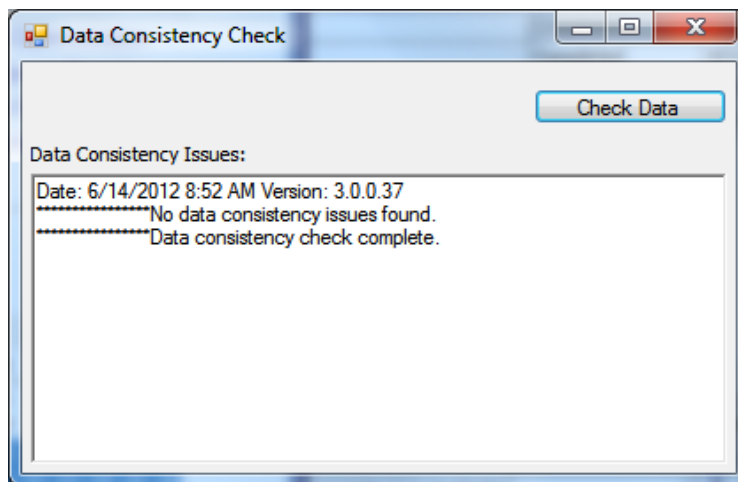


Figure 15-13

16 Quick Guides

The following quick guides are intended to be used as a pre-installation and installation guide. They may also be used as a check sheet.

16.1 Pre-Installation

The following items should be in place or available prior to installation.

Server

- ___ 1. Dedicated server machine installed and operating.
- ___ 2. Will SQL Express or full SQL be installed?
 - a. Install SQL if full version or SQL Express 2008 or newer to be used.
- ___ 3. Server machine connected to the internet and to the network so it can see all intersections.
- ___ 4. Server machine has sufficient disk space for SQL database and CMS.
- ___ 5. All phase selectors installed, configured, operating and connected to the network.
- ___ 6. Ping all phase selector IP addresses from server location to verify connectivity.
- ___ 7. Managed switches on network configured to allow only bandwidth required for all devices on the network.
- ___ 8. Have a list of all system user names in the format expected by the network
- ___ 9. Have the mail server name/address and a dedicated user name and password if anonymous users are not allowed.
- ___ 10. Mutual aid plan (if used) (What codes are vehicles using?)
 - a. Will default code and 0 code be blocked?
- ___ 11. CD or memory stick with CMS and license key
- ___ 12. CD or memory stick with map database for area. (GPS users only)
 - a. May be downloaded if server/client is connected to the internet.
- ___ 13. CD or memory stick with Opticom firmware package.
 - a. May be downloaded if server/client is connected to the internet.

Opticom Equipment Lists

- ___ 1. A complete list of all Opticom equipped vehicles with emitter IDs names, owning agencies etc.
 - a. Should be in import format.
- ___ 2. A complete list of all Opticom equipped intersections with IP addresses, port numbers, owning jurisdictions.
 - a. Should be in import format

- ___ 3. Should have green sense phase assignments. Which phase associated with which direction. (if used)
 - a. a. i.e. Northbound is phase1+6
- ___ 4. Should have channel direction assignments.
 - a. i.e. Channel A is southbound.
 - b. Should list unused channels

Server Installation

The following items must be done on the server machine.

- ___ 1. Install CMS on server machine
 - a. Select Server option
 - b. Install SQL express only if express version is to be used.
- ___ 2. If full SQL is to be used, select the SQL Instance when prompted.
- ___ 3. Verify that Port 8081 is open.
- ___ 4. Open SQL for remote access.
- ___ 5. Verify that correct date and time is set on the server.
- ___ 6. Add all system users to Opticom users group in Windows.
- ___ 7. Import the GIS map database.
- ___ 8. Install the Opticom firmware package.

Client Installation

The following must be done on each client machine. Each client must be connected to the network where the server resides.

- ___ 1. Install CMS on client machine
 - a. Select Client option
 - b. When prompted enter name of server computer/SQL Instance.
 - c. Look on bottom of the CMS user interface for the name of the server computer/SQL Instance.
- ___ 2. Import the GIS map database.
- ___ 3. Install the Opticom firmware package.

Additional Setup

The following items may be done on the server machine or one of the clients. These items only need to be done one time.

- ___ 1. Enter License key.
- ___ 2. Enter mail server information.
- ___ 3. Enter name of region
- ___ 4. Set view option to appropriate setting (i.e Opticom IR, Opticom GPS)
- ___ 5. Add each user to CMS with their permission level
 - a. Use the format specifying network i.e. network name\user name
 - b. Must be done originally by the user who was logged in(installed) the server.
- ___6. Test e-mail settings by creating and e-mailing a report.

System Setup

The following may be done from the server or a client. It should be done by a user with sufficient permission level.

- ___1. Import vehicle information into CMS.
 - a. Use import utility
 - b. Import form should allocate code ranges
- ___2. If manually adding vehicle data. First add jurisdictions and agencies
- ___3. Allocate and configure code ranges and classes.
- ___4. Manually add vehicle data
- ___5. Configure mutual aid (if used).
- ___6. Import intersection information into CMS.
 - a. Use import utility
 - b. Run a discovery job to discover and add phase selectors.
- ___7. Or manually add intersection data and IP addresses and manually discover phase selectors.
- ___8. Update code maps, turn on logging, update firmware and enter channel and green sense information.
- ___9. Turn on and configure monitoring for each phase selector.
- ___10. The system is now fully setup and ready to train user and create recurring reports and jobs.

