MANEUVER CONTROL SYSTEM (MCS)
System Administration Manual (SAM)

VERSION 6.4.4.3 P1

CONTRACT DAAB07-96-C-E008
CDRL # TMSS-01
DOCUMENT # MCS(L)-U1-2018

18 October 2005

PREPARED FOR

PROJECT MANAGER, GROUND COMBAT COMMAND AND CONTROL
SFAE-C3S-MVR
FORT MONMOUTH, NEW JERSEY 07703-5405

PREPARED BY

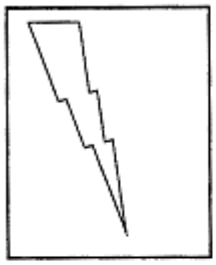
LOCKHEED MARTIN INTEGRATED SYSTEMS & SOLUTIONS
106 APPLE STREET
TINTON FALLS, NEW JERSEY 07724

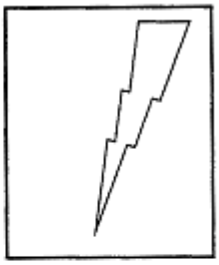
Documentation/Tech Data

Warning Page

5 SAFETY STEPS TO FOLLOW IF SOMEONE IS THE VICTIM OF ELECTRICAL SHOCK

1. SEND FOR HELP AS SOON AS POSSIBLE
2. DO NOT TRY TO PULL OR GRAB THE INDIVIDUAL
3. IF POSSIBLE, TURN OF THE ELECTRICAL POWER
4. IF YOU CANNOT TURN OFF THE ELECTRICAL POWER, PULL, PUSH, OR LIFT THE PERSON TO SAFETY USING A DRY WOODEN POLE, A DRY ROPE, OR SOME OTHER INSULATING MATERIAL
5. AFTER THE INJURED PERSON IS FREE OF CONTACT WITH THE SOURCE OF ELECTRIC SHOCK, MOVE THE PERSON A SHORT DISTANCE AWAY AND IMMEDIATELY START ARTIFICIAL RESPIRATION



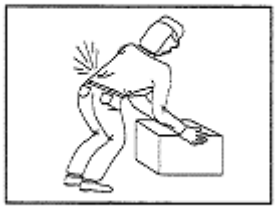


ELECTRICAL HAZARD

Under adverse conditions, the voltage used in this equipment can cause death or serious injury. Observe the following safety precautions:

GROUND THE EQUIPMENT	Before connecting primary power cables, connect the grounding cable from the ground lug on the power control box to earth ground. Do not remove the grounding cable until the signal cables and primary power cables have been disconnected and the generator has been shut down.
AVOID THE POWER INPUT	Be careful not to contact the 115 Vac input connections when installing or servicing the equipment.
DO NOT SERVICE ALONE	Never work on the equipment unless there is another person nearby who is familiar with the operation and hazards of the equipment and who can administer first aid.
USE ONLY ONE HAND	Whenever possible, use only one hand to service the equipment. Keep the other hand away to reduce the hazard of current flowing through the vital organs of the body.

WARNING



HEAVY EQUIPMENT

Improperly lifting or carrying heavy equipment can result in serious injury or death. Refer to the following weight limits as guidelines:

Handling Function	One Person Max. Lift	Two Person Max. Lift	Two Person Max. Lift (Male Only)
Lift an object from the floor and place it on a surface not greater than 5 feet above the floor.	37 lbs	74 lbs	112 lbs
Lift an object from the floor and place it on a surface not greater than 3 feet above the floor.	44 lbs	88 lbs	174 lbs
Carry an object 33 feet or less.	42 lbs	84 lbs	164 lbs

CAUTION

THIS EQUIPMENT CONTAINS PARTS
AND ASSEMBLIES SENSITIVE TO
DAMAGE BY ELECTROSTATIC DISCHARGE (ESD).
USE ESD PRECAUTIONARY PROCEDURES
WHEN TOUCHING, REMOVING OR INSERTING
PRINTED CIRCUIT BOARDS.

ESD
CLASS 1

GENERAL HANDLING PROCEDURES FOR ESD ITEMS

- USE WRIST GROUND STRAPS OR MANUAL GROUNDING PROCEDURES.
- KEEP ESD ITEMS IN PROTECTIVE COVERING WHEN NOT IN USE.
- GROUND ALL ELECTRICAL TOOLS AND TEST EQUIPMENT.
- PERIODICALLY CHECK CONTINUITY AND RESISTANCE OF GROUNDING SYSTEM.
- USE ONLY METALIZED SOLDER SUCKERS.
- HANDLE ESD ITEMS ONLY IN PROTECTED AREAS.

MANUAL GROUNDING PROCEDURES

- MAKE CERTAIN EQUIPMENT IS POWERED DOWN.
- TOUCH GROUND PRIOR TO REMOVING ESD ITEMS.
- TOUCH PACKAGE OR REPLACEMENT ESD ITEM TO GROUND BEFORE OPENING.
- TOUCH GROUND PRIOR TO INSERTING REPLACEMENT ESD ITEMS.

ESD PROTECTIVE PACKAGING AND LABELING

- COVERING OF ANTI-STATIC MATERIAL WITH AN OUTER WRAP OF EITHER TYPE 1 ALUMINIZED MATERIAL OR CONDUCTIVE PLASTIC FILM OR HYBRID LAMINATED BAGS HAVING AN INTERIOR OF ANTI STATIC MATERIAL WITH AN OUTER METALIZED LAYER.
- LABEL WITH SENSITIVE ELECTRONIC SYMBOL AND CAUTION NOTE.

Record of Changes

MCS System Administration Manual (SAM)

Summary of MCS 6.4.4.2 P7 Updates

Changes	Topics Impacted
AIS, BCS • There is now only one type of PASS. There will no longer be references to EZPASS/MCS PASS or AIS PASS. References to EZPASS, MCS PASS and AIS PASS will be changed to PASS. • The BCS is a Server machine that will have PASS, C2R and SQL software on it. There have been problems with putting SQL Server software on the BCS, but the intent is that SQL Server software will be on the BCS. Any reference to the location of SQL Server has been changed to BCS.	1-2.1, 1-2.3, 1-2.4, 1-2.7, 1-7.1, 3-3.1, 3-4.2.6, 3-7.1,3-7.6, 3-7.9

MCS System Administration Manual (SAM)

Summary of MCS 6.4.4.3 Updates

Changes	Topics Impacted
Server Configuration Console	
• There is now the ability to subscribe, publish, add and remove CPOF data provider topics.	3-3.4, 3-3.4.7
• The user can now start and stop the NRTS data provider upon configuration.	3-3.3
• The Server Configuration Console now monitors its connection to NRTS every 5 seconds and prevents the user from entering data if the connection goes down.	3-4.3.1
• NRTS data will not be loaded/configured if the NRTS connection is not good. The errors reported will better explain what is happening.	3-4.3
• The Start/Stop/Pause buttons have been made inoperable on the server status GUI for the time being, until the capability is added to NRTS to allow the Server Configuration Console to start and stop individual data providers.	3-4.9

Changes	Topics Impacted
• There is now an enhanced error and exception logging for the “Test NRTS to PASS Connection” button on the NRTS General page.	3-4.3.4

MCS System Administration Manual (SAM)

Summary of MCS 6.4.4.3 P1 Updates

Changes	Topics Impacted
Server Configuration Console	
• There is now the ability to add and remove both Multicast and UDP Addresses into the Group Settings for the FBCB2 Injector.	3-4.3.4.4
• The GCCS injector now displays the current box's IP address in the TMS Broker address text box if NRTS sends "127.0.0.1" to Server Configuration Counsel (SCC).	3-3.4.2
• NRTS is no longer starting as a Service. The executable is running as a process. Starting MCSServicesStartup will not start NRTS Server Console.	3-3.1
Battle Command Server (BCS)	
• A Battle Command Server overview section was added.	1-2

Table Of Contents

Chapter 1 Roles and Responsibilities

1-1 Duties and Responsibilities

1-1.1 Overview of Duties and Responsibilities

The Maneuver Control System (MCS) environment is viewed differently depending upon the task to be performed. For example the role and responsibility of installing and configuring the Unit Server differs from the role and responsibility of installing and configuring the MCS/BCS Server, MCS Gateway or MCS Workstation.. The role of a soldier using MCS to view a mission differs greatly from the role of the administrator configuring the database server. The following will identify the duties and responsibilities of each of the various members within the MCS environment.

1-1.2 MAU Duties and Responsibilities

The Mission Application User (MAU) is responsible for utilizing the resources available within MCS to plan and implement the goals and objectives of the ARMY.
The MAU will utilize messaging to send and receive United States Message Text Format (USMTF) and Joint Variable Message Format (JVMF) messages.
The MAU will utilize Maps & Overlays to create and view geo-referenced data. This data can be received from all ABCS systems. Additionally, MCS Maps and Overlays integrated NBC products from the JWARN system. The Maps & Overlays application uses unit name and roles to determine user ownership of data. Data not owned by the unit/role cannot be altered by that user. Commanders, G3 and S3 have additional permission to modify data in order to maintain the COP when data is not available.
The MAU will utilize the Military Decision Making Process – Assistant (MDMP-A) to support the planning process. This tool embeds CAPES war gaming engine and MS Office. It can disseminate plans to a Web server, via E-mail, as a JVMF message and to the PASS Server.
The MAU will utilize the Task Organization Program to create both friendly and hostile units organizational structure. This tool can be used to create new friendly and hostile units. This unit data can be sent to the SQL Server MCS-DB, Access MCS-DB, archived to a file, and sent to the PASS Server. Only users with the role of commander, G3 or S3 can create new units and modify the unit(s) organizational structure. Other roles can view the task organization.

1-1.3 MAA Duties and Responsibilities

The Mission Application Administrator (MAA) is responsible for configuring the MCS Workstation and the MCS Gateway for operation. Given a properly configured computer system complete with the Operating System, Microsoft Office products, virus protection software, and all additional applications necessary prior to the installation of MCS, the MAA will install the MCS Workstation software using the MCS installation disks. Once the workstation software has been installed, the MAA will configure the workstation using the Army C2 Management Console (referred to as Management Console herein).

NOTE

On the Server and MCS Gateway, the Management Console is specifically referred to as the Client Auto Setup Console. On the MCS Workstation, the Management Console is specifically referred to as the Army C2 Management Console.

The MAA will perform basic configuration troubleshooting using the available resources of MCS. These resources include the MCS release notes, available log files, on-line help system, and the troubleshooting section of the Management Console.
The following diagram identifies the MCS Workstation and the MCS Gateway system assets.

Figure 1-1 Workstation and Gateway assets

1-1.4 SA Duties and Responsibilities

1. The System Administrator (SA) is responsible for installing the base Operating System and necessary Common Off The Shelf (COTS) software onto the Server, Gateway and Workstation systems. The Server requires SQL Server 2000 to host the MCS database. The Windows Domain Login is used to authenticate users. The Server utilizes the Windows Server 2003 Operating System. The MCS Gateway and the MCS Workstation utilize the Windows XP Professional Operating System. Additionally, the entire Microsoft Office Suite of applications needs to be installed and configured onto each of the MCS systems (i.e., MS WORD, Power Point, Excel, Outlook, and Access).
2. Upon completion of configuring the Operating System and COTS, the System Administrator will install and configure the Server computer system.
3. The following diagram identifies the Server system assets:

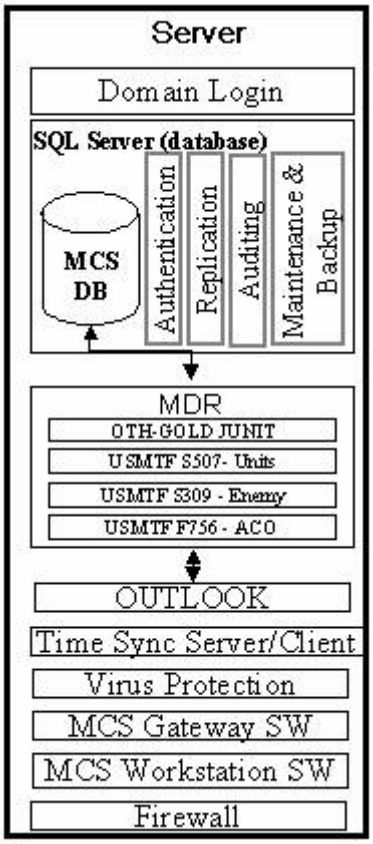


Figure 1-2 Server Assets

1-1.5 Server Administrator Duties and Responsibilities

The Server Administrator is responsible for installing and configuring the Unit Server. The Unit Server provides critical services at CORPS and DIV to meet the needs of MCS. Unit Servers are located at CORPS and DIV. Typically there are three sets of servers for each CORPS/DIV that are allocated to the Main, TAC and Rear. Other TOCs access these servers via a TCP/IP connection obtained using unit owned communication assets. The unit server utilizes the Windows Server 2003 operating system.
Maintenance and backup plans are setup by the Server Administrator and typically occur every hour. The backup file is placed on another machine in the network. Additionally, backup data is to be archived to external media.
These services must be configured on the Unit Server before MCS is installed.

- Active Directory with Domain Login accounts and Policy Management
- Virus Protection Software
- System Management Services (SMS)
- Network Services; DNS, DHCP
- Microsoft's Exchange Server 2000
- Internet Information Services (IIS)

The following diagram identifies the Unit Server Assets.

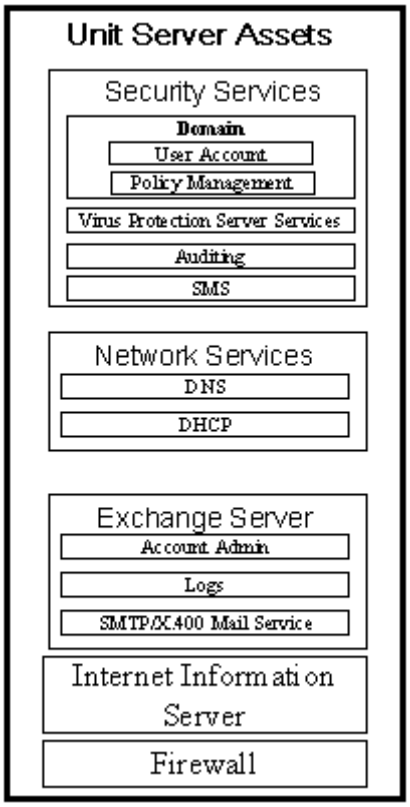


Figure 1-3 Unit Server Assets

Windows Server 2003 Time Synchronization Server and client are used. These services use Network Time Protocol (NPT). Server time is synced with GCCS-A. MCS Gateways and Workstations sync their time with the Server.

1-2 Battle Command Server Overview

The Battle Command Server (BCS) is a MCS system that is fielded to units with Army Battle Command System (ABCS) 6.4 requirements. BCS consolidates the services of the MCS Server, MCS Gateway and PASS Server, and provides backward compatibility to legacy ABCS 6.3d capabilities.

The BCS compacts the service of three separately fielded components at Brigade and Division Echelons: MCS Server, MCS Gateway, and the PASS Server.

- MCS Server located at Division level units.
  - PASS failover mechanism
  - Data Hub for all MCS Clients
- MCS Gateway located in Battalion and Brigades.
  - Primary PASS engine for Battalion level units
  - Secondary PASS engine for Brigade level units
- PASS Server located at Division and Brigade level units.
  - Primary PASS engine for Brigade and Division
  - Primary Time, C2R server for all units

BCS is fielded to all Brigade and Division Echelons, while MCS Gateway continues to be fielded to Battalion for PASS services.
BCS supports the following services:

- Command and Control Personal Computer (C2PC)
- Publish and Subscribe Services (PASS)
- Near Real Time Server (NRTS)
- Database Management Utility
- Command and Control Registry (C2R)
- Multilateral Interoperability Program (MIP)
- Advanced Field Artillery Tactical Data System (AFATDS) AXE Client
- SA Data Flow from Multicast

1-3 MCS Data Flow

1-3.1 Description of General Data Flow

The Maneuver Control System (MCS) acts as a conduit for all information affecting the battlefield, gathering intelligence and other data from systems and sensors across the battle space. MCS integrates this data and shares it among all systems in a Common Operating Picture (COP) that is recognizable to commanders at all levels. The MCS system exchanges this information with two other key Army Battle Command System (ABCS), the Global Command and Control System - Army (GCCS-A) and the Force XXI Battle Command Brigade and Below (FBCB2) to provide a continuous battle picture across all force echelons.

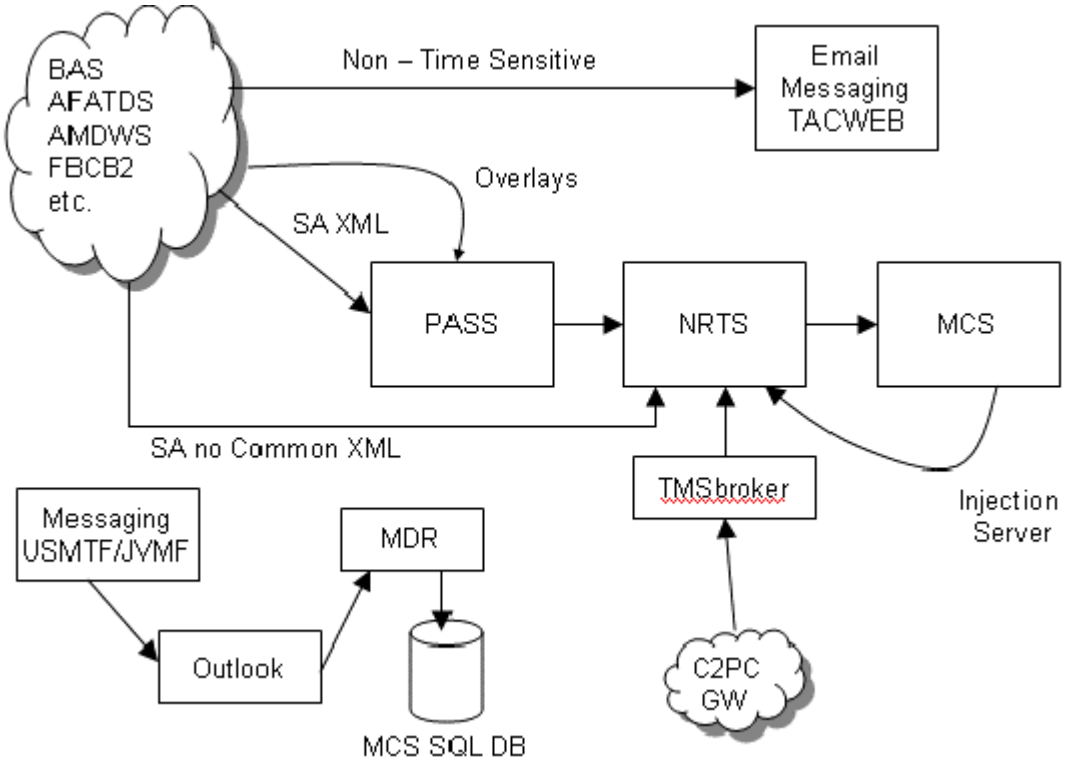


Figure 1-4 General Data Flow

There are many external forms of digitized information available to the commander which must be integrated into MCS. To integrate the various forms of information, the following components are available:

- Command and Control Personal Computer (C2PC)
- Publish and Subscribe Services (PASS)
- Near Real Time Server (NRTS)
- Database Management Utility
- Command and Control Registry (C2R)
- Multilateral Interoperability Program (MIP)
- Advanced Field Artillery Tactical Data System (AFATDS) AXE Client
- SA Data Flow from Multicast
- Time Sync

1-3.2 Command and Control Personal Computer (C2PC)

Command and Control Personal Computer (C2PC) is a Windows-based client software application designed to facilitate military command and control functions by improving situational awareness (SA) and to enhance operational and tactical decisions. When connected to a network, C2PC exchanges position tactical track data with UNIX based Tactical Data Base Management (TDBM) Systems such as Tactical Combat Operations (TCO) system, Intelligence Analysis System (IAS), and Global Command and Control System (GCCS) and provides a complete geographically based situational awareness capability including the capability to display the GCCS Common Operational Picture (COP) data.
C2PC is composed of two distinct components - the C2PC Gateway, and the C2PC Client. These components can reside on the same computer or on different computers. The C2PC Gateway interfaces with a UNIX-based TDBM host computer. The Gateway also receives track updates from the clients and forwards them back to the TDBM server. See the C2PC Gateway overview and information flow below.

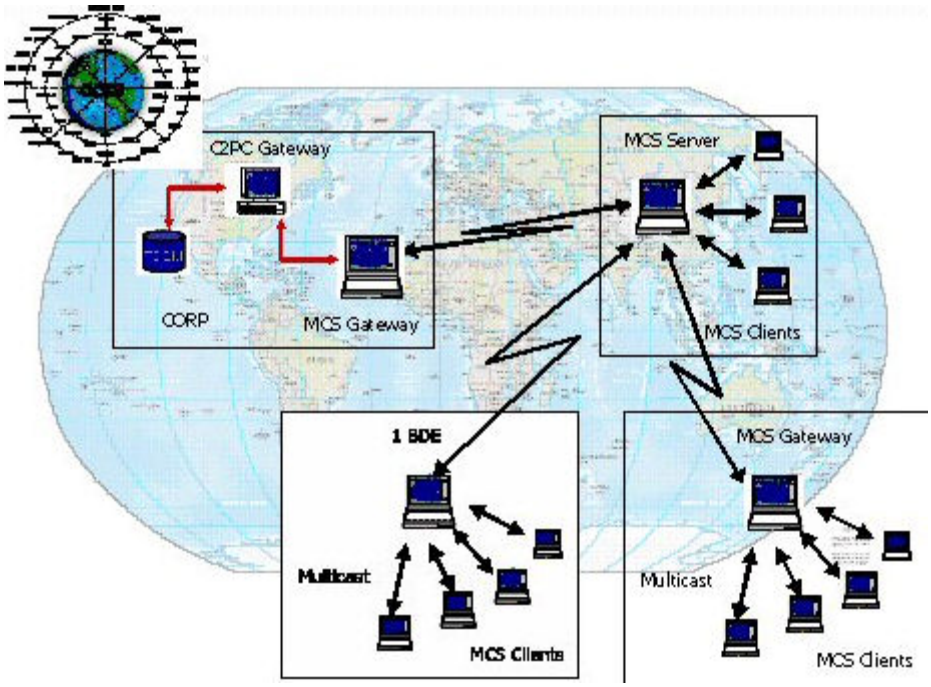


Figure 1-5 C2PC Overview

1-3.3 PASS

PASS is an information routing system which delivers data from publishers to subscribers. Publishers publish data to a topic without knowledge of which subscribers are subscribing to that topic. Subscribers subscribe to information topics without knowledge of which publishers are publishing information to that topic.

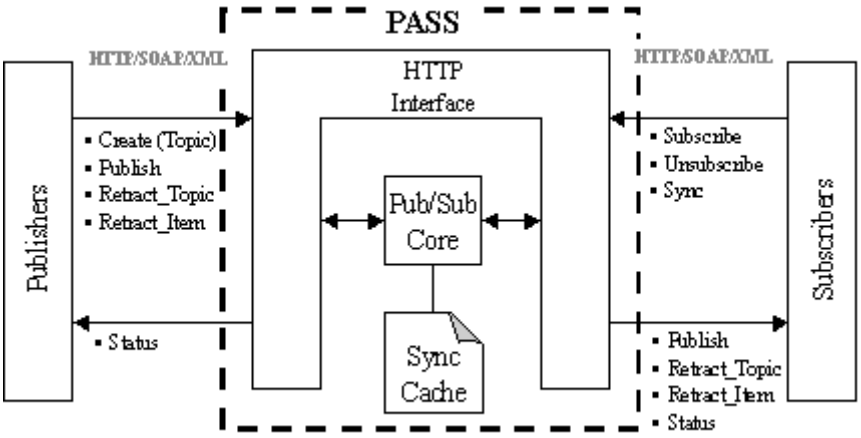


Figure 1-6 PASS

1-3.4 Near Real Time Server (NRTS)

The Near Real Time Server (NRTS), receives data from Battlefield Automated System (BAS), processes and disseminates the information to the Live Feed Clients running on MCS. The NRTS System Administrator section of this document describes the setup, configuration and startup procedures for NRTS System Administrators. In brief, that section details how to connect the NRTS with data providers and how to ensure the MCS clients are able to receive the NRTS feed. The Near Real Time Server information flows via the following path:

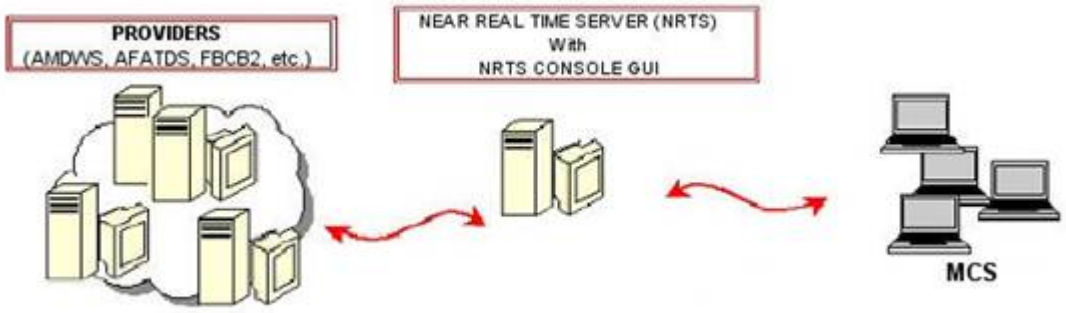


Figure 1-7 NRTS Information Path

1-3.5 Database Management Utility

The Database Management Utility allows the system administrator to maintain data consistency between two or more SQL Servers. Replication can be configured by altering the replication interval, enabling or disabling replication, and adding or removing SQL Servers to the Group of available SQL Replication Servers. The SQL Server Group consists of Publishers and Subscribers. There can exist only one Publisher in the group at a time, the remaining members

act as Subscribers. The Publisher will replicate its SQL data onto the Subscribers at regular intervals as configured. Group member roles can also be configured. At any time, an Administrator can alter the role of a Publisher making that SQL Server a Subscriber, then alter the role of a Subscriber to becoming the new Publisher.

1-3.6 Command and Control Registry (C2R)

Either the Server Computer or the Battle Command Server (BCS) hosts the Command and Control Registry (C2R). Included with the C2R server installation is the C2R Planner application which is used to create and edit the C2R organizational data, as well as to create certain files that are required for proper operation of the MCS messaging software.

1-3.7 Multilateral Interoperability Program (MIP)

The MCS MIP Gateway capability is designed to support coalition force operations. When US forces are working in close proximity of other national forces in a command, support, or proximity relationship, those units are required to interoperate. NATO, US Joint, and Army doctrine provide guidance on communications and liaison responsibilities.
The Multilateral Interoperability Program (MIP) component consists of the two essential components: The mapping engine (“Mapper”) and the MIP Gateway. The Mapper ensures proper formatting between incoming and outgoing data. It is also the PASS interface and requires the SQL Server to operate, and the MIP Gateway is installed on a dual-LAN card machine so that it is connected to both the Army TOC and the Coalition Forces networks. Normally installed on two separate machines, the MIP Gateway can be installed on the Mapper machine if that machine has both SQL Server and dual LAN connections. At the present time the Mapper runs on Windows Server 2000, and the MIP Gateway runs under Windows 2000 Professional. The figure below shows an overview of the MIP Gateway and mapping engine configured on a single server.

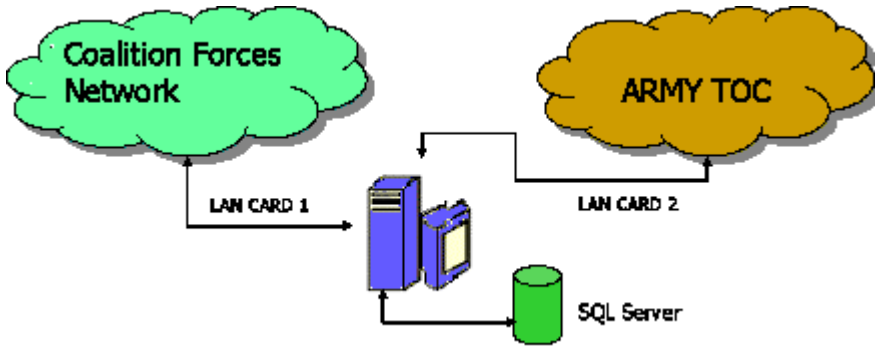


Figure 1-8 MIP Gateway and Mapping Engine

1-3.8 AFATDS AXE Client

The Advanced Field Artillery Tactical Data System (AFATDS) AXE Client allows MCS to receive AFATDS data such as fire support, units and battlefield geometries.

1-3.9 SA Data Flow from Multicast

Situational Awareness (SA) Data Flow from Multicast allows FBCB2 data to be received via a multicast group. The information received includes reports of units and platforms, observed position reports, bridges, minefields and obstacles.

1-3.10 Time Sync

Time Sync is a software program that synchronizes time throughout the servers.

NOTE

The SQL Server is the software application that runs on the MCS database (MCS_DB). The SQL Server can reside on the Battle Command Server hardware, or on a separate database

server. Server Setup installations can automatically restore the SQL Server MCS_DB if the SQL Server is running on the BCS. Your Systems Administrator will know the TOC requirements at the time the system is being built.

1-4 Assistance and Problem Reporting

1-4.1 Reporting Errors or Making Suggestions Regarding the SAM

You can help improve this manual. If you find any mistakes, or if you know of a way to improve the procedures, please let us know. We'd prefer that you submit your recommended changes electronically, either by e-mail (AMSEL-LC-LEO-PUBS-CHG@mail1.monmouth.army.mil) or online (http://edm.monmouth.army.mil/pubs/2028.html).
Alternatively, you may mail or fax your letter, DA Form 2028 (Recommended Changes to Publications and Blank Forms) to: Commander, US Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-E-ED, Fort Monmouth, NJ 07703-5006. The fax number is 732-532-3421, DSN 992-3421. In any case, we will send you a reply.

1-4.2 Reporting Equipment Improvement Recommendations (EIR)

If your equipment needs improvement, let us know. Send us an EIR. You, the user, are the only one who can tell us what you don't like about your equipment. Let us know why you don't like the design or performance. Put it on an SF 368 (Product Quality Deficiency Report). Mail it to: Commander, US Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-D-CS-CFO, Fort Monmouth, New Jersey 07703-5006. We'll send you a reply.

1-4.3 MCS Technical Support

The technical support department at the Communications-Electronics Command (CECOM) Software Engineering Center (SEC) would like to provide detailed and accurate answers to all of your questions. In order to do so, our representatives will need the following information:

- The version of the MCS software. This can be determined by right-clicking on the classification banner. Select About Classification Banner from the pop up menu to display the Version ID.
- The system information for the computer you are using, including the make and model of the machine, the operating system version, the amount of memory, and system resources.
- The version and service packs/releases, of the following Microsoft products: Windows, Office, and Internet Explorer.
- Please provide a detailed description of the problem. Describe any error messages exactly as they appear. In addition, please list the steps and conditions that led to the problem.

Description	Phone, Address
Phone Mon-Fri 0800-1700 CST Phone (24 hours)	Com: 254-532-8321 EXT 4079 Com: (254) 644-7273
E-mail	bruce.thoms@us.army.mil

Mail

Bruce Thoms
MCS 6.4 Lead
53rd and North Ave, CTSF, Trailer 15
Fort Hood, Tx. 76544

1-5 Modes of Operation in MCS

MCS 6.4 has three modes of operation:

1. **MCS Workstation**: This is the standard MCS Client. Most MCS laptops will be configured in this mode. It provides all functionality for the basic MCS user.
2. **MCS Gateway**: This mode includes everything in the MCS Workstation, plus the ability to serve as a provider on the C2PC Gateway network. Note that all MCS Workstations have the ability to exchange data using the C2PC/GCCS-A network, but the MCS Gateway configuration includes the Gateway manager software, allowing this machine to function as a 'hub' on the Gateway. The MCS Gateway also hosts the PASS server, the Near Real Time Server (NRTS) and the Alerts server for TOCs without PASS, and to facilitate CONOPS.
3. **Server**: This mode includes everything in the MCS Workstation and the MCS Gateway, plus the Microsoft SQL-Server database and the Message Data Replicator (MDR).

1-6 Conventions

1-6.1 Description of Conventions

Conventions are methods of describing procedures using familiar terms. They are designed to standardize procedures for all system functions. Computer industry standard conventions are used as much as possible. The table shown below includes the conventions used in this document.
It should also be noted that whenever pronouns or other references denoting gender appear in this document, they refer to both male and female users unless otherwise indicated.
Table 1: Manual Style Conventions

CONVENTION/TECHNIQUE/TERM	TEXT TYPEFACE	DESCRIPTION
1. Messages and Text:		
Computer-generated text used in narrative text.	Arial	Computer-generated text (file names, directories, and error messages) is in Arial type face.
2. User Inputs:		
a. Commands, for example: From the System Main Menu, select the....	Boldface	Indicates a command, or an action that the user must perform.

b. Object of Commands. For example: From the System Main Menu, select the *Applications* button.	Italics	Commands appear in boldface with objects in *italics*. In the example, select is the command, and *Applications* is the object. Even though this is computer-generated text, when used as the object of a command, it will appear in *italics*.
c. Single Character Keys: *W, M, 8, 9,:,;, &,* and #.	Italics	Single character keys (letters, numbers, punctuation marks, or individual symbols) are in *italics*.
d. Multi-Character Keys: <*Enter*>, <*F2*>, and <*Shift*>.	*Italics* inside angle brackets	Multi-character keys (initial cap words) are shown as labeled on the keyboard, and enclosed and *italic* in angle brackets as shown: <*Enter*>, <*F2*>, and <*Shift*>.
3. Accelerator Keys (Hot Keys or Short-Cut Menu Selection Keys):		
<*F1*> through <*F10*> are multi-character keys as defined in 2(d), and are also function keys.	*Italics* inside angle brackets	The function keys, <*F1*> through <*F10*>, are the top row of keys.
Extend character keys, otherwise known as the <*ALT*> keys.	*Italics* inside angle brackets	The <*ALT*> keys are located on both sides or on one or the other side of the space bar.
Press the <*ALT*> key and the <*F5*> key to restore.	*Italics* inside angle brackets	Function Keys <*F3*> through <*F5*> and <*F7*> through <*F10*> are used with the <*ALT*> key. These keys are known as the accelerator keys, hot keys, or short-cut keys.
Press the <*Shift*> key and the *left mouse* or *track-ball* button.	*Italics* inside angle brackets	The <*Shift*> keys located on both sides of the keyboard used in conjunction with the left click, allow multiple sequential selection of Overlays, Symbol Sets, and objects.
Press the <*Control*> key and the *left mouse* or *track-ball* button.	*Italics* inside angle brackets	The <*Control*> key located on the left sides of the keyboard used in conjunction with the left click, allow multiple un-sequential selection of Overlays, Symbol Sets, and objects.