17 Opticom Firmware Package

If you are using Model 760 series, or Model 1000 phase selectors, you will want to install the Opticom Firmware Package on your server and workstations. There is no need to install the firmware package if you are only using Model 750 series devices. But since the Model 750 series has been discontinued and any newly purchased devices will be Model 760 series it is recommend that the firmware package be installed in all CMS installations.

Firmware is software that resides on a chip inside of a device. The Opticom system has multiple pieces of firmware.

- Phase Selector Firmware which resides on a chip in the phase selector.
- Vehicle Firmware which resides on a chip in the vehicle control unit.
- Radio Firmware which resides on a chip in both the vehicle and intersection radios.
- GPS Receiver Firmware which resides on a chip on the GPS receiver in both the vehicle and intersection radio/GPS units.
- Auxiliary Interface Panel A(IP) Firmware which resides on a chip on the AIP
- All pieces of firmware are upgraded by computer. No components need to be replaced.

The following devices have upgradable firmware:

- Model 1000, 762 and 764 phase selectors.
- Model 768 Auxiliary Interface Panels (AIP).
- Model 1010 and 1012 Radio/GPS units.
 - Not upgradeable through a Model 764 phase selector
- Model 2100 and 2101 radio/GPS control units.
- Model 1020 and 1021 vehicle control units also have upgradable firmware but is only upgradable using the On-site software.

17.1 Firmware Package Installer

All of the firmware files for the Opticom system are distributed via the Firmware Package Installer. Each time a new version of any of the pieces of firmware is released, this package will be updated and a new revision of the Firmware Package Installer will be released. The release notes for the latest version will also be included so that the user can determine if a firmware upgrade is warranted in their location. When installed on your computer, this installer places all of the current versions of firmware and associated files on your computer in a specific location that this software uses when upgrading firmware.

17.2 Determining the versions available on your machine

1. Select Check for New Firmware from the Tools menu.
2. A window will appear telling you which firmware package is installed on your machine. It will also ask you if you want to check the website for a newer version.

17.3 Download the latest version

1. Go the GTT Technical support Literature and downloads page
<http://www.gtt.com/support-customer-portal>

2. Or Press the "Check for new firmware" button and you will be sent to this page after you press the "Yes" button.
3. Click on "Click here to login to Login and Access Software Downloads"
4. Login to the download page
 - o If you are not a registered user, you will need to create a user account.
 - o Click on "Register" to be directed to the register new user page.
5. Check to see if there is a later version of the firmware package installer.
6. Save the latest Firmware Package to your machine.

17.4 Installing the Firmware Package

1. Double click on the file FirmwarePackage_x_x_Setup.exe.
2. The firmware files will be placed on your computer in a location that CMS will find.
 - Windows XP: C:\Documents and Settings\All Users\Application Data\GTT\Opticom Firmware Package
 - Windows 7: C:\Program Data\GTT\Opticom Firmware Package
3. The release notes and supporting files are also placed on your machine.
4. Shortcuts to the release notes will be placed in the Windows Start Menu.
5. Old versions of the firmware and release notes will be uninstalled.
6. Proceed to update the firmware.

18 GIS Maps

If you are using Opticom GPS, then install the GIS map for your region. Skip this section if you are only using the IR version of Opticom.

With the map installed, the CMS Active Map and Approach Map Editor will display Opticom intersection and vehicle information overlaid on a street map, in addition to any other installed layers. A GIS Assistant utility is provided in the software to help you install and configure the map. This map data, which is downloaded by County, is available at no cost from the U.S. Census Bureau. Canadian users may download the map data by Province from Statistics Canada.

You may also use your own map database if it is in the .shp file format.

18.1 Delete old map data

It is recommended that you delete any older versions of the map database (if present) prior to installing the latest version otherwise CMS may use the older version.

1. Select **GIS Assistant** from the **Tools** menu.
2. Select the first file to be deleted and press the **Delete** button.
3. Press **Yes** to confirm.
4. Repeat steps 2-3 for the rest of the files.
 - a) Each county has four files, delete all four files.
 - Arealm
 - Areawater
 - Edges
 - Pointlm

18.2 Download Map Data (US):

1. The latest map data may be downloaded at: <http://www.census.gov/cgi-bin/geo/shapefiles2010/main> (This page also contains a link to an FAQ which will answer questions about data accuracy, format etc.
2. Under the Select Layer Type pull down menu; select: **Features/ All Lines** and then press the **Submit** button.
3. Select the desired **State** from the pull down list and press the **Submit** button.
4. Select the desired **County** from the pull down list and press the **Download** button.
5. Internet Explorer may try to block the download, if it does, click on the bar on the top of the screen and select download file.
6. Press **Save** on the dialog box that appears.
7. Another dialog box will appear, allowing you to select the location to save the file.
8. Select the **Location** and press **Save**.
9. Press the **Close** button when the file has finished downloading.
10. Go back to the page that you started at or press your browser back button three times.
11. Under the Select Layer Type pull down menu; select: **Features/ Landmarks** and then press the **Submit** button.
12. Under **Point Landmark**, Select the desired **State** from the pull down list and press the **Submit** button.