Right-click the mouse or track ball button on an object.	Boldface	Used to open object pop-up menus.
4. Mnemonic Keys:		
Mnemonic keys are generally the letter key that relate to the first or underlined letter of a displayed menu option.	*Italic* single characters	Mnemonics are generally the first letter of a displayed menu option, and are shown with underscores. For example, to select the *Restore* menu option using a Mnemonic keying process, press the <*R*> key and then the <*Enter*> key.
5. Text Selection:		
highlight, select, or click	Boldface	To highlight, select, or click means to place the cursor on an option or field and, unless otherwise noted, press the left mouse button once and then release it.
double-click	Boldface	To double-click means to place the cursor on an option or field, press the left mouse button twice in rapid succession, and then release it.

1-6.2 System Messages

System messages are presented in Courier New, upper case, italic and centered on the page, as shown in the following example:
THIS PROGRAM HAS PERFORMED AN ILLEGAL OPERATION AND WILL BE TERMINATED.

1-6.3 Other Highlighting

In addition to the examples shown above, italics are used to highlight some other items in this manual. Italic type is used to highlight buttons on windows, as in the following example:

1. **Click** on *OK* to confirm your selection.

   Italic type is also used for names of windows, menus, and fields (areas on a window in which you enter text). The following examples show the use of italic type in this manual.

2. **Set** the clearance from the *Security Officer* window.
3. **Select** the *Exit* option from the *File* menu.
4. **Enter** the password in the *New Password* field.

1-7 Typical MCS Desktop Configuration

The typical MCS desktop has five important features, which are shown below:

- *Start Menu* - Start menu for applications, setup, and documents.
- *Classification Banner* - Displays classification, received alerts, user and time information.
- *Task Bar* - Displays a list of open applications.
- *Desktop Area* - Displays of MCS Applications.
- *Shortcut Icons* - Quick access to applications, utilities and documents.

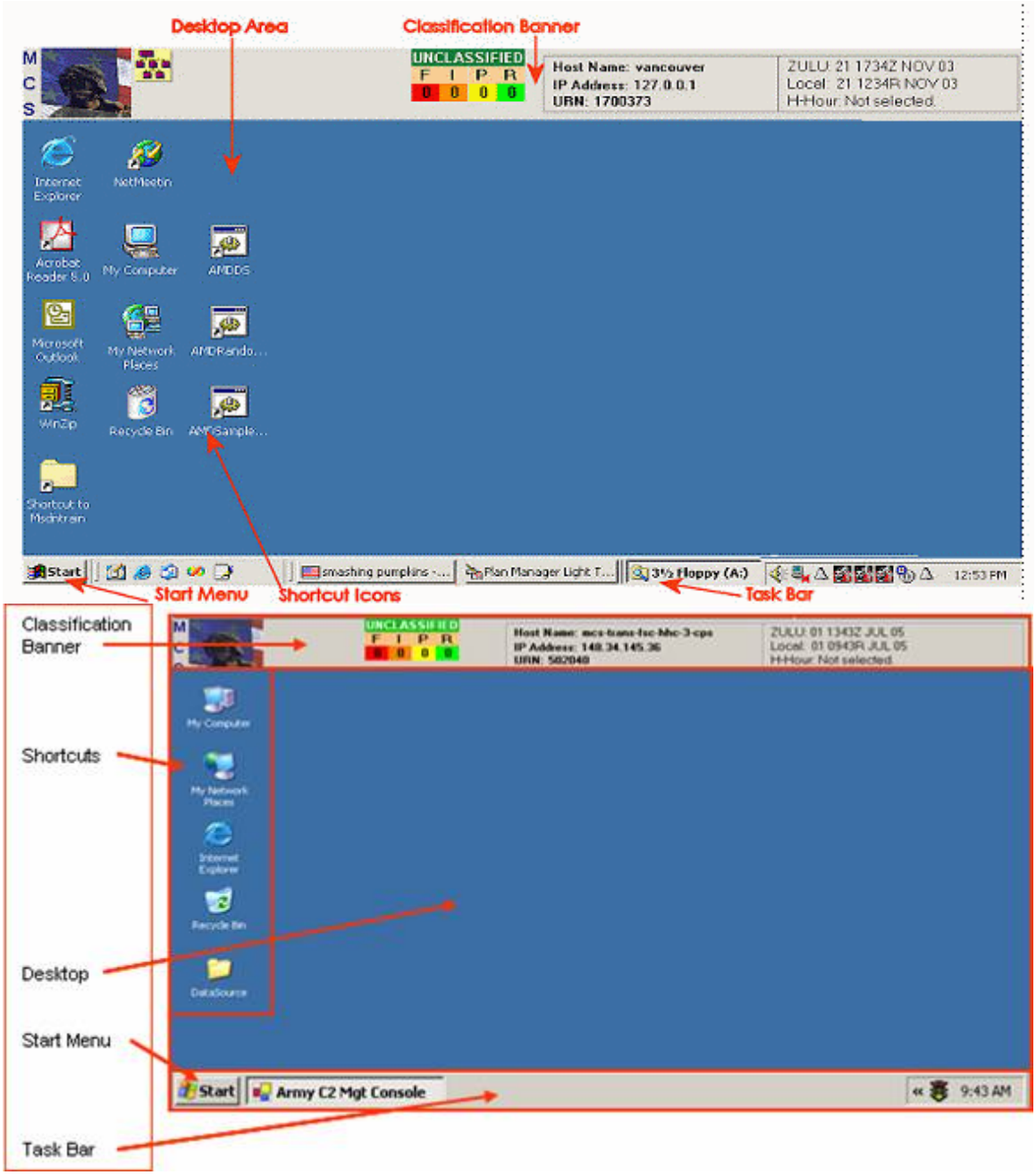


Figure 1-9 Typical MCS Desktop

Task Bar
The Task Bar is a Windows operating system area that is used to display a list of open applications, documents and utilities. Information on how to add or delete items from the Task Bar is available from Windows Help.
Classification Banner
The Classification Banner is one of the tools in the MCS Application Suite. It is displayed on the Desktop Area and consists of the: MCS Logo, shortcuts, Classification Banner, Unread Message Count, User Information and Time
Information.

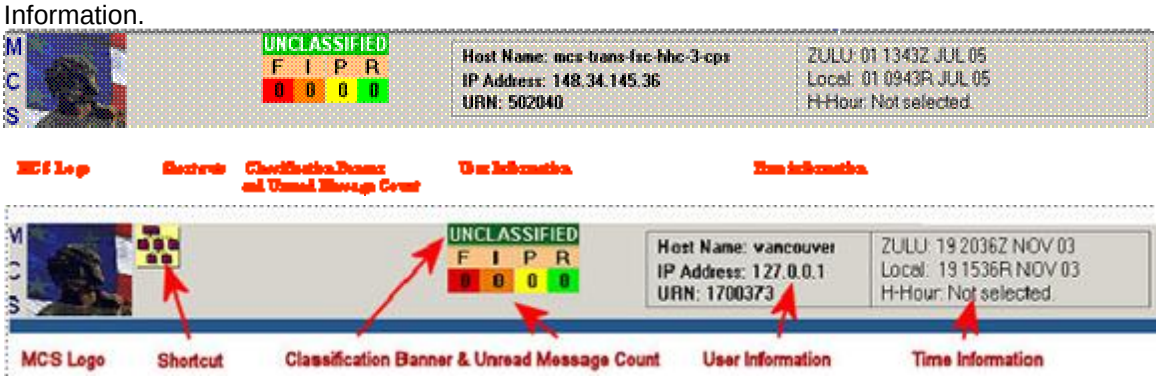


Figure 1-10 MCS Classification Banner

Desktop Area
The desktop area is used to display the MCS Application Suite graphical user interfaces (GUI).

1-8 Starting the MCS Management Console

MCS Management Console is started from the Windows Start menu:

1. **Select** *Start* from the Windows Start menu.
2. **Select** *Programs* from the list.
3. **Select** BCS from the list of programs.
4. **Select** *Administration* from the list.
5. **Select** *Management Console* from the list. The *Army C2 Management Console* window opens.

1-9 Help

1-9.1 Accessing Help

To open Help, **click** Help on the window menu bar (or **press** the *F1* key) and the help window opens. Navigate to the desired topic by using the Table of Contents, Index, or Search function.

1-9.2 Table of Contents

1. **Click** on a closed book icon to expand and view topics.
2. **Click** on the desired topic to open.

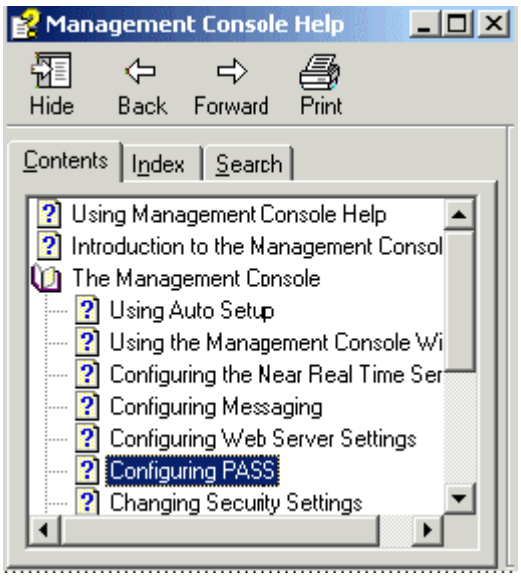


Figure 1-11 Help Table of Contents

1-9.3 Index

1. **Click** the *Index* tab to open the Help Index.
2. **Scroll** down the list, or **type** the first letter(s) of the desired topic. The Index will jump to the topics beginning with the typed letter(s).
3. **Click** on the topic. If there is more than one topic related to the selection, a multiple topic window will open. You can also choose from subtopics listed below the main topic.

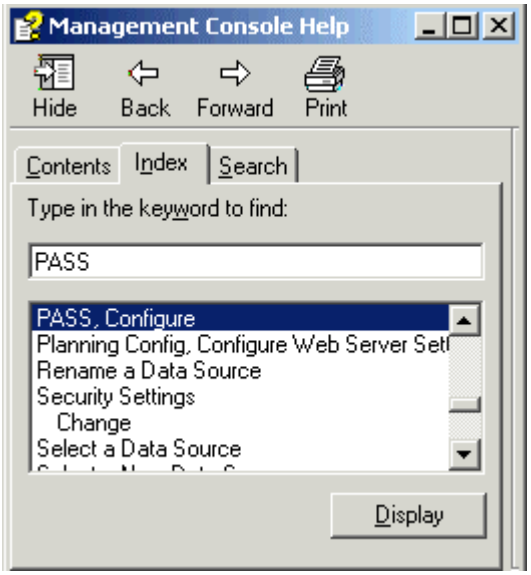


Figure 1-12 Help Index

1-9.4 Search

1. **Click** the *Search* Tab to search the database for a specific topic.

2. **Enter** the desired word(s) in the *Type in the keyword to find:* field, and then **click** the *List Topics* button. All topics related to the word(s) will appear in the left lower panel.

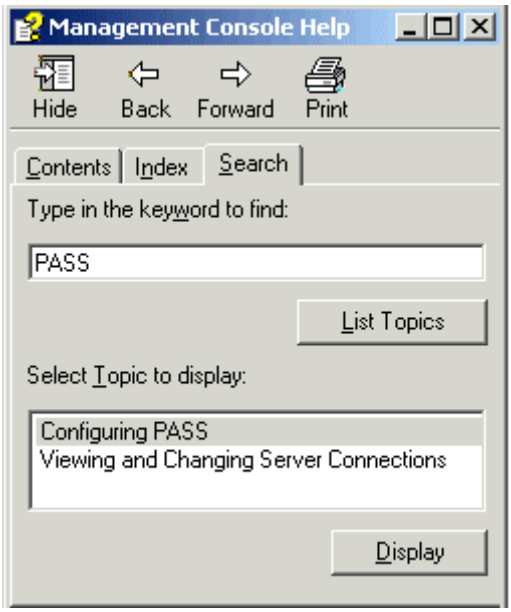


Figure 1-13 Help Search

Chapter 2 Install MCS Software

2-1 Install MCS Workstation

2-1.1 Prepare for MCS Workstation Installation

1. **Review** the *Release Notes* to obtain information regarding changes/known problems in the installation procedures
2. **Review** these installation instructions.
3. **Log on** as *administrator.*
4. **Verify** that MCS is not currently installed on the workstation. If MCS is installed, the Hard Drive must be reimaged to include baseline software requirements only. However, a patch is installed over existing software. Do not install MCS 6.4.4.3 on a computer that has another version of MCS software installed.
5. **Review** and **collect** the configuration parameters identified in the MCS Configuration Preparation Check List section. See your System Administrator for site specific details.
6. **Ensure** the installation disks are from the same version set and that all 5 disks (MCS Gold, #1a, #1b, #1c, #1d and #2) are present.
7. Prerequisites: All Microsoft and other commercial software must be installed and configured prior to MCS Installation. Prior to installation see the Release Notes for details.

2-1.2 Install MCS Workstation

The purpose of this chapter is to provide detailed instructions on installing MCS workstation software on a workstation.

NOTE

The default installation directory for MCS is "D:\MCS". This can be changed if needed during the disk #2 installation procedure.

NOTE

If possible, install and configure an MCS Gateway or Server before installing software on the Workstations, so that the AutoSetup Utility can be used.

- Required MCS workstation installation CDs for Release 6.4.4.3 are: MCS Gold, #1a, #1b, #1c, #1d, and #2. Refer to the Release Notes for all subsequent patch installation procedures.
- Install all programs as an Administrator of the local system.
- Accept all software licenses.
- Select the "Complete" Installation.
- Install all programs to the recommended directories unless directed otherwise by the System Administrator.
- Follow any instructions displayed during the installation.

2-1.2.1 MCS Workstation Installation Procedures - MCS Gold CD

1. **Insert** the *MCS Gold* CD into the CD drive.
2. In the Windows Explorer, **navigate** to the *Setup.exe* file on the CD.

3. **Double-click** *Setup*. Several messages appear and an *Installation Finished* window opens.
4. **Select** *Restart your computer now*.
5. **Remove** the CD.
6. **Log back** on to the computer (or the domain).

NOTE

After the Gold CD is installed, the Administrator password for the workstation will be changed to match the Administrator password for the domain. Other accounts with Administrator privileges are not affected.

2-1.2.2 MCS Workstation Installation Procedures - CD #1a

1. **Insert** the *MCS Installation CD #1a* into the computer CD drive.
2. From *Windows Explorer*, **navigate** to *Setup.exe* on the CD.
3. **Double-click** *Setup*. The MCS Install window opens and the installation begins.

NOTE

If .NET Framework is not part of the operating system, a message box will display to install it. Click 'Yes' to install. At the completion of the .NET installation, rerun 'Setup.exe' to continue the installation process.

4. The *ArcGIS Desktop Setup* window opens. **Select** *Next*.
5. Another *ArcGIS Desktop Setup* window opens. **Accept** the *License Agreement* and **select** *Next* again.
6. In the next *ArcGIS Desktop Setup* window, **choose** *Setup the License Manager Later*, and then **select** *Next*.
7. Another *ArcGIS Desktop Setup* window appears. **Choose** to set up the *ArcEditor*, and then **select** *Next*.
8. **Choose** a *Complete* installation and **select** *Next*. Software installation begins.
9. The next two windows ask you to select installation directories for ArgGIS and Python. In both cases, accept the default directories and **select** *Next*.
10. Another *ArcGIS Desktop Setup* window appears. Check your settings and **select** *Next* again.
11. **Select** *Finish*.
12. The *ArcGIS Setup Additional Installation Components* window opens. None of these components are required. **Ensure** that none of the Additional Installation Components are checked, and **select** *OK*.
13. **Ensure** that *Restart your Computer* is selected, and **select** *Finish*.
14. After restarting, log in to the computer. **Remove** *CD #1a* from the drive.

2-1.2.3 MCS Workstation Installation Procedures - CD #1b

1. **Insert** the *MCS Installation CD #1b* into the computer CD drive.
2. From *Windows Explorer*, **navigate** to *Setup.exe* on the CD.
3. **Double-click** *Setup.* The *MCS Install* window opens and the installation begins.
4. **Follow** the instructions on the screen (if any) until the message *Installation is complete!* appears.

5. **Select** *Restart your computer* option button and then **click** *Finish*. The workstation restarts.
6. After restarting, log in to the computer.
7. **Remove** the CD.

2-1.2.4 MCS Workstation Installation Procedures - CD #1c

1. **Insert** the *MCS Installation CD #1c* into the computer CD drive.
2. From *Windows Explorer*, **navigate** to *Setup.exe* on the CD.
3. **Double-click *Setup***. The *MCS Install* window opens and installation begins.
4. When the *Installation Finished* message appears, you may **continue** and **install** CD #2 without rebooting first. **Select** *Do not restart my computer* and then *Finished*.

2-1.2.5 MCS Workstation Installation Procedures – CD #1d

1. **Insert** the *MCS Installation CD #1d* into the computer CD drive.
2. From *Windows Explorer*, **navigate** to *Setup.exe* on the CD.
3. **Double-click *Setup***. The *MCS Install* window opens and installation begins.
4. When the *Installation Finished* message appears, you may **continue** and **install** CD #2 without rebooting first. **Select** *Do not restart my computer* and then *Finished*.

2-1.2.6 MCS Workstation Installation Procedures - CD #2

1. **Insert** *MCS Installation CD #2* into the computer.
2. From *Windows Explorer*, **navigate** to the *Setup.exe* on the CD.
3. **Double-click** *Setup*.exe. The *MCS Setup Destination Folder* window opens. The default installation directory is D:\MCS. Change this, if necessary, then **select** *Next*. The *MCS Setup Select Installation Type* window opens.

NOTE

If prompted to install the .NET software, select the Yes option.

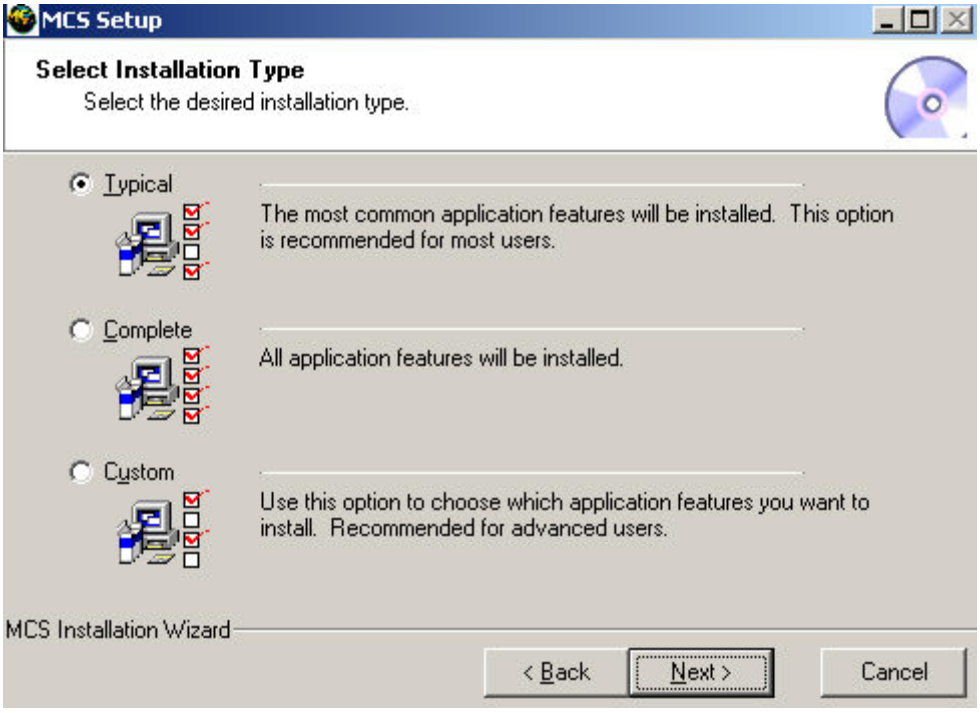


Figure 2-1 MCS Setup Window for Workstation – Select Installation Type

4. If a Typical or Complete installation is desired, **select** the appropriate installation type on the screen above and **click** *Next*. The *MCS Install* window then opens and this message appears: "MCS Client Disk 2 installation is complete!"
5. **Remove** Disk #2 from the cd drive. The MCS Workstation installation is now complete. Refer to "Configure MCS" for information about running the Management Console.

2-2 Install MCS Gateway

2-2.1 Prepare for MCS Gateway Installation

1. **Read** the *Release Notes.*
2. **Review** and **collect** the necessary configuration parameters identified in *the MCS Setup Select Installation Type* window.
3. **Ensure** the installation disks are from the same version set, and the MCS Gold, MCS #3, and C2PC disks are present.
4. **Review** the *Installation Security and Troubleshooting Notes* document in *the <drive letter>:\MCS\Documents\Admin\Installation Security and Troubleshooting Notes*. **Perform** the necessary post installation steps.

2-2.2 Install MCS Gateway Software

Prerequisites: All appropriate Microsoft and other commercial software must be installed and configured prior to Application Installation and Configuration. Additionally, if MCS software is installed on the Gateway, it must be removed before re-installing the software.
In order to install the Netscape Directory Services, the computer must belong to a Domain. Be sure that your domain membership has been properly configured before attempting to install the Gateway software.

- Required MCS gateway installation CDs for Release 6.4.4.3 are: MCS Gold and #3. Refer to the Release Notes for all subsequent patch installation procedures.
- Install all programs as an Administrator of the local system.
- Accept all software licenses.
- Select the "Typical" Installation.
- During installation, depending on your computer's configuration, you may be asked to accept software licenses (always accept) or to select a type of install for external products like Java (always select Typical). Install all programs to the recommended default directories unless directed otherwise by the System Administrator. For external products, accept all default options. Anything that's important to MCS will be changed later.
- Follow any instructions displayed during the installation.
- If installing MCS over a network, the folder containing the files MUST be mapped to a drive letter. MCS will not install correctly unless the files are read from a folder or drive with a drive letter assigned.

2-2.2.1 MCS Gateway Installation Procedures - CD's MCS Gold and #3

1. When building version 6.4.4.3 MCS Gateway, **complete** the procedures for installing the MCS Gold CD located at "MCS Workstation Installation Procedures - MCS Gold CD." Restart your computer and install CD #3.

2-2.2.2 MCS Gateway Installation Procedures - CD #3

1. **Insert** *MCS Install CD #3* into the computer.
2. From *Windows Explorer*, **navigate** to the *Setup.exe* on the *CD*.
3. **Double-click** *Setup.exe* and the *InstallShield Wizard* opens.

NOTE

If .NET Framework is not part of the operating system, a message box will display to install it. Click 'Yes' to install. At the completion of the .NET installation, rerun 'Setup.exe' to continue the installation process.

4. Once the installation starts, the *MCS Setup Select Installation Type* window opens.
5. The *Typical* installation option is the default.
6. **Select** the *Complete* option to install all components.
7. **Use** the *Custom* option to **choose** which options to install and which options not to.
8. The *Release Notes* recommend using the complete option.
9. When the *Installation Finished* window opens **select** *Restart Your Computer* and **click** *Finish*.

2-2.2.3 MCS Gateway Installation Procedures - C2PC 6.1.0

1. **Insert** *MCS Install CD C2PC 6.1.0* into the CD drive.
2. From *Windows Explorer*, **navigate** to the C2PC directory and **run** *Setup.exe* on the CD.
3. **Double-click** *Setup.exe* and the *InstallShield Wizard* opens.
4. Once the installation starts, **select** the appropriate information during the Wizard Setup process.

5. **Except** all license agreements and **follow** the instructions on the screen (if any) and refer to the *Release Notes* regarding any issues encountered.
6. When the C2PC Installation Completed window opens **select** *Restart Your Computer* and **click** *Finish*.
7. After restarting, log in to the computer having Administrator privileges.
8. Remove the CD.

2-2.2.4 MCS Gateway Installation Procedures – C2PC 6.1.0 P1

1. **Insert** *MCS Install CD C2PC 6.1.0 P1* into the CD drive.
2. From *Windows Explorer*, **navigate** to the directory and **run** *Setup.exe* on the CD.
3. **Double-click** *Setup.exe* and the *InstallShield Wizard* opens.
4. Once the installation starts, **select** the appropriate information during the Wizard Setup process.
5. **Except** all license agreements and **follow** the instructions on the screen (if any) and **refer** to the *Release Notes* regarding any issues encountered.
6. When the C2PC Installation Completed window opens, **select** *Restart Your Computer* and **click** *Finish*.
7. After restarting, log in to the computer having Administrator privileges.
8. Remove the CD.

2-2.2.5 MCS Gateway Installation Procedures – C2PC 6.1.0 P2

1. **Insert** MCS Install *CD C2PC 6.1.0 P2* into the CD drive.
2. From *Windows Explorer*, **navigate** to the directory and **run** Setup.exe on the CD.
3. **Double-click** *Setup.exe* and the *InstallShield Wizard* opens.
4. Once the installation starts, **select** the appropriate information during the Wizard Setup process.
5. **Except** all license agreements and **follow** the instructions on the screen (if any) and refer to the *Release Notes* regarding any issues encountered.
6. **Manually** configure Server Files and NRTS (i.e., confirm or set configuration items as needed).
   - **Configure** the computer server functions via the *Server Configuration Console*. **Refer** to Chapter 3, *Configure MCS* for more information about configuration procedures.
   - **Configure** the computer MCS settings via the *Client AutoSetup Console*. Note that the server and gateway does not have OrgID configuration options. This is no longer required on Servers and Gateways.
   - **Ensure** the *AutoSetup Utility* is running once the system is configured.
   - **Run** *MCSServer Startup* from the desktop shortcut.
7. When the installation is complete, **install** required Firewall software. **Refer** to the Security Administrator for installing Symantec Firewall.

Chapter 3 Configure MCS

3-1 Configure Workstations and Gateways Overview

CAUTION

The MCS Release Notes contain known issues and suggested workarounds. Follow the Release Notes when configuring MCS.

NOTE

It is recommended that the MCS Gateway or Server be configured before Workstations. Workstations will use the AutoSetup Utility to obtain their configuration information from the Gateway or Server.

This chapter provides detailed instructions for configuring MCS Workstations and Gateways.

The Army C2 Management Console is the tool used to configure an MCS Workstation. The Management Console is used to configure data connections and user roles for the various MCS applications, and to select an AutoSetup server. The AutoSetup Utility simplifies setup for MCS Workstations by letting them get their settings from a Server or Gateway.

Both the Army C2 Management Console and the Server Configuration Console are used to configure an MCS Gateway. Both are described in this chapter. Additional configuration instructions are provided for NRTS and PASS.

3-2 Determine/Adjust MCS Network Settings

The computer's Windows networking settings will be different, depending on whether the TOC LAN does, or does not, use DNS (Domain Name Service) and/or DHCP (Dynamic Host Configuration Protocol).

1. **Determine** (by consulting the System Administrator) whether the TOC network uses DHCP.
2. **Obtain** (by consulting the System Administrator) the hostname (if any) and (if DHCP is not being used) IP address for the MCS system being configured and any PASS Servers present in the TOC).
3. **Determine** (by consulting the System Administrator) whether the TOC LAN uses DNS.
4. **Open** the *Network Connections* Window (*Start*, *Settings*, *Network Connections*).
5. There may be several connections shown. The connection to the TOC LAN should be Active. **Right-Click** on the Active connection and select *Properties*.
6. **Open** the *Properties* window for *Internet Protocol (TCP/IP)*.
7. **Adjust** the settings:
   - If DNS is being used:
     a. **Add** the *IP* of the DNS Server to the *Primary DNS* area.
     b. **Close** the *TCP/IP* and *Network Adapter Card Properties* windows.
     c. **Ping** the *PASS Server* and the system being configured by Computer Name. If a reply is not received, correct the settings.
   - If DNS is **not** being used:
     a. **Remove** any entry in the Primary DNS area.

b. **Open** the *C:\Windows\System32\drivers\etc\Hosts* file.

c. **Add** the IP and Computer Name for the PASS Server (if present) and your system.

d. **Save** and close the file.

- If DHCP is being used:

  a. **Select** Obtain an IP Address Automatically.

- If DHCP is **not** being used:

  a. **Select** *Use the Following IP Address*.

  b. **Enter** the *IP address*, *Subnet Mask*, and *Default Gateway* you received from the System Administrator for this computer.

3-3 Configure MCS Gateway

3-3.1 Configure MCS Gateway Machine

Prerequisites: All required Microsoft and other commercial software and MCS software must be installed prior to MCS Gateway configuration. Additionally, the MCS Gateway must be connected to the TOC network.

Before attempting to configure a Gateway machine:

1. **Determine** (by consulting the System Administrator) whether the TOC network uses DHCP.
2. **Obtain** (by consulting the System Administrator) the hostname (if any) and (if DHCP is not being used) IP address for the MCS system being configured and any PASS Servers present in the TOC.
3. **Read** the release notes. The release notes are located on Installation Disk 2, in the top-level directory (<drive-letter>:\Release Notes.doc). If the MCS Configuration Preparation Check List was not completed prior to Gateway installation, complete it now before attempting the MCS Gateway configuration.

This section provides detailed instruction for configuring MCSServicesStartup, PASS and the Near Real-Time Server (NRTS) using the Server Configuration Console. Refer to the appropriate installation/configuration documents for the components not covered here.

NOTE

Starting MCSServicesStarup will not start the NRTS Server Console. NRTS is no longer starting as a service. The executable runs as a process.

1. From the desktop **select** *Start*, **select** *Programs*, *BCS*, *Server Config Console*. The *Server Configuration Console* will open after a brief splash screen.
2. **Select** an option from the tree on the left of the window. The settings for that service are displayed.
3. **Verify** or **enter** the configuration settings for the item.
4. **Click** the *Configure* button after completing the configuration settings to configure the item. Unless Configure is pressed, the changes you have made to configuration will not take effect.

NOTE

Before closing the Server Configuration Console, ensure that the settings are saved by clicking the Configure button.

NOTE

When any Configure button is clicked in the Server Configuration Console, an icon for the MCSServerStartup program appears on the Microsoft Windows desktop.

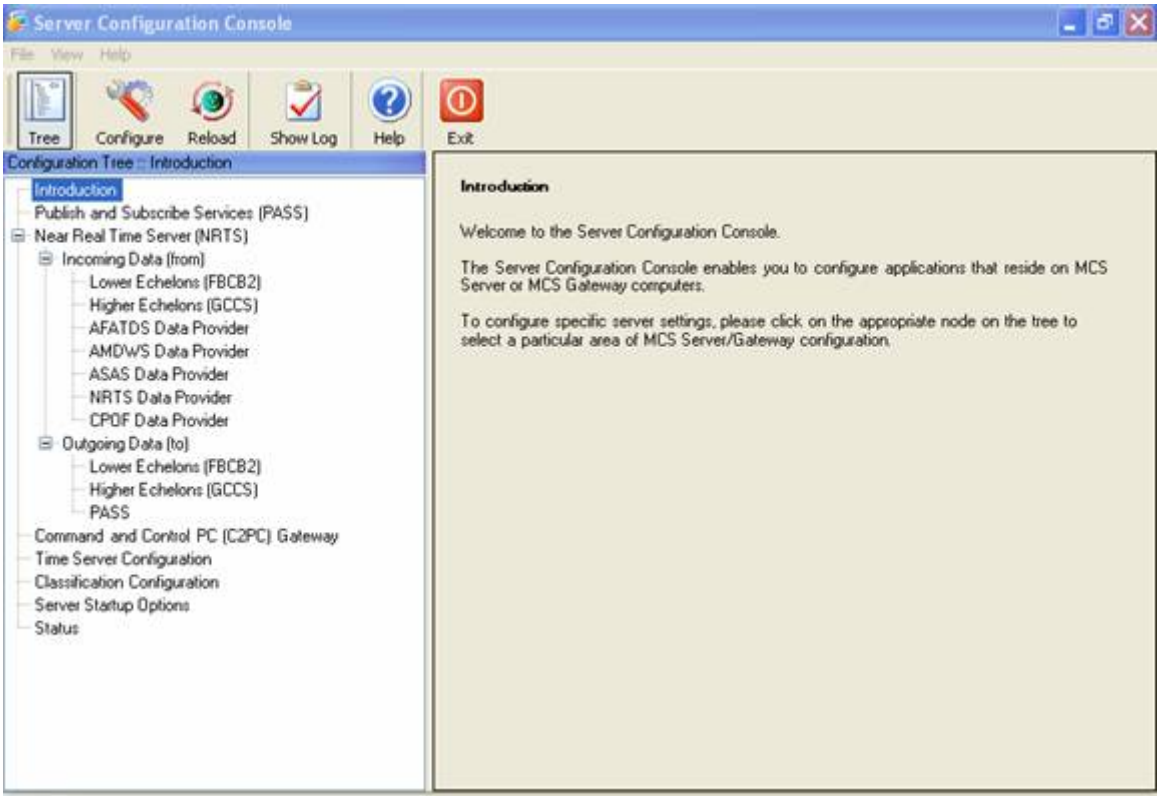


Figure 3-1 Server Configuration Console

3-3.2 Configure PASS Server

1. In the Server Configuration Console, **select** *Publish and Subscribe Service (PASS).* The *Publish and Subscribe Services PASS Settings* configuration area appears on the right side of the window.