13. Select the desired **County** from the pull down list and press the **Download** button.
14. Internet Explorer may try to block the download, if it does click on the bar on the top of the screen and select download file.
15. Press **Save** on the dialog box that appears.
16. Another dialog box will appear, allowing you to select the location to save the file.
17. Select the **Location** and press **Save**.
18. Press the **Close** button when the file has finished downloading.
19. Press the **Back** button on your web browser three times.
20. Under the Select Layer Type pull down menu; select: **Features/ Water** and then press the Submit button.
21. Under **Area Hydrography**, Select the desired State from the pull down list and press the Submit button.
22. Select the desired **County** from the pull down list and press the **Download** button.
23. Internet Explorer may try to block the download, if it does click on the bar on the top of the screen and select download file.
24. Press **Save** on the dialog box that appears.
25. Another dialog box will appear, allowing you to select the location to save the file.
26. Select the **Location** and press **Save**.
27. You may optionally also download and import the **Area Landmarks** database.
Depending on the county additional landmarks such as parks may be displayed.
28. Proceed to Section 18.4 for details on importing the downloaded data into CMS.

18.3 Download map data (Canadian users):

1. The map data may be downloaded at:
http://geodepot.statcan.gc.ca/2006/040120011618150421032019/1814062006_05-eng.jsp
2. Under Step 1, select the most recent available **Year** and press the **Next** button.
3. Under Step 2, select the desired **Language** and press the **Next** button.
4. Under Step 3, select **ARC/INFO(.shp)** and press the **Next** button.
5. Under Step 4, select the **Province** that you are operating in and press the **License Agreement** button. GTT does not recommend using the "all of Canada" download. We recommend downloading only the province(s) that you need.
6. After reading the license use conditions press the **I Agree** button.
7. Press the **Download** button under Step 4.
8. This will bring you to a new page with a link to .zip file. Click on the **link**.
9. Press **Save** on the dialog box that appears.
10. Another dialog box will appear, allowing you to select the location to which you wish to save the file.
11. Select the **Location** and press **Save**.
12. Press complete when the file has finished downloading
13. Select **GIS Assistant** from the tools menu.
14. Proceed to Section 18.4 for details on importing the downloaded data into CMS.

18.4 Import Map Data into CMS:

1. Select **GIS Assistant** from the **Tools** menu.

2. Press the **import** button and navigate to the one of the **files** that you downloaded and saved in the previous section.
3. Press the **Open** button. After a few moments a dialog box will appear and tell you that index files are being built.
4. Repeat **steps 1-3** for all the downloaded files.
5. Close the GIS assistant.
6. Map data for your area will be displayed when you open the approach map editor or active map screen.

19 Moving an Existing CMS Database to another Machine

This section describes the procedure for moving the database to another machine. This may be done when moving CMS to a different server or if you are upgrading the SQL database from SQL Express to a full version of SQL.

19.1 Steps to perform on the existing Server Machine

1. Stop active monitoring (if being used)
2. Shut down CMS on all client user interfaces.
3. Stop the GTT Scheduling service and GTT Communication service.
 - a. From the services control panel
4. Open SQL Management Studio
 - a. Press Connect when prompted
 - b. Go to the OpticomManagement database and right click on it,
 - c. Click on Tasks menu item and then select the Detach menu item. See Figures 19-1&19- 2.
 - d. Verify that there are no active connections and Press OK and it will detach. You should no longer see the database.
5. Go to wherever the data base is saved.
 - a. The location of the database file varies depending on the version of SQL that you are using as well as the operating system that you are using.
 - b. An example of the location on Windows 7 with SQL 2005:
 - c. C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data.
 - d. To find the exact path:
 - i. Open SQL Management Studio.
 - ii. Press Connect when prompted.
 - iii. Go to the OpticomManagement database and right click on it.
 - iv. Click on the Properties menu item and the properties screen will open.
 - v. Click on Files item on left side of the properties page.
 - vi. In the Database Files section, scroll to the right until you come to the Path column and that tells you the exact location of the Opticom Management database files.
6. Put the OpticomManagement.mdf and OpticomManagement_log.ldf on a USB drive or burn to a CD so they can be copied to the new server.
 - a. You do not really need the .ldf file, but put it on USB drive for safety.
7. Uninstall CMS from the old machine

19.2 Steps to perform on the new Server Machine (Full SQL)

1. Install SQL
2. Copy the OpticomManagement.mdf to C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data.
3. Open SQL Management Studio and right click on the Databases folder.
4. Select the 'Attach' menu item and a window will open. See Figures 19-3,4,5.
 - a. Click 'Add' button in the middle of screen.
 - b. Navigate to the OpticomManagement database.
 - c. Select the OpticomManagement.mdf then click OK.

- d. Note that after it is selected it will be in the bottom half of the screen. Highlight it and then select OK at the bottom of the screen. Notice that the Opticom Management database is now in SQL.
5. Delete the OpticomUsers out of Security Users in the OpticomManagement database. See Figure 19-6.
 - a. Right click the item (example in red box in Figure 6) and select the delete menu item.
6. Install CMS Server on the new machine
7. Point to the instance of SQL to be used.
8. Proceed as usual to finish the installation on the server machine.

19.3 Steps to perform on the new Server Machine (SQL Express)

1. Install CMS server
2. Select SQL Express option and finish the installation
3. Stop the GTT Scheduling service and the GTT Communication service
4. Open SQL Management Studio
 - a. Press Connect when prompted
 - b. Go to the OpticomManagement database and right click on it,
 - c. Click on Tasks menu item and then select the Delete menu item.
 - d. Verify that there are no active connections and Press OK and it will delete.
5. Copy the OpticomManagement.mdf to the appropriate location.
 - a. See Step 5 of Section 19.1
 - b. Or go to the Services and scroll down to the SQL Server service with the specific SQL instance just installed in parenthesis and right click on it and select properties and under the General tab the instance path is under Path to executable and the path to copy the OpticomManagement database files would be under the ...MSSQL\Data because if
 - c. On a 64 bit machine it won't be in program files but program file (x86).
6. Open SQL Management Studio and right click on the Databases folder.
7. Select the 'Attach' menu item and a window will open. See Figures 19-3, 19-4 & 19-5.
 - a. Click 'Add' button in the middle of screen.
 - b. Navigate to the OpticomManagement database.
 - c. Select the OpticomManagement.mdf then click OK.
 - d. Note that after it is selected it will be in the bottom half of the screen. Highlight it and then select OK at the bottom of the screen. Notice that the Opticom Management database is now in SQL.
8. Delete the OpticomUsers out of Security Users in the OpticomManagement database. See Figure 19-6.
 - a. Right click the item (example in red box in Figure 19-6) and select the delete menu item.
9. Install CMS server again
 - a. This is necessary in order to recreate the OpticomUser group that needed to be deleted for the OpticomManagement database that needed to be deleted. It needed to be deleted since it was part of the database that was migrated and it will not work after being migrated.
10. Proceed as usual to finish the installation on the server machine.