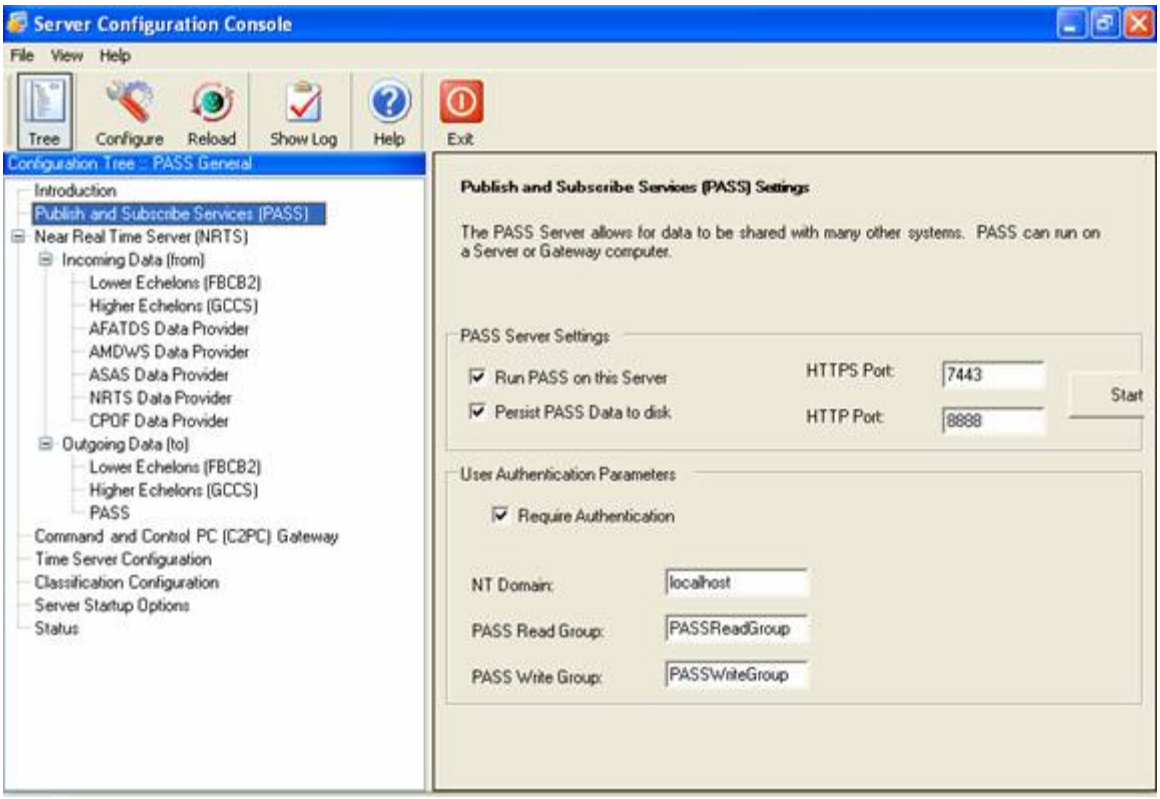


Figure 3-2 Server Configuration Console - Publish and Subscribe Services Selected

2. If the Gateway will run the MCS PASS Server, **check** the *Run PASS on this Server* checkbox. Otherwise, **confirm** that the checkbox is **not** checked, and **proceed** to the next configuration feature.
3. **Verify** the port number in the *HTTPS Port:* field. Normally, the default value does not need to be changed.

NOTE

Performance is improved if PASS Data is not saved to disk. However, it may be advisable for PASS to save its data to disk to facilitate CONOPS.

4. If persistence is required, **check** the *Persist PASS Data to disk* checkbox.
5. User Authentication will normally be required. **Obtain** the necessary information from the System Administrator, and **enter** it.
6. **Click** the *Configure* button to save the PASS Server settings.
7. If any changes have been made to PASS settings, **restart** PASS in order to apply them.

3-3.3 Configure NRTS

1. From the *Server Configuration Console*, **select** *Near Real Time Server (NRTS)*. The Configure NRTS Server configuration area appears on the right side of the window.

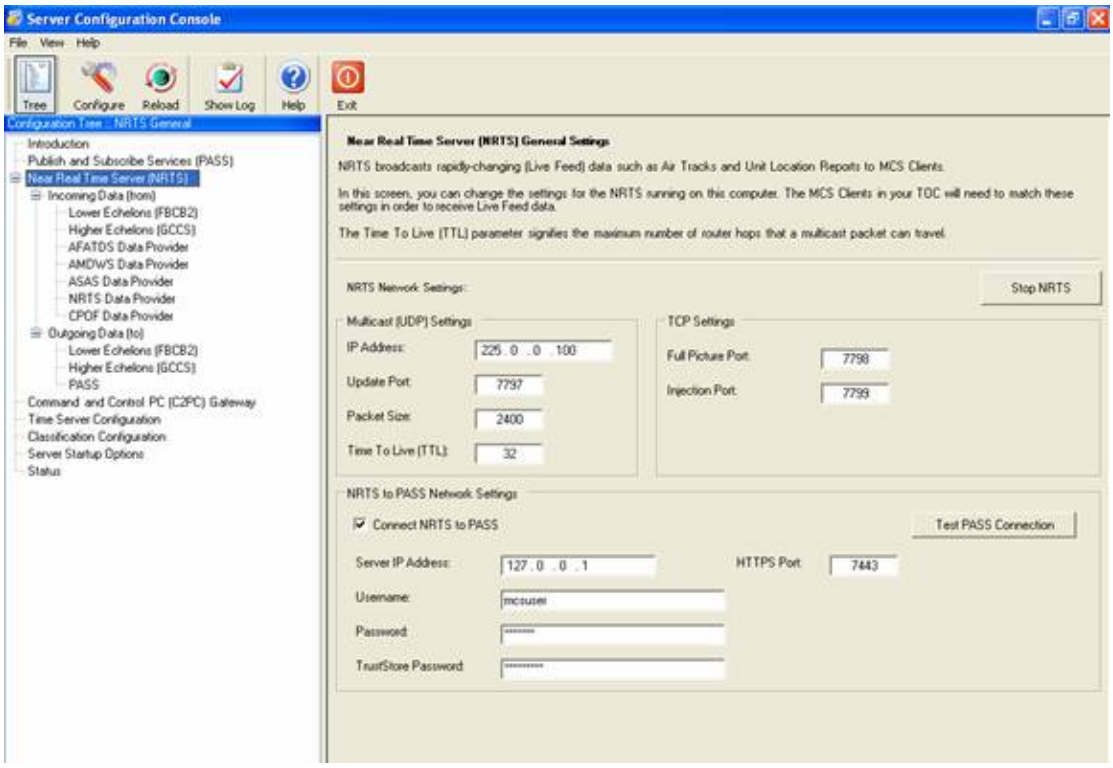


Figure 3-3 Server Configuration Console - Near Real Time Server (NRTS)

NOTE

Use the Start and Stop NRTS button to start and stop the NRTS data provider upon configuration.

2. In the *NRTS Network Settings* area, **change** the port numbers NRTS uses if necessary. Normally, there is no need to change these from the defaults unless there is a port conflict.
3. **Change** the address in the *IP Address* field if necessary. Normally, there is no need to change the default address unless there is a conflict.
4. The *Time to Live* option identifies the number of network hops allowed before a packet is dropped from the network. **Verify** the *Time to Live* setting or change it as desired.
5. **Click** the *Configure* button to save the NRTS settings.
6. If you have changed any NRTS settings, **restart** NRTS to apply them.
7. If NRTS will connect to PASS, **check** the *Connect NRTS to PASS* checkbox in the NRTS to PASS Network Settings area. **Verify** the default values in the *HTTPS Port, IP Address*, *User Name* and *Password* fields for correctness. If necessary, **change** the values in these fields.
8. **Use** the *Get Role* button to locate the assigned messaging role, i.e., MMCS-CP-HQ-CP-4-MP.
9. **Click** the *Configure* button to save the NRTS to PASS settings.
10. **Click** the *Test PASS Connection* button to confirm that your settings are correct.

3-3.4 Configure Incoming Data

The Incoming Data configuration for NRTS in the Server Configuration Console includes:

- Lower Echelons (FBCB2)
- Higher Echelons (GCCS)
- AFATDS Data Provider
- AMDWS Data Provider
- ASAS Data Provider
- NRTS Data Provider
- CPOF Data Provider

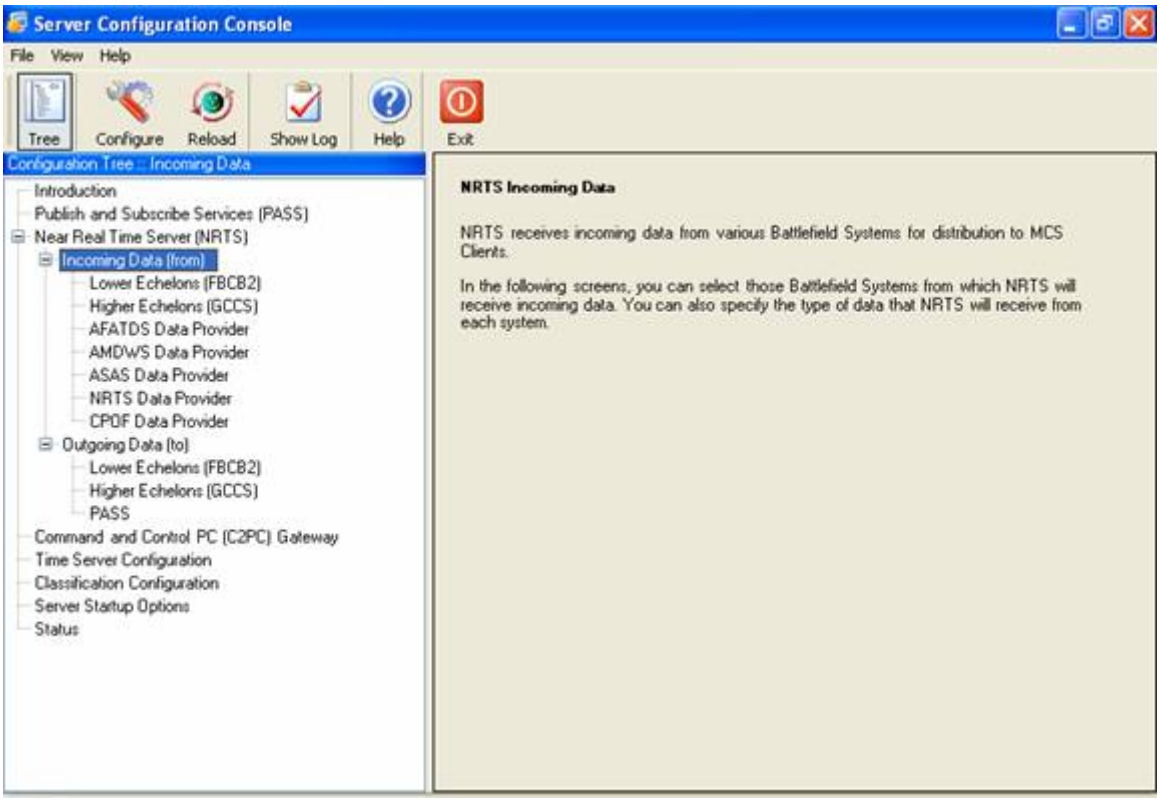


Figure 3-4 Server Configuration Console - Incoming Data (from)

3-3.4.1 Lower Echelons - FBCB2

If the lower echelons are equipped with FBCB2, NRTS will listen to their data. It must be determined whether the FBCB2 feed will come from the PASS or whether the NRTS will listen directly to the FBCB2 Multicast groups.

NRTS needs to know which PASS topics to listen to for FBCB2 data. PASS topic categories that FBCB2 is publishing to must be selected.

NOTE

The topic names include 'wildcards'. This means you do not have to pick every single topic individually. So, for example, if you check off "POS-RPT:FBCB2*", the NRTS will listen to every topic that starts with POS-RPT:FBCB2.

1. **Select** the *Lower Echelons (FBCB2)* branch of the Incoming Data (from) feature in the Server Configuration Console. The FBCB2 Incoming Data Settings configuration pane appears on the right side of the window.
2. **Click** on the appropriate radio button in the Receive FBCB2 data from area of the pane. The area below the radio button selections changes accordingly.
3. For the selected configuration area displayed, **select** the information to be shown.

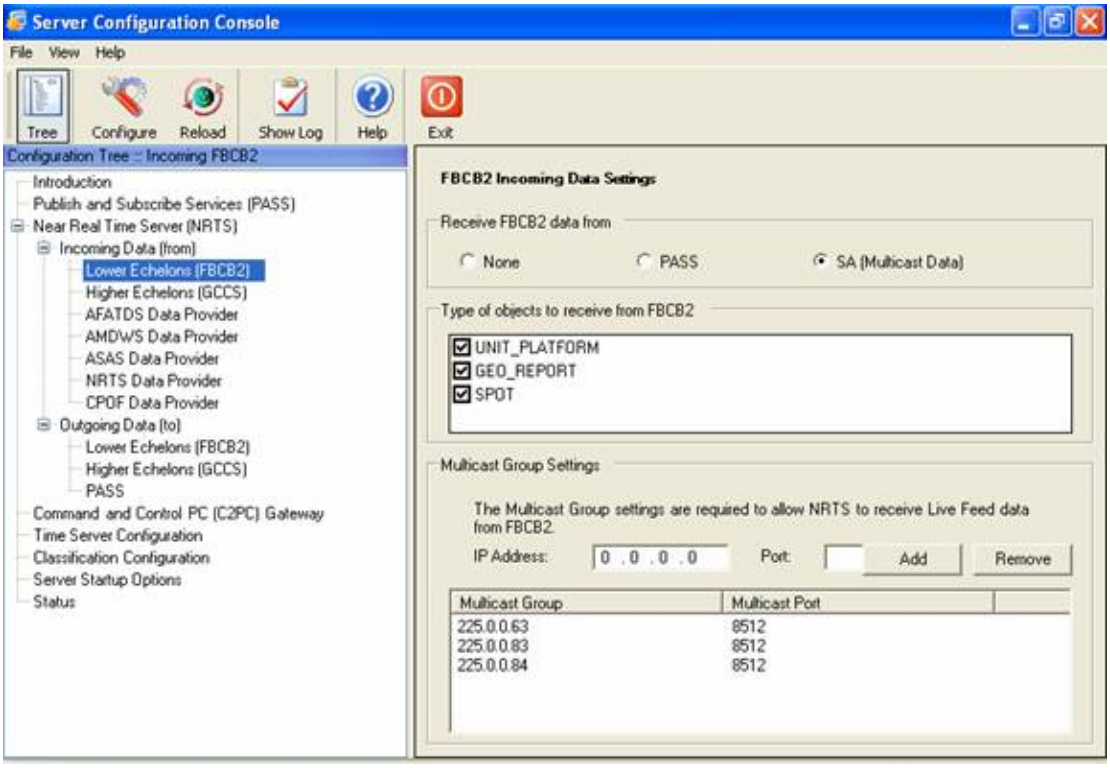


Figure 3-5 Server Configuration Console - Lower Echelons (FBCB2)

3-3.4.2 Higher Echelons - GCCS

NRTS can receive joint data from GCCS-A, and broadcast this data to the MCS Workstations. It must be determined whether the NRTS will receive GCCS-A information via PASS or whether it will listen to the C2PC Gateway.

If PASS is selected, NRTS needs to know which PASS server to listen to for GCCS-A data. **Select** the topic categories to add to the Live Feed.

NOTE

The topic names include 'wildcards'. This means you do not have to pick every single topic individually. So, for example, if you check off "POS-RPT:GCCS-A*", the NRTS will listen to every topic that starts with POS-RPT:GCCS-A.

1. **Select** the *Higher Echelons* branch of the *Incoming Data* feature in the *Server Configuration Console*. The *GCCS Incoming Data Settings* configuration options appear on the right side of the window.
2. **Click** on the appropriate radio button in the *Receive GCCS data from* area of the pane. The area below changes accordingly.
3. The port used by NRTS to receive GCCS (joint) data can be changed. Only modify this number if directed to do so by the System Administrator.

NOTE

The GCCS injector now displays the current box's IP address in the TMS Broker address text box if NRTS sends 127.0.0.1 to the Server Configuration Console.

4. **Click** *Configure* to save the Higher Echelons (GCCS) settings.