19.4 Steps to perform on the existing Client Machine/s

1. Uninstall CMS
2. Reinstall CMS pointing it to the new location of the database (SQL instance)

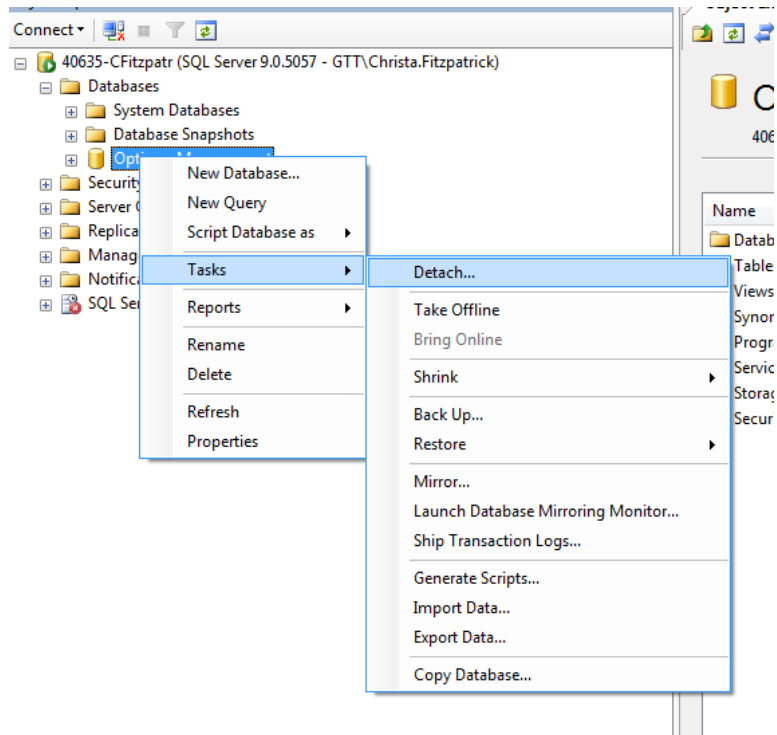


Figure 19-1

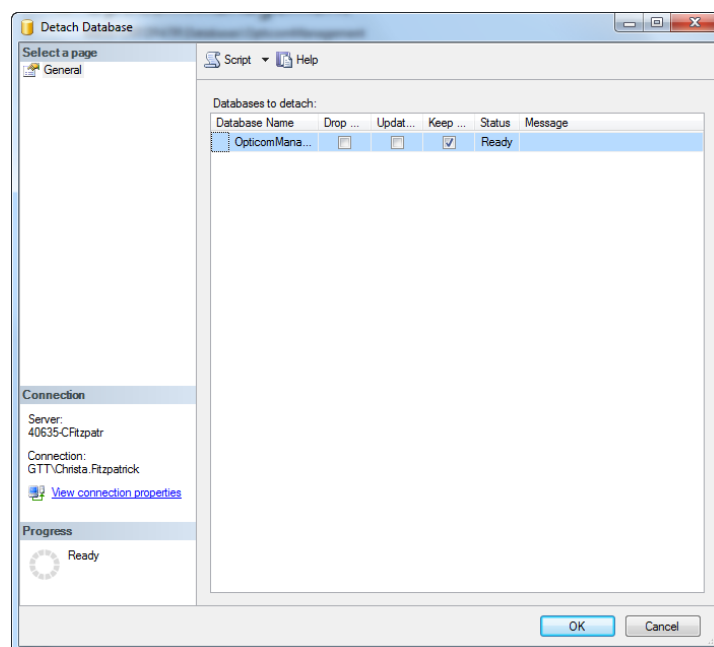


Figure 19-2

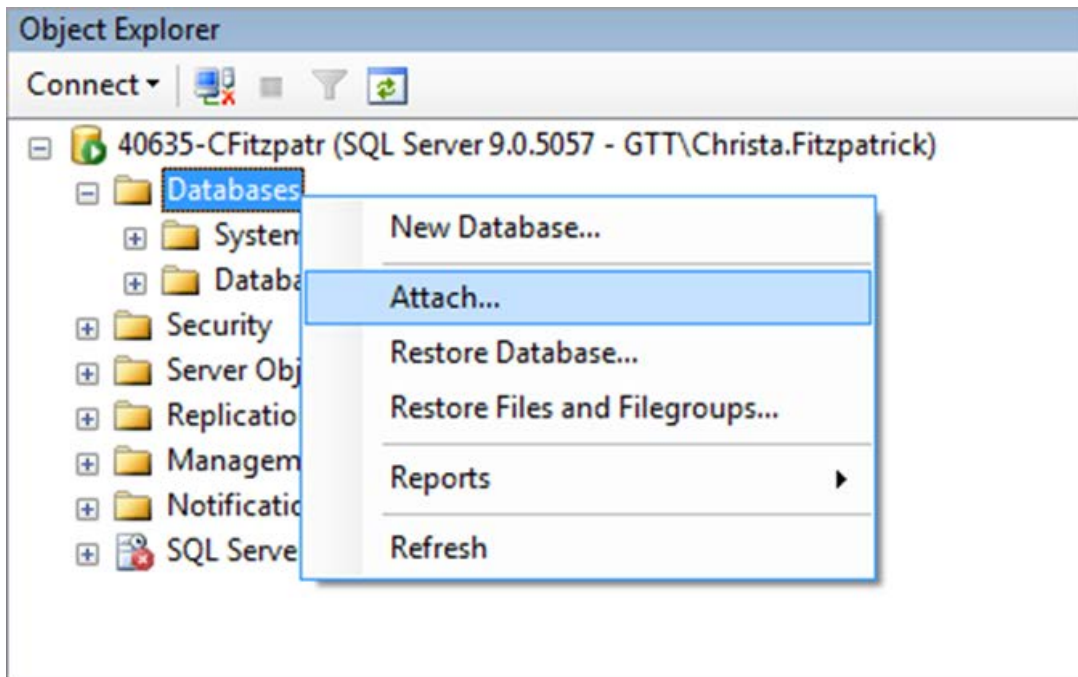


Figure 19-3

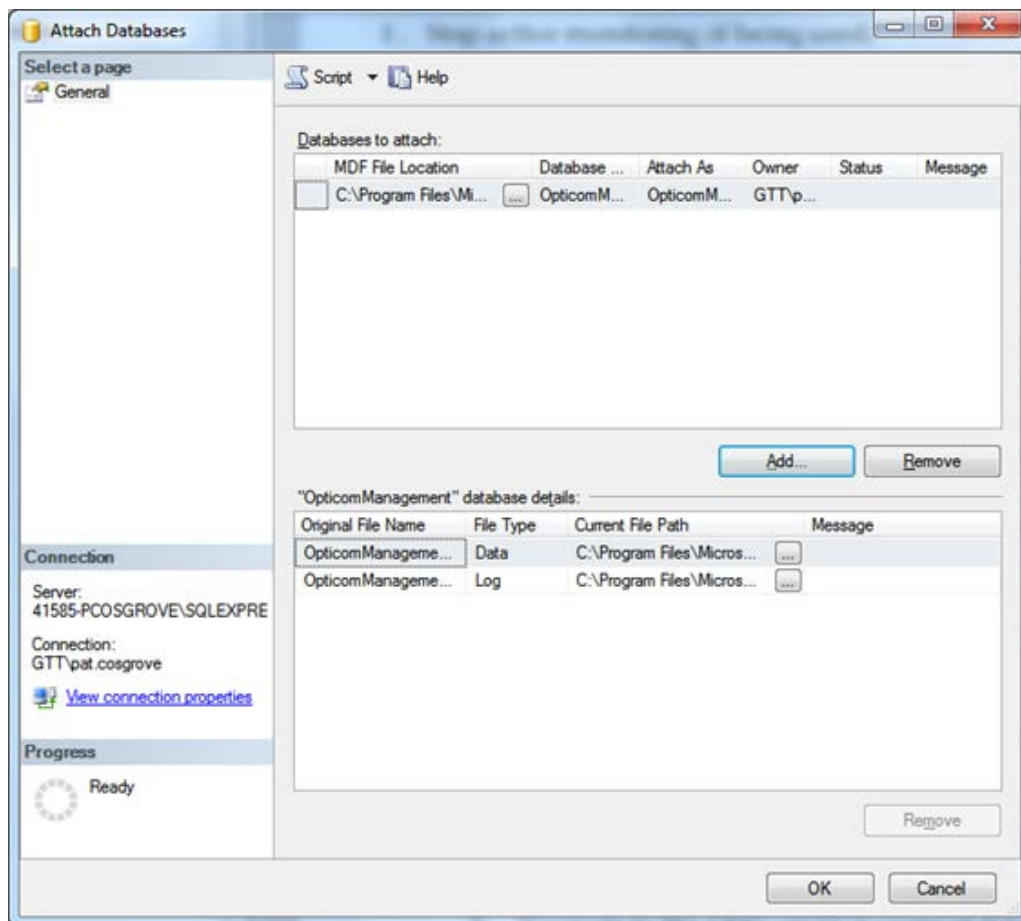


Figure 19-4

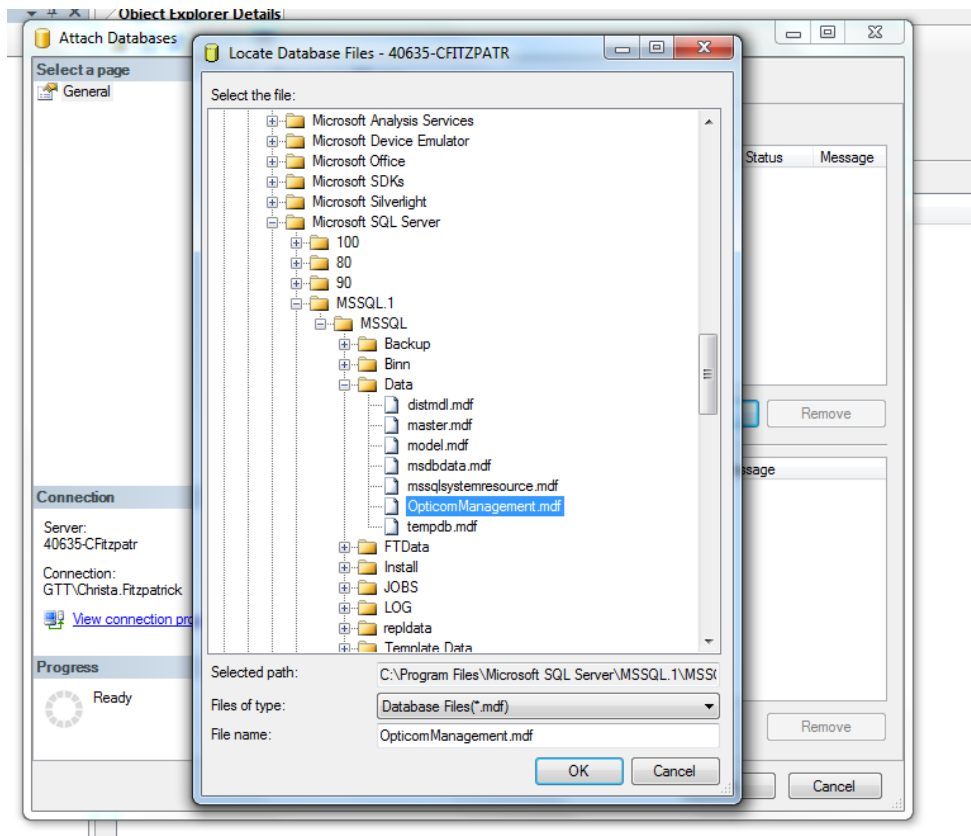


Figure 19-5

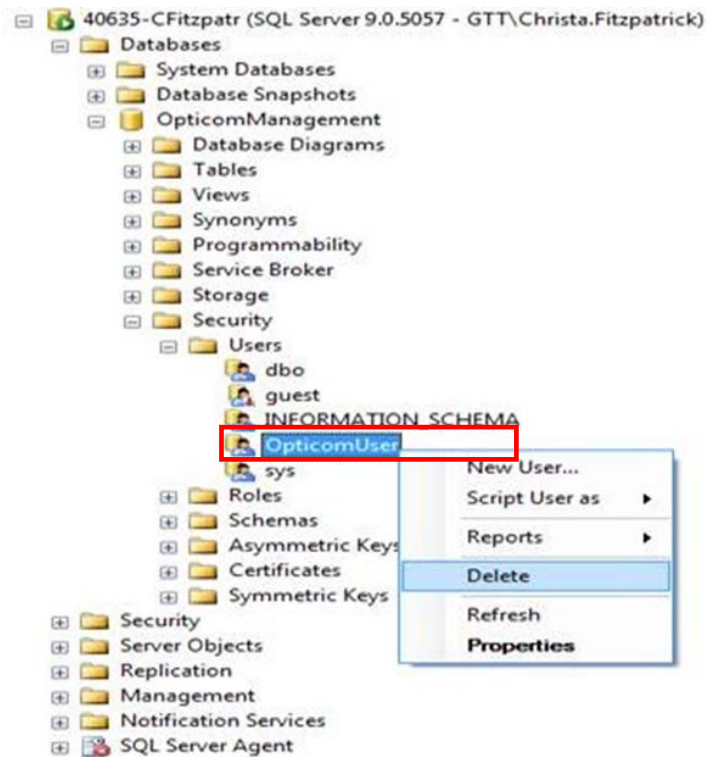


Figure 19-6

20 Create exceptions in Windows Firewall

Note:

- **GTT recommends that any modifications to the firewall described in this section be performed only by your IT department.**

This section contains additional details on opening the firewall. The basic process is described in section 3.4.

These steps apply to the version of Windows Firewall that is included in Windows XP SP2 and in Windows Server 2003. If you are using a different OS, see your firewall documentation for more information.

If you are running a firewall on the computer that is running SQL Server 2005, external connections to SQL Server 2005 will be blocked unless SQL Server 2005 and the SQL Server Browser service can communicate through the firewall. You must create an exception for each instance of SQL Server 2005 that you want to accept remote connections and an exception for the SQL Server Browser service.

SQL Server 2005 uses an instance ID as part of the path when you install its program files. To create an exception for each instance of SQL Server, you must identify the correct instance ID. To obtain an instance ID, follow these steps:

1. Click **Start**, point to **Programs**, point to **Microsoft SQL Server 2005**, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
2. In SQL Server Configuration Manager, click the SQL Server Browser service in the right pane, right-click, and then click **Properties**.
3. On the **SQL Server Browser Properties** page, click the **Advanced** tab, locate the instance ID in the property list, and then click **OK**.

To open Windows Firewall, click **Start**, click **Run**, type **firewall.cpl**, and then click **OK**.

20.1 Create an exception for SQL Server 2005 in Windows Firewall

To create an exception for SQL Server 2005 in Windows Firewall, follow these steps:

1. In Windows Firewall, click the **Exceptions** tab, and then click **Add Program**.
2. In the Add a Program window, click **Browse**.
3. Click the C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe executable program, click **Open**, and then click **OK**.