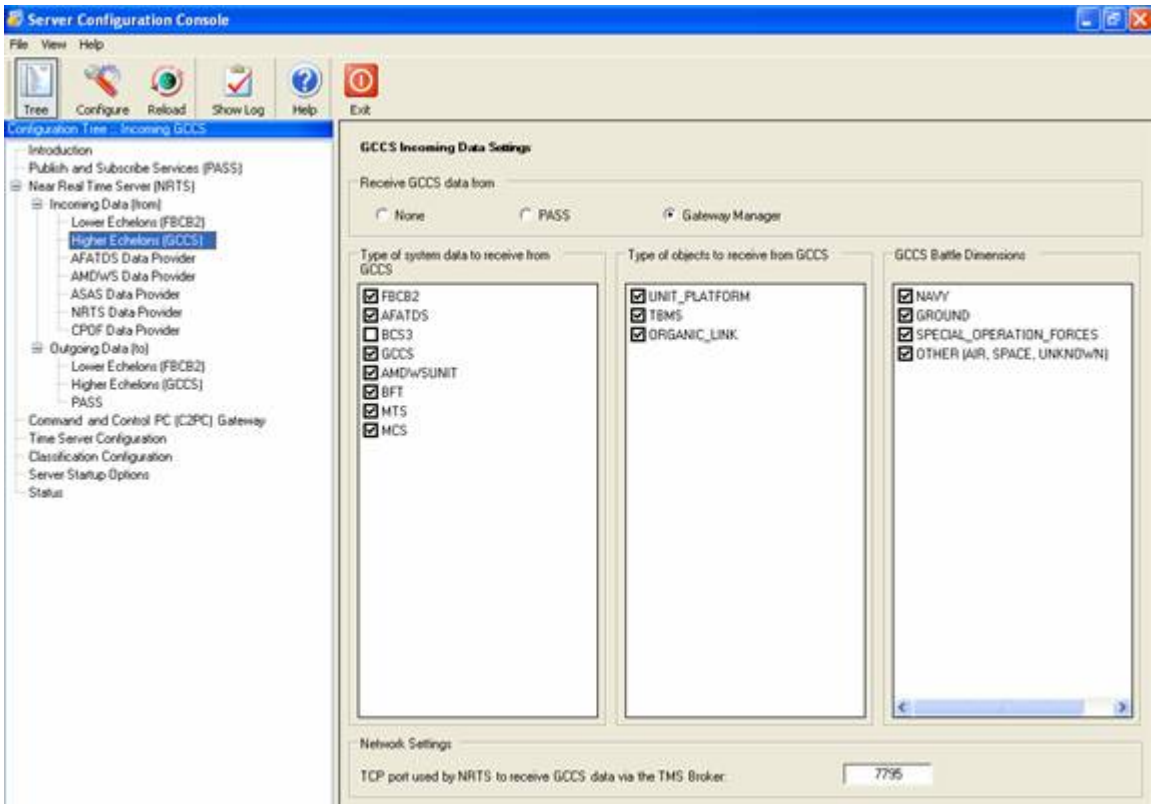


Figure 3-6 Server Configuration Console - Higher Echelons (GCCS)

3-3.4.3 AFATDS Data Provider

NRTS can receive AFATDS data either directly from AFATDS (using the AFATDS client, AXE) or from PASS.
If receiving data from AXE, NRTS needs to know the IP address of the AFATDS Client. A valid account, password, and classification level must be provided by the AFATDS operator.

NOTE

Some AFATDS workstations have two IP addresses. Make sure you are using the correct one for the AXE (it will be the same one that EMP clients use).

1. **Select** the *AFATDS Data Provider* branch of *Incoming Data* in the *Server Configuration Console.* The *AFATDS Incoming Data Settings* configuration pane appears on the right side of the window.
2. **Select** the appropriate choice in the *AFATDS Incoming Data Settings* area of the pane. The area below changes accordingly.
3. For each configuration area, **select** the data to show.
4. **Click** the *Configure* button to save the *AFATDS Data Provider* settings.

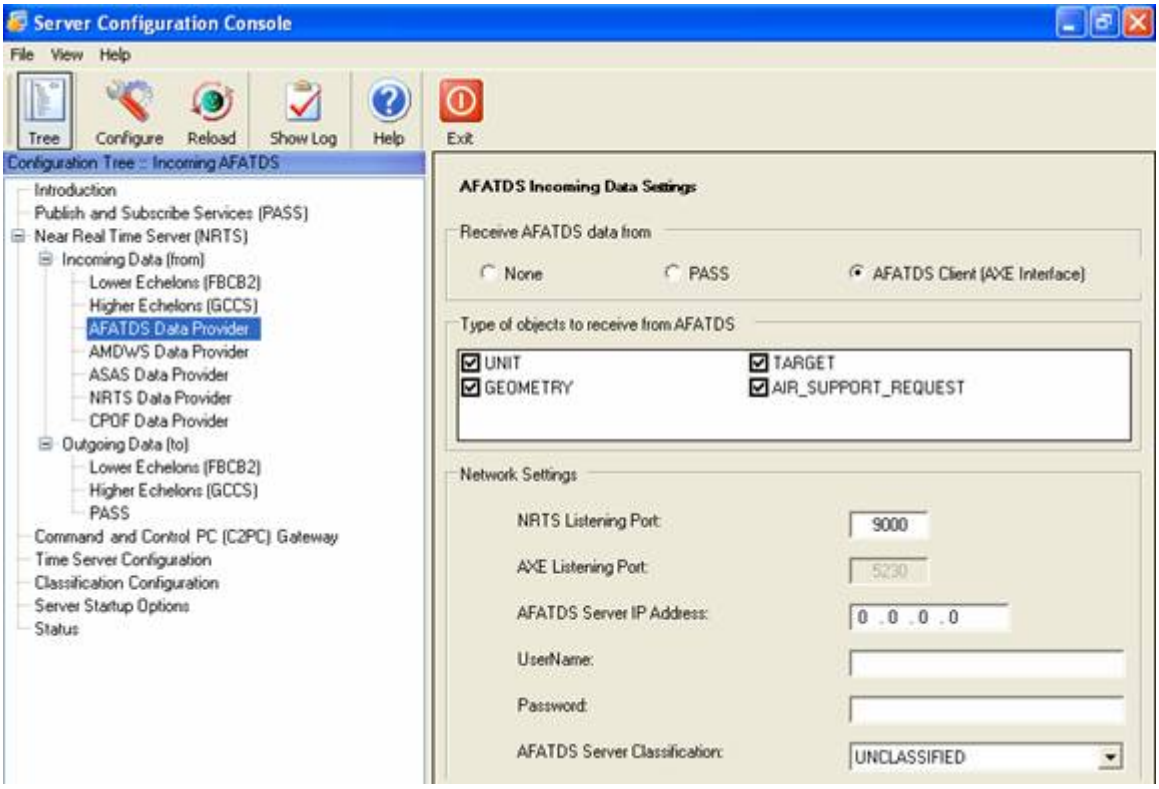


Figure 3-7 Server Configuration Console - AFATDS Data Provider

3-3.4.4 AMDWS Data Provider

1. **Select** *AMDWS Data Provider* from the *Server Configuration Console*'s *Incoming Data (from)* branch.
2. **Determine** and **select** whether the AMDWS feed will come from the PASS or whether the NRTS will listen directly to the AMDWS Client, or whether NRTS will receive no AMDWS data at all.

   If AMDWS data comes from PASS, NRTS needs to know which PASS topics to listen to for AMDWS data.

3. **Select** the PASS topic categories for AMDWS to publish.

NOTE

The topic names include 'wildcards'. This means you do not have to pick every single topic individually. So, for example, if you check off "AIR-TRK:AMDPCS*", the NRTS will listen to every topic that starts with AIR-TRK:AMDPCS.

If NRTS will not be receiving AMDWS data from the PASS, **connect** to the AMDWS client directly using the procedure in the following steps.

1. For example, **select** the *AMDWS Data Provider* branch of *Incoming Data* (from) in the *Server Configuration Console*. The Air Defense (AMDWS) configuration pane appears on the right side of the window.
2. **Click** on the appropriate radio button in the *AMDWS Incoming Data Settings* area of the pane. The area below changes accordingly.

3. For the selected configuration area displayed, select the necessary data to be shown.
4. **Click** *Configure* to save the AMDWS settings.

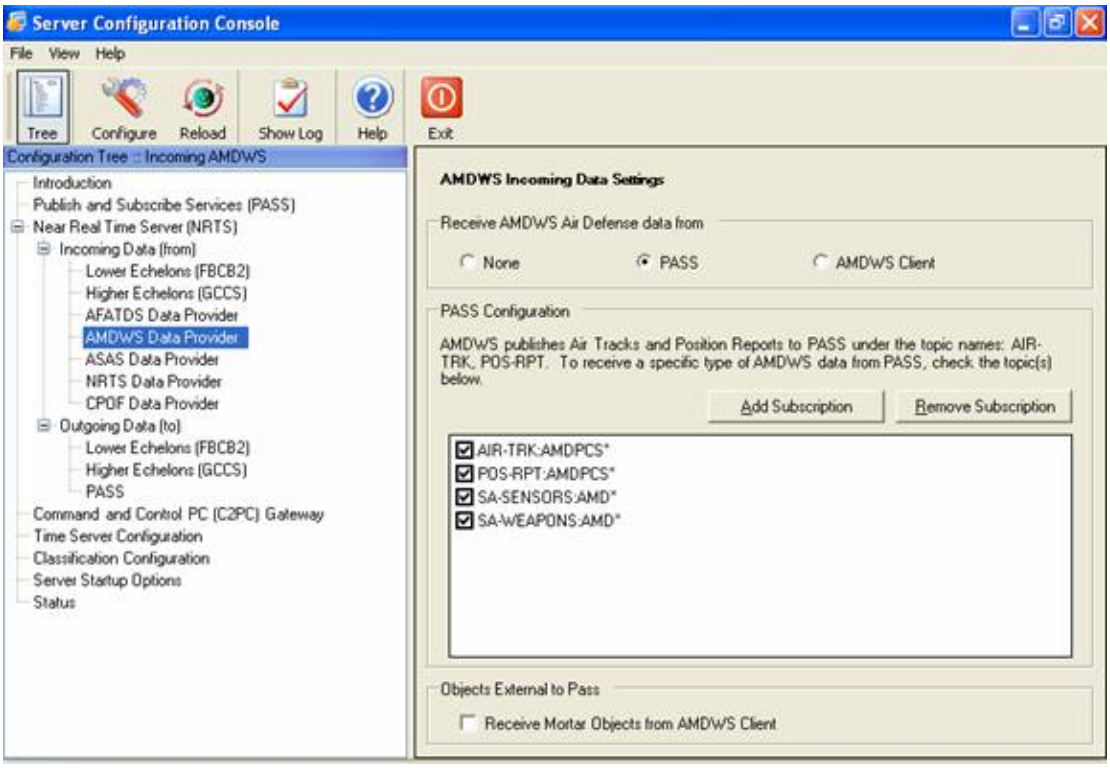


Figure 3-8 Server Configuration Console - AMDWS Data Provider

3-3.4.5 ASAS Data Provider

ASAS publishes the Correlated Enemy to PASS. Additional topics may also be published by ASAS. Selecting *PASS* will configure NRTS to receive the ASAS data from PASS. NRTS will then multicast the data to the MCS Workstations.

1. **Select** the *ASAS Data Provider* branch of *Incoming Data* in the *Server Configuration Console.* The *AFATDS Incoming Data Settings* configuration pane appears on the right side of the window.
2. **Select** the appropriate settings from those listed in the figure below.
3. **Click** the *Configure* button to save the Correlated Enemy (ASAS) settings.

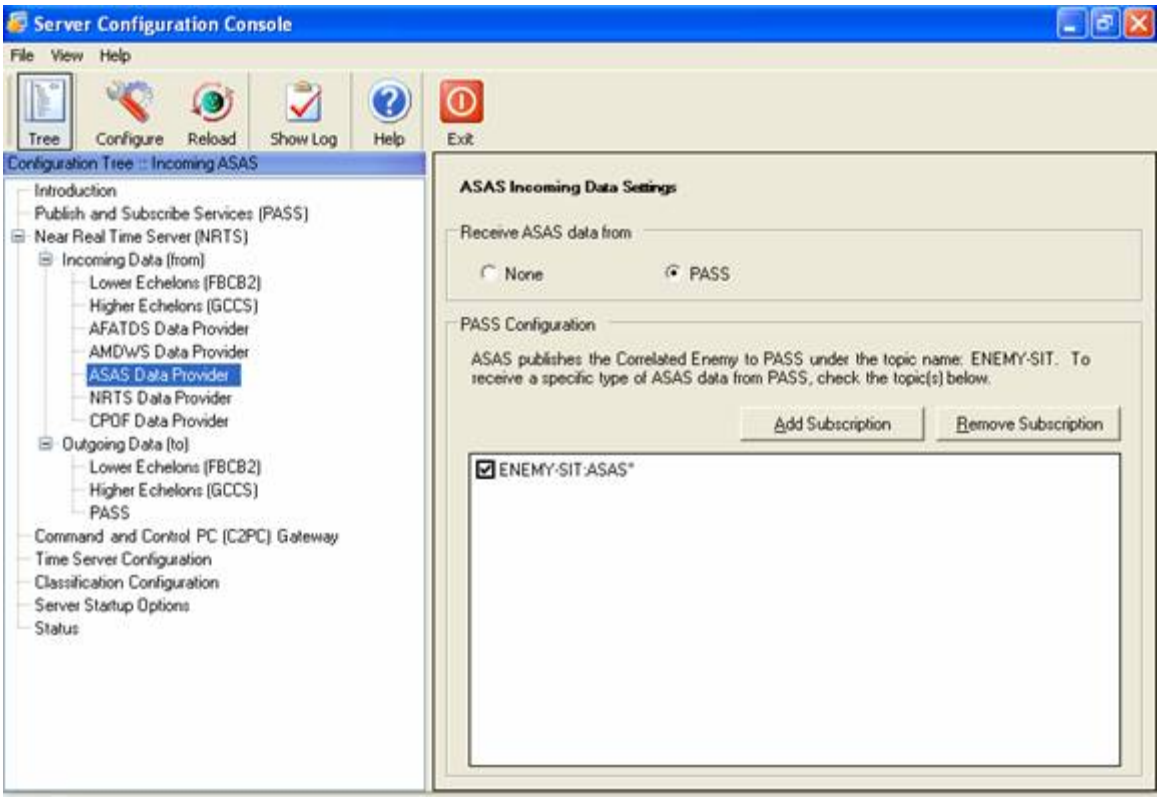


Figure 3-9 Server Configuration Console - ASAS Data Provider

3-3.4.6 NRTS Data Provider

1. **Select** the *NRTS Provider* branch of *Incoming Data* in the *Server Configuration Console.* The *NRTS Incoming Data Settings* configuration pane appears on the right side of the window.
2. **Use** the *Add* and *Remove* buttons to add or remove remote handlers as required.
3. **Click** the *Configure* button to save the NRTS settings.

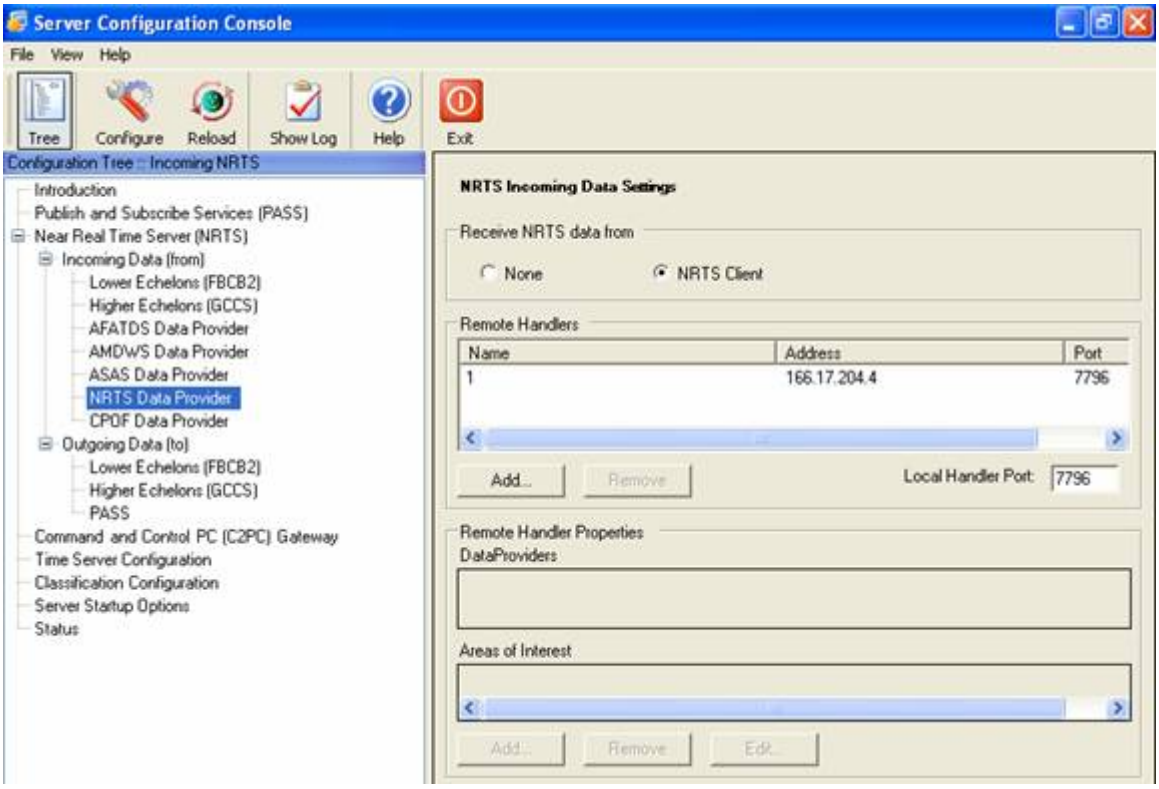


Figure 3-10 Server Configuration Console - NRTS Data Provider

3-3.4.7 CPOF Data Provider

1. **Select** the *CPOF Provider* branch of *Incoming Data* in the *Server Configuration Console.* The *CPOF Incoming Data Settings* configuration pane appears on the right side of the window.
2. **Use** the *Add Subscription* and *Remove Subscription* buttons to add or remove CPOF data from PASS as required.
3. **Click** the *Configure* button to save the CPOF settings.