Note:

- **The path may be different depending on where SQL Server 2005 is installed. *MSSQL.1* is a placeholder for the instance ID that you obtained in step 3 of the previous procedure.**
 - **The path may also vary depending on which version of Windows you are using.**
4. Repeat steps 1 through 3 for each instance of SQL Server 2005 that needs an exception.

20.2 Create an exception SQL Server Browser service in Windows Firewall

To create an exception for the SQL Server Browser service in Windows Firewall, follow these steps:

1. In Windows Firewall, click the **Exceptions** tab, and then click **Add Program**.
2. In the Add a Program window, click **Browse**.
5. Click the C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe executable program, click **Open**, and then click **OK**.

Note:

- **The path may be different depending on where SQL Server 2005 is installed. *MSSQL.1* is a placeholder for the instance ID that you obtained in step 3 of the previous procedure.**
- **The path may also vary depending on which version of Windows you are using.**

21 Additional steps to open SQL for remote access

This section is only necessary if the steps in section 3-5 were not successful in opening SQL for remote access. There are separate subsections for SQL 2005 and SQL 2008.

21.1 SQL 2005

If you are running SQL Server 2005 by using an instance name and you are not using a specific TCP/IP port number in your connection string, you must enable the SQL Server Browser service to allow for remote connections. For example, SQL Server 2005 Express is installed with a default instance name of *Computer Name\SQLEXPRESS*. You are only required to enable the SQL Server Browser service one time, regardless of how many instances of SQL Server 2005 you are running. To enable the SQL Server Browser service, follow these steps.

Important These steps may increase your security risk. These steps may also make your computer or your network more vulnerable to attack by malicious users or by malicious software such as viruses. We recommend the process that this article describes to enable programs to operate as they are designed to, or to implement specific program capabilities. Before you make these changes, we recommend that you evaluate the risks that are associated with implementing this process in your particular environment. If you choose to implement this process, take any appropriate additional steps to help protect your system. We recommend that you use this process only if you really require this process.

1. Click **Start**, point to **Programs**, point to **Microsoft SQL Server 2005**, point to **Configuration Tools**, and then click **SQL Server Surface Area Configuration**.
2. On the **SQL Server 2005 Surface Area Configuration** page, click **Surface Area Configuration for Services and Connections**.
3. On the **Surface Area Configuration for Services and Connections** page, click **SQL Server Browser**, click **Automatic** for **Startup type**, and then click **Apply**.

Note When you click the **Automatic** option, the SQL Server Browser service starts automatically every time that you start Microsoft Windows.

4. Click **Start**, and then click **OK**.

When you run the SQL Server Browser service on a computer, the computer displays the instance names and the connection information for each instance of SQL Server that is running on the computer. This risk can be reduced by not enabling the SQL Server Browser service and by connecting to the instance of SQL Server directly through an assigned TCP port. Connecting directly to an instance of SQL Server through a TCP port is beyond the scope of this document. For more information about the SQL Server Browser server and connecting to an instance of SQL Server, see the following topics in SQL Server Books Online:

1. SQL Server Browser Service
2. Connecting to the SQL Server Database Engine
3. Client Network Configuration

Some people have been having issues when trying to make remote connections to SQL Express. This document will hopefully clarify most of the issues around remote connections.

First, networking protocols are disabled by default in SQL Server Express. Thus, if someone simply installs Express and chooses all the defaults, SQL Server Express will only be able to have connections originating on the local machine where SQL Server is installed.

STEP 1: Enabling TCP/IP

First we must tell SQL Server Express to listen on TCP/IP, to do this perform the following steps:

1. Launch the SQL Server Configuration Manager from the "Microsoft SQL Server 2005 CTP" Program menu
2. Click on the "Protocols for SQLEXPRESS" node,
3. Right click on "TCP/IP" in the list of Protocols and choose, "Enable"

STEP 2: To Browse or not to Browse

Next, we have to determine if we want the SQL Browser service to be running or not. The benefit of having this service run is that users connecting remotely do not have to specify the port in the connection string. Note: It is a security best practice to not run the SQLBrowser service as it reduces the attack surface area by eliminating the need to listen on an udp port.

OPTION A: If you want to always specify a TCP port when connecting (Not using SQL Browser service) perform the following steps else skip these steps:

1. Launch the SQL Server Configuration Manager from the "Microsoft SQL Server 2005 Configuration Tools" Program menu
2. Click on the "Protocols for SQLEXPRESS" node
3. Right Click on the "TCP/IP" child node
4. You will notice an entry on the right panel for "IPAll", right click on this and select, "Properties"
5. Clear out the value for the "TCP Dynamic Ports" property.
6. Give a TCP Port number to use when making remote connections, for purposes of this example lets choose, "2301"

At this point you should restart the SQL Server Express service. At this point you will be able to connect remotely to SQL Express. Check the connection by using SQLCMD from a remote machine and connecting like this: SQLCMD -E -S YourServer\SQLEXPRESS,2301
The "," in the server name tells SQLCMD it's a port.

If you still get an error. Go to Step 3 below.

STEP 3: Firewall

At this point you should be able to remotely connect. If you still can't chances are you have a firewall configured on the computer where SQL Express is running. The instructions below are for Windows XP SP2's firewall settings.

To enable the firewall to allow SQL Server Express traffic:

1. Launch the Windows Firewall configuration tool from the control panel.
2. Click the Exceptions Tab
3. Click the "Add Programs." button and select "sqlservr.exe" from the location where you install SQL Server Express.
4. You should now be able to remotely connect.

Notes:

- **You can get more restrictive by just specifying the port number that will be allowed (used best when configured with Option A).**
- **If you chose to use the SQL Browser service, you must also add sqlbrowser service executable to the exception list as it listens on udp port 1434.**

21.2 SQL 2008

1. Click **Start**, and open **SQL Server Management Studio**.
2. Press the Connect button to connect to the server,
3. Right click the server and select **Properties**. See Figure 21-1.
4. Click on **Connections** and check the **Allow remote connections box**. See Figure 21-2.
5. If you receive still receive errors when the client CMS is launched, refer to the following link.

<http://blogs.msdn.com/b/walzenbach/archive/2010/04/14/how-to-enable-remote-connections-in-sql-server-2008.aspx>

6. Or do a web search for "How to enable remote connections in SQL Server 2008".

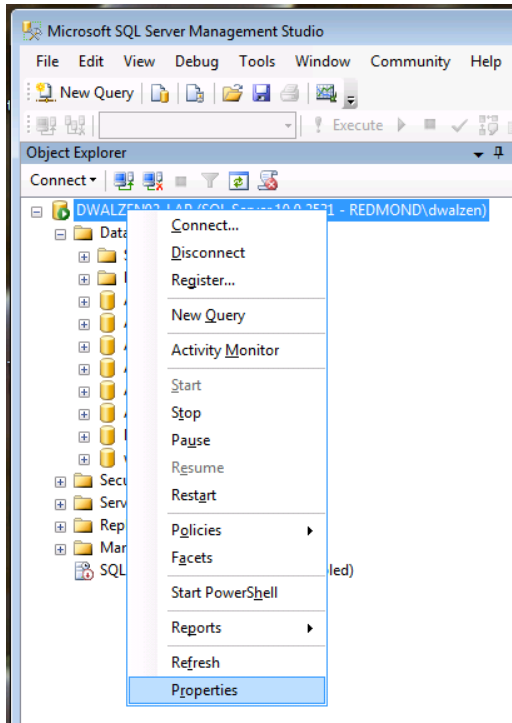


Figure 21-1

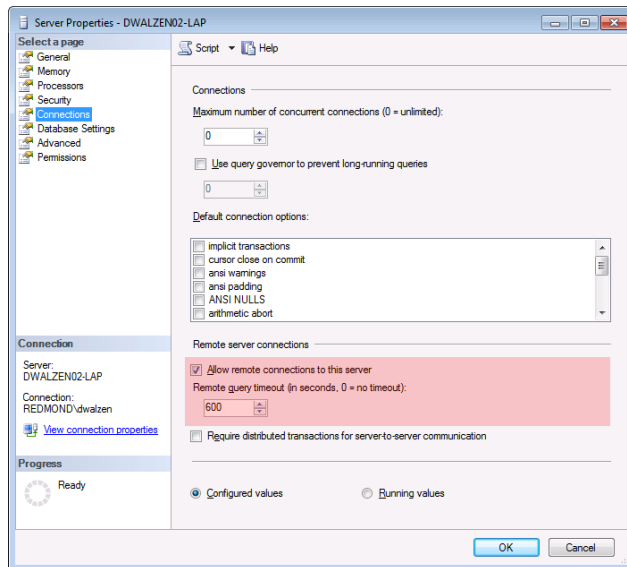


Figure 21-2

22 Upgrading to a new version

This section describes the procedure for upgrading your Central Management Software to a newer version.

Notes:

- **The CMS version on your server machine and all client machines must be the same. If the version on the client machine does not match the version on the server machine you will not be able to open CMS on the client machine.**
1. Shut down CMS on all client machines.
 2. Stop the monitoring job (if running) Section 9.2.1.
 3. Shut down CMS on the server machine.
 4. Shut down the Communications and Scheduling service on the server machine. See Section 3.3.1.
 - a. Not required but recommended.
 - b. CMS will prompt you to shut them down during installation if not stopped manually
 5. Install the new version on the server machine.
 - a. Select **Server Installation** option when prompted.
 - b. Verify **SQL instance name** when prompted and press **Next**. See section 3.2
 - c. Click **OK** to database upgrade prompt.
 - d. Click **Yes** to stopping the services if you have not stopped them manually.
 6. Allow process to complete and press **Finish**.
 7. Reboot the server machine.
 - a. Not necessary if final message says that the Communication and Scheduling services have started successfully.
 8. Verify that the Scheduling and Communication services have started.
 - a. Not necessary if final message says that the Communication and Scheduling services have started successfully.
 - b. Or see section 3.3.1 for details on starting services
 9. Install CMS on client machines.
 - a. Select **Client** option when prompted.
 - b. Verify **SQL instance name** when prompted and say press **Next**. See section 4.1.
 10. Verify that CMS will start on the client machines
 11. Restart the Monitoring job (if used)



Global Traffic Technologies

Global Traffic Technologies, LLC
7800 Third Street North
St. Paul, Minnesota 55128-5441
1-800-258-4610
651-789-7333
www.gtt.com

Global Traffic Technologies
Canada, Inc.
157 Adelaide Street West
Suite 448
Toronto, ON M5H 4E7
Canada
1-800-258-4610

Opticom and the GTT logo mark are
trademarks
of Global Traffic Technologies, LLC
Please recycle. Printed in the U.S.A.
© Global Traffic Technologies, LLC 2012
All rights reserved.
79-1000-0722-0 Rev. A