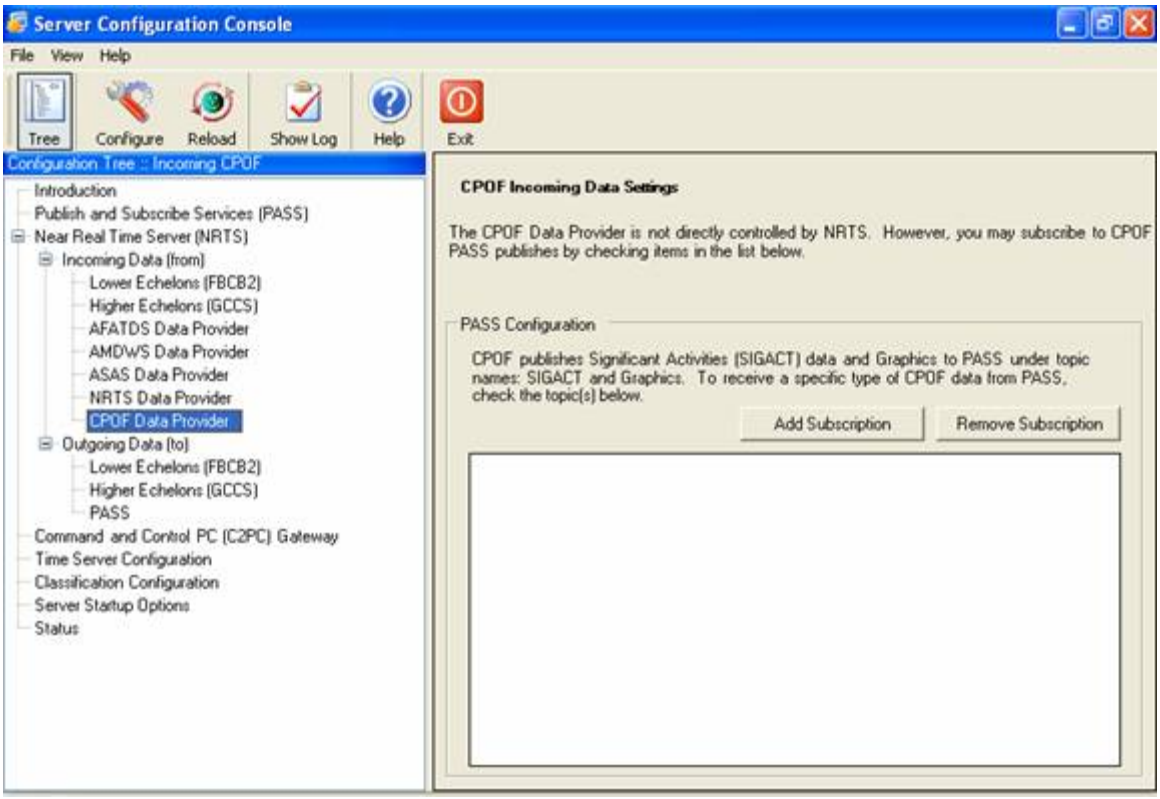


Figure 3-11 Server Configuration Console - CPOF Data Provider

3-3.5 Outgoing Data

Outgoing Data configuration in the Server Configuration Console includes:

- Lower Echelons - FBCB2
- Higher Echelons - GCCS
- PASS

3-3.5.1 Lower Echelons - FBCB2

You may want the NRTS to inject Live Feed data into the FBCB2 multicast groups.

1. **Select** the *Lower Echelons (FBCB2)* branch of *Outgoing Data (to)* in the *Server Configuration Console*. *FBCB2 Outgoing Data Settings* configuration options appear on the right side of the window.
2. **Check** the appropriate checkboxes in the *Type of objects to inject into FBCB2* area to what data types to inject.
3. Messages sent to FBCB2 systems need a Unit Reference Number as the sender. You can use either the same URN used for military messaging on your system, or another one that you enter here. Either:
   - **Check** the *Use Messaging URN* checkbox, or
   - **Enter** your URN in the *Originating URN* field in the *Messaging Settings* area.
4. **Complete** the *Multicast Group Settings* with the guidance of your System Administrator.
5. **Complete** the *UDP Settings* with the guidance of your System Administrator.

6. **Click** the *Configure* button to save the Lower Echelons (FBCB2) settings.

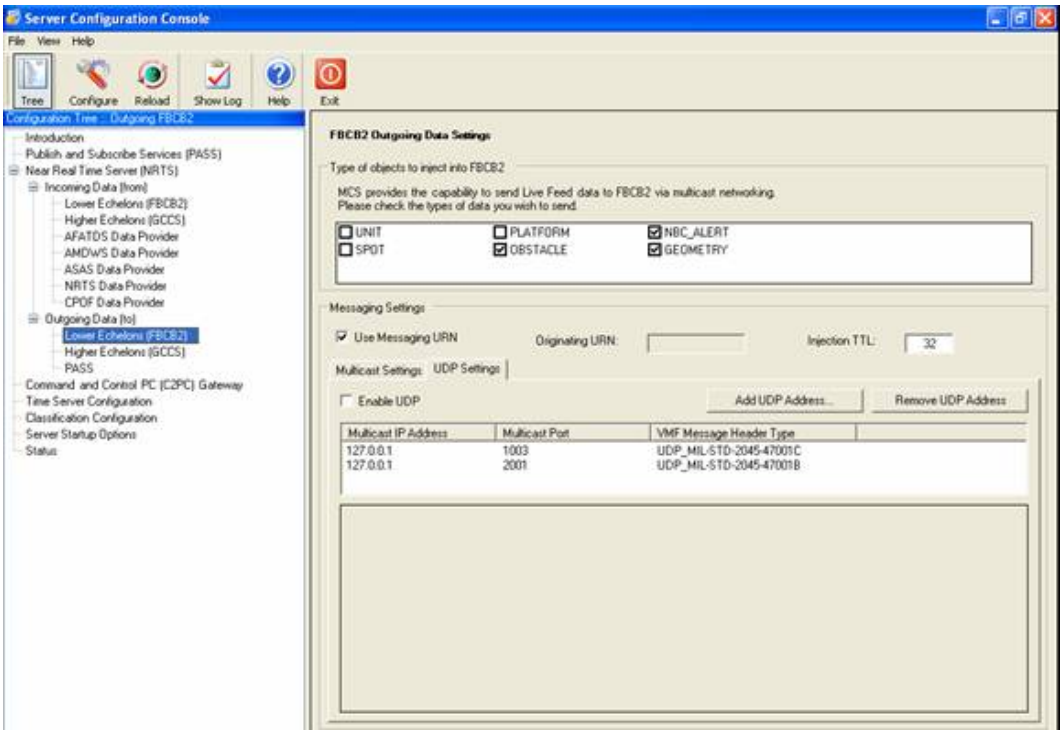


Figure 3-12 Server Configuration Console - Outgoing Data Lower Echelons (FBCB2)

3-3.5.2 Higher Echelons - GCCS

The Near Real Time Server can inject information into the C2PC Gateway, feeding data into GCCS to make it available to higher echelons. The Higher Echelons (GCCS) configuration controls what information is sent to the Gateway.

1. **Select** the *Higher Echelons (GCCS)* branch of *Outgoing Data* in the *Server Configuration Console*. The *GCCS Outgoing Data Settings* configuration appears on the right side of the window.
2. **Click** the appropriate checkboxes to select the types of data to send to higher echelons.
3. **Modify** *TMS Broker Settings* to connect to the C2PC Gateway. You can get the required settings from your System Administrator.
4. **Click** *Configure* to save the Higher Echelons (GCCS) settings.

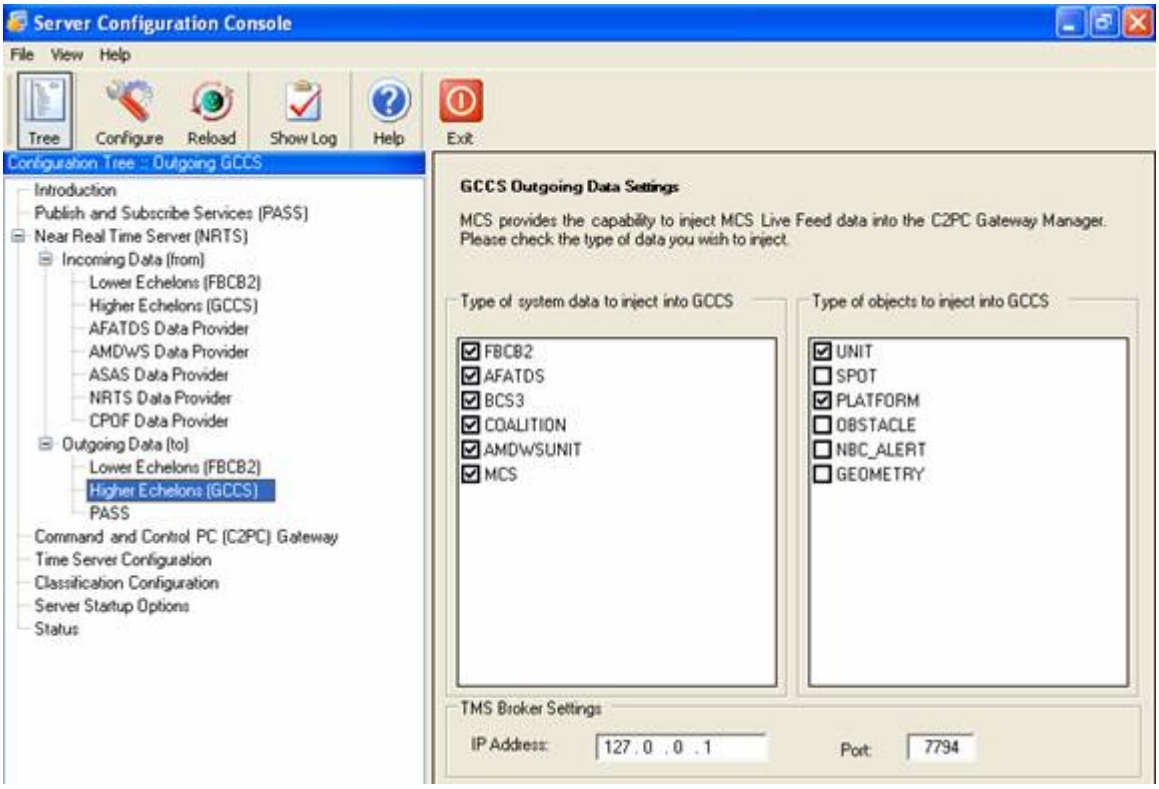


Figure 3-13 Server Configuration Console - Outgoing Data Higher Echelons (GCCS)

3-3.5.3 PASS

By default all Live Feed data is published to PASS so that non-MCS systems in the TOC have access to it.

NOTE

The Unit Identification becomes part of the topic name in PASS (for example POS-RPT:MCS:US/ARMY/DMAIN/10TH MTN). The Unit Identification may be changed based on the PASS naming convention SOP.

1. **Select** the *PASS* branch of *Outgoing Data* in the *Server Configuration Console*. *PASS* configuration appears on the right side of the window.
2. **Check** the appropriate checkboxes in the *PASS Outgoing Data Settings* area of the pane to select the type of data to inject.
3. You can choose to publish particular topics to be published to PASS.
4. **Click** *Configure* to save the PASS settings.

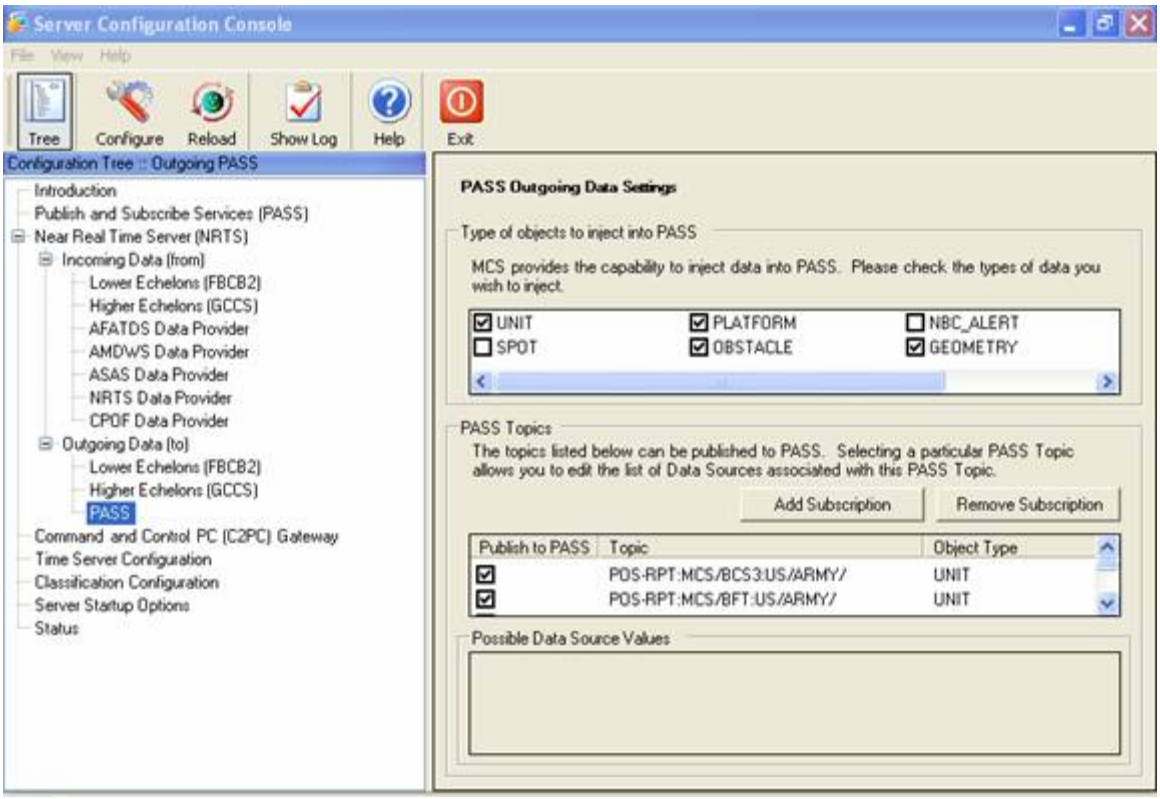


Figure 3-14 Server Configuration Console - Outgoing Data (to) PASS

3-3.6 Command and Control PC (C2PC) Gateway

C2PC is configured on the MCS Gateway using the Army C2 Management Console, exactly as it is for an MCS Workstation.

1. **Select** *Command and Control PC (C2PC)* in the *Server Configuration Console*. The *C2PC General Settings* information appears on the right side of the window.
2. **Make changes** in the C2PC General Settings section, as appropriate for your location.
3. **Click** *Configure* to save the Command and Control PC (C2PC) settings.

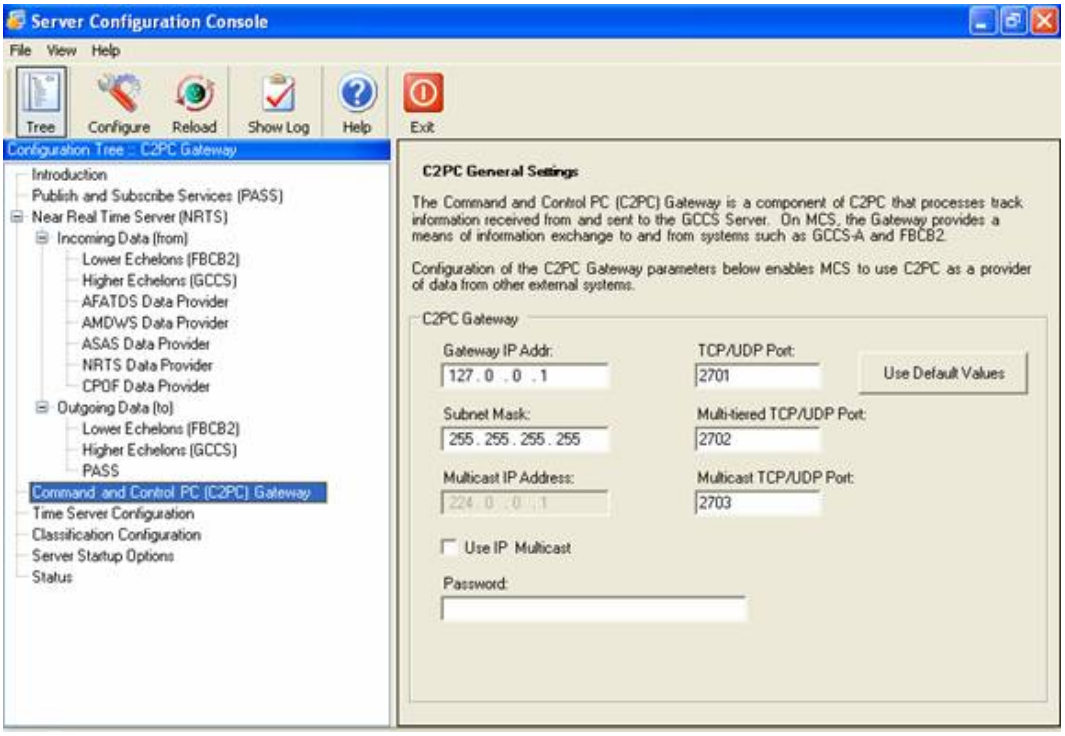


Figure 3-15 Server Configuration Console - Command and Control PC (C2PC) Gateway

3-3.7 Time Server Configuration

1. **Select** *Time Server Configuration* in the *Server Configuration Console*. The *Time Server Configuration Settings* information appears on the right side of the window.
2. **Check** the Enable *Time Synchronization on this computer* checkbox, if instructed to do so by your System Administrator.
3. Checking the *Enable Time Synchronization on this computer* checkbox, makes the *Time Sync Role* radio buttons available. **Select** the appropriate role: *Server, Slave Server or Client*. Then, **enter** the IP address of the server in the *Server IP Address* field.
4. **Click** *Configure* to save the Time Server Configuration settings.

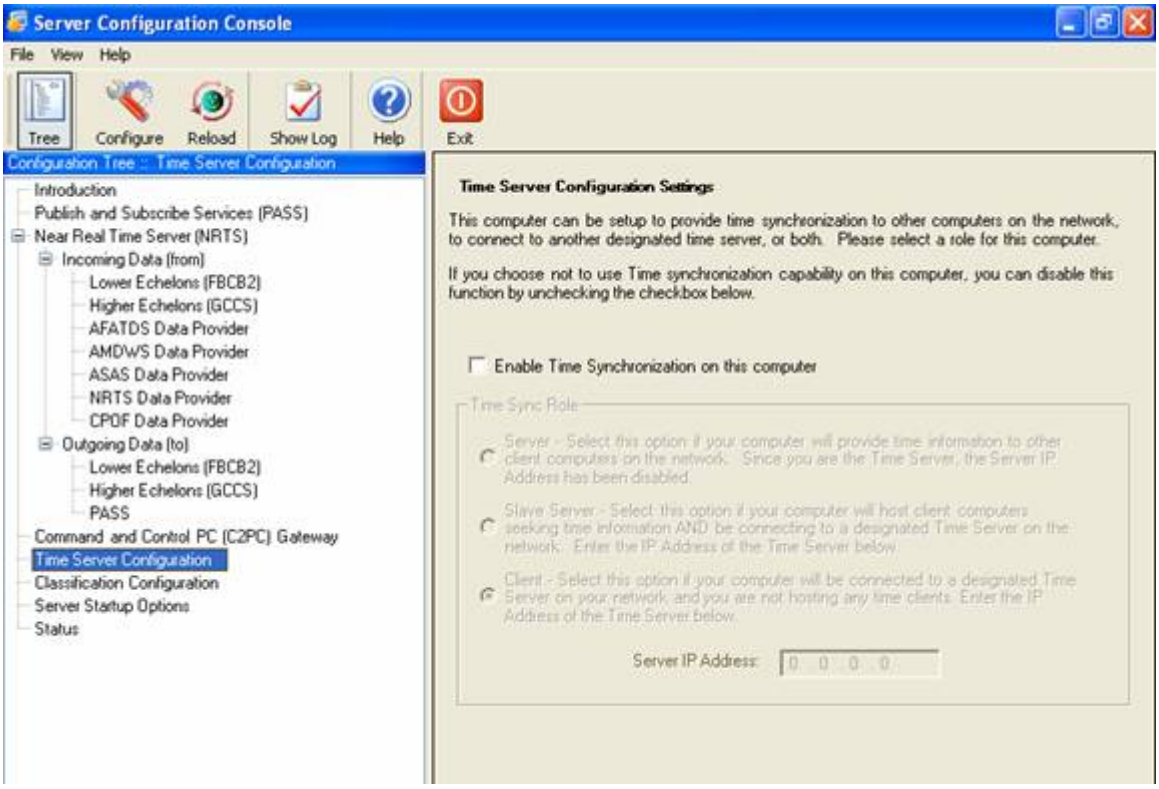


Figure 3-16 Server Configuration Console - Time Server Configuration

3-3.8 Classification Configuration

1. **Select** *Classification Configuration* in the *Server Configuration Console*. The Classification *Config* information appears on the right side of the window.
2. **Enter** the *Level Settings*, if instructed to do so by your System Administrator.
3. **Click** *Configure* to save the Classification Config settings.

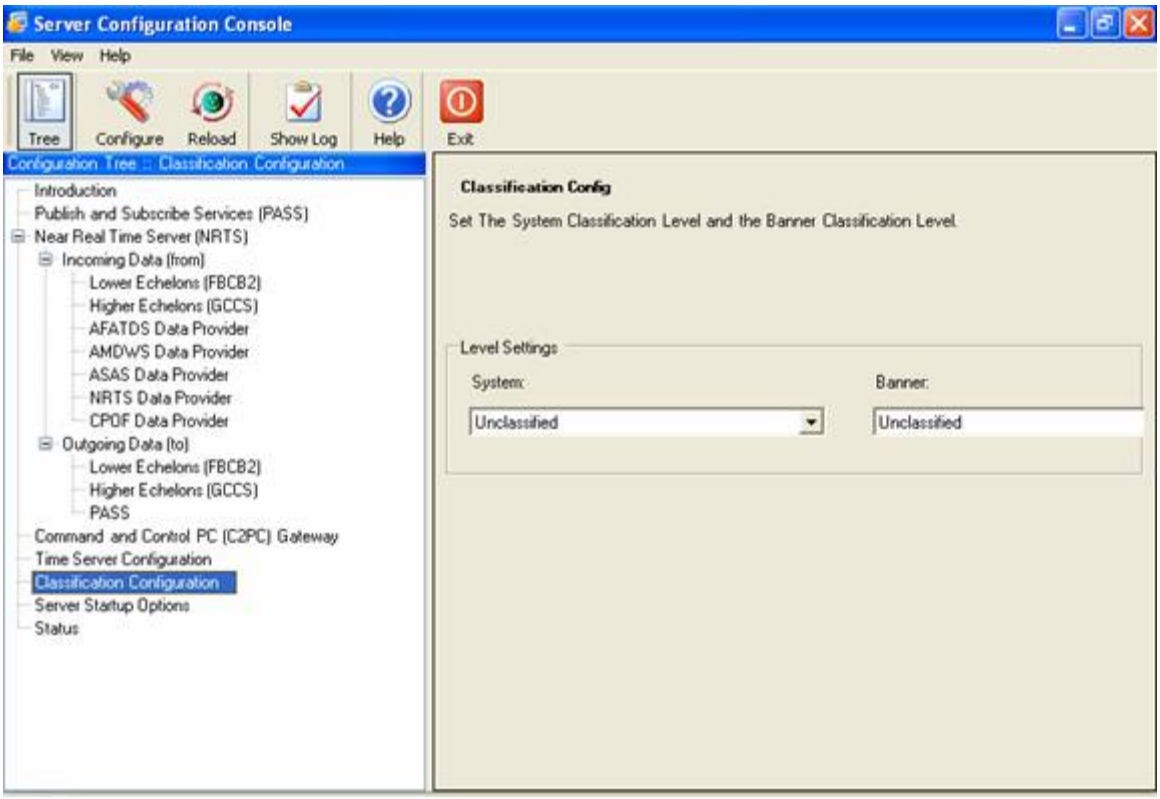


Figure 3-17 Server Configuration Console - Classification Configuration

3-3.9 Server Setup Options

NOTE:

The startup options here control only the listed services. Other MCS-related software (such as MIP and SQL Server) must be configured separately.

1. **Select** *Server Startup Options* feature in the *Server Configuration Console. Server Startup Options* appear on the right side of the window.
2. In the Server *Startup Options* area, **check** the first checkbox if you want MCS services to start automatically. **Check** the second checkbox if you want an icon for the startup program to appear on the Windows Desktop.
3. In the Automatic Startup Selection area, **click** the checkbox for each service you choose to start automatically.
4. **Click** *Configure* to save the *Server Startup Options* settings.

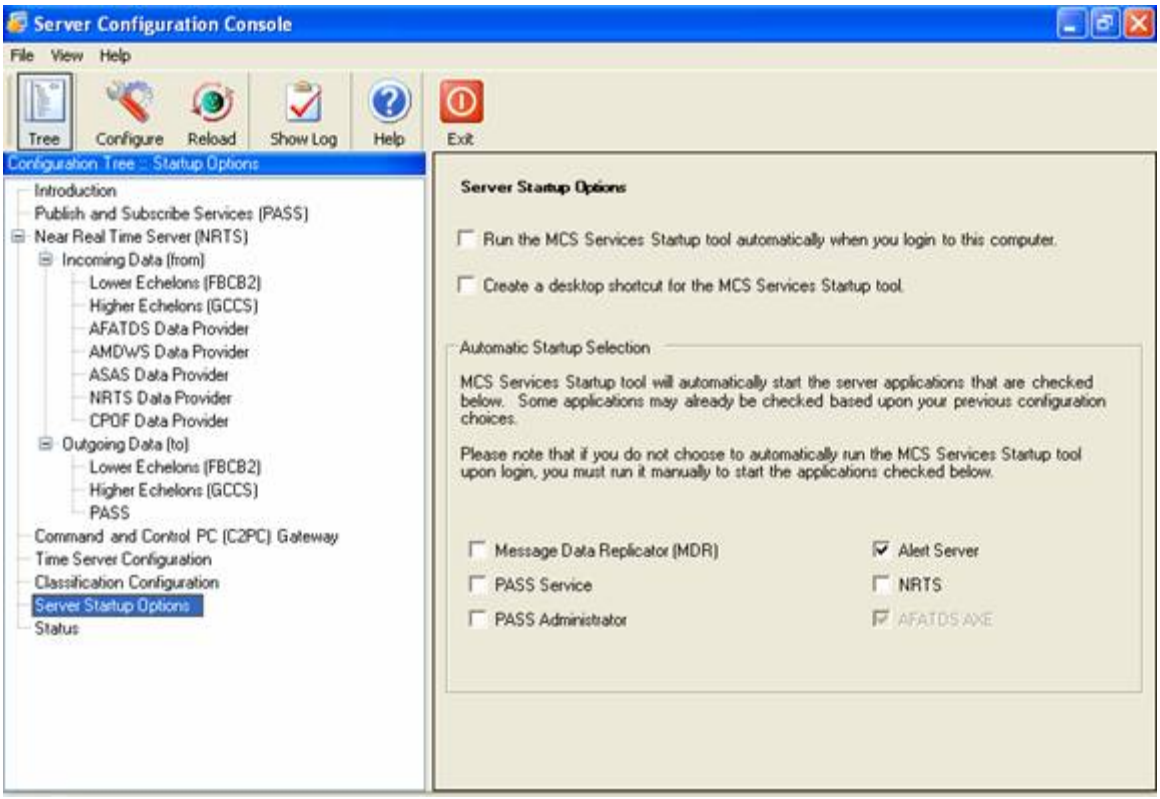


Figure 3-18 Server Configuration Console - Set Server Startup Options

3-3.10 Status of Server Functions

1. **Select** *Status* in the *Server Configuration Console.* The *Server Interfaces* list appears on the right side of the window.

NOTE

If NRTS or PASS is already running, you will need to restart them before any changes made in the *Server Configuration Console* take effect and are shown in the *Server Interfaces* listing.

NOTE

The Start, Pause and Stop buttons have temporarily been disabled on the Server Status screen. Functionality will be restored once NRTS is enabled to allow the Server Configuration Console to start and stop individual data providers.

2. **Confirm** that required server functions are working.

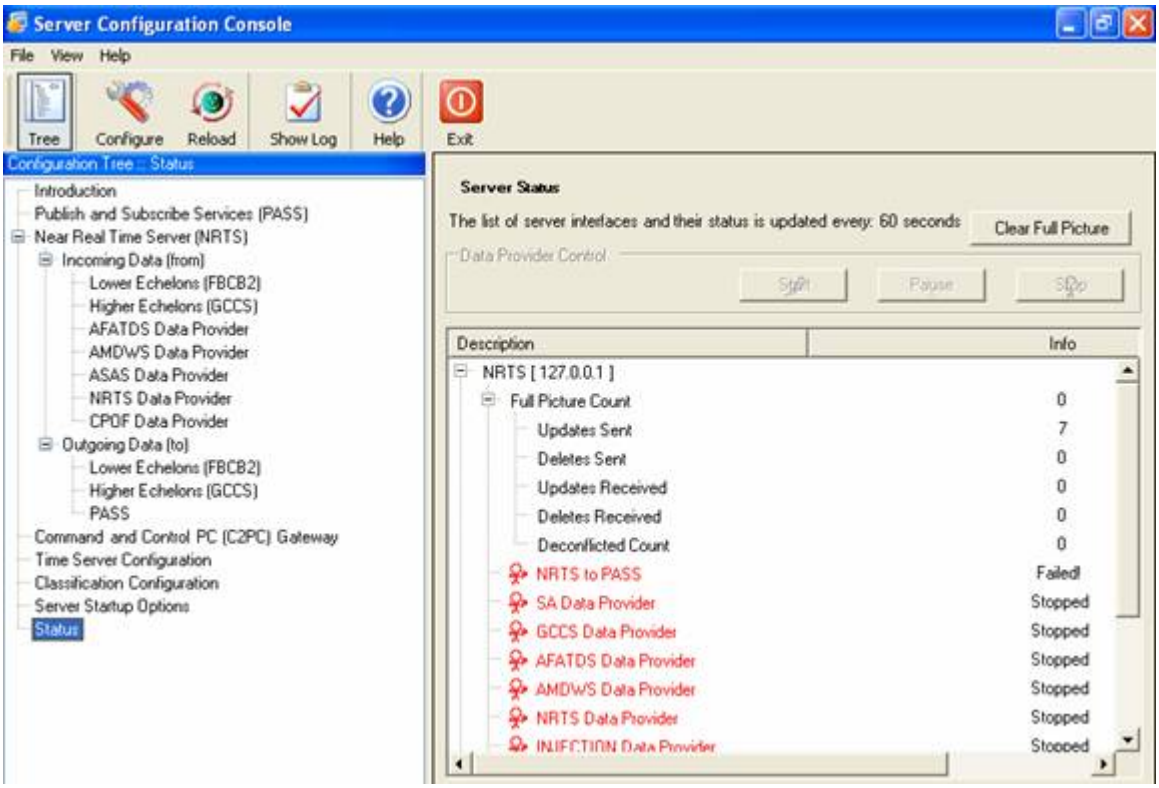


Figure 3-19 Server Configuration Console - Status

3-4 Additional MCS Gateway Configuration Tools

3-4.1 Install PASS Certificates

To connect to a PASS Server from any machine, the appropriate certificates must be installed on the connecting machine. Certificates from a PASS Server can be obtained either from a CD or another source. The truststore.jks is a file that contains certificates and should be found in the <drive letter>:*MCS**shared**certificates* directory. This is the truststore that should be used for all Java tools that reference the PASS Server.

For all other applications to work properly with the PASS Server, the certificate from the PASS Server, as well as the DoD certificate, need to be installed.

NOTE

Get the IP Address and exact directory location of where the certificates are stored on the PASS Server, or another medium (for example CD) that contains the certificate from the System Administrator.

3-4.1.1 Installing PASS Certificates

1. Using Internet Explorer, **navigate** to the address of the PASS Server. **Ensure** the port number is included at the end of the address (e.g., https://1.2.3.4:<port#>). A warning window opens.
2. **Click** *OK*. A Security Alert window opens.

3. **Click** the View *Certificate* button. A *Certificate* window will open.

Figure 3-20 Certificate Window

4. **Select** the *Install Certificate* button. Another *Certificates* window opens.
5. In the second *Certificates* window, **select** *OK*. The certificates are now installed.
6. If the certificate is contained on other media, **copy** the certificate to the <drive letter>:\MCS\shared\certificates directory.

3-4.1.2 Installing the Personal Information Exchange Certificate

The Personal Information Exchange certificate is installed using the Certificate Import Wizard. The following steps and figures will describe how to install the Personal Information Exchange certificates onto MCS system to allow access to the PASS services.

NOTE

Contact your PASS Administrator for a copy of the Personal Information Exchange file and the password for the private key.

1. **Locate** the *appropriate certificate* on your MCS System. **Double-click** the *certificate* to start the Certificate Import Wizard.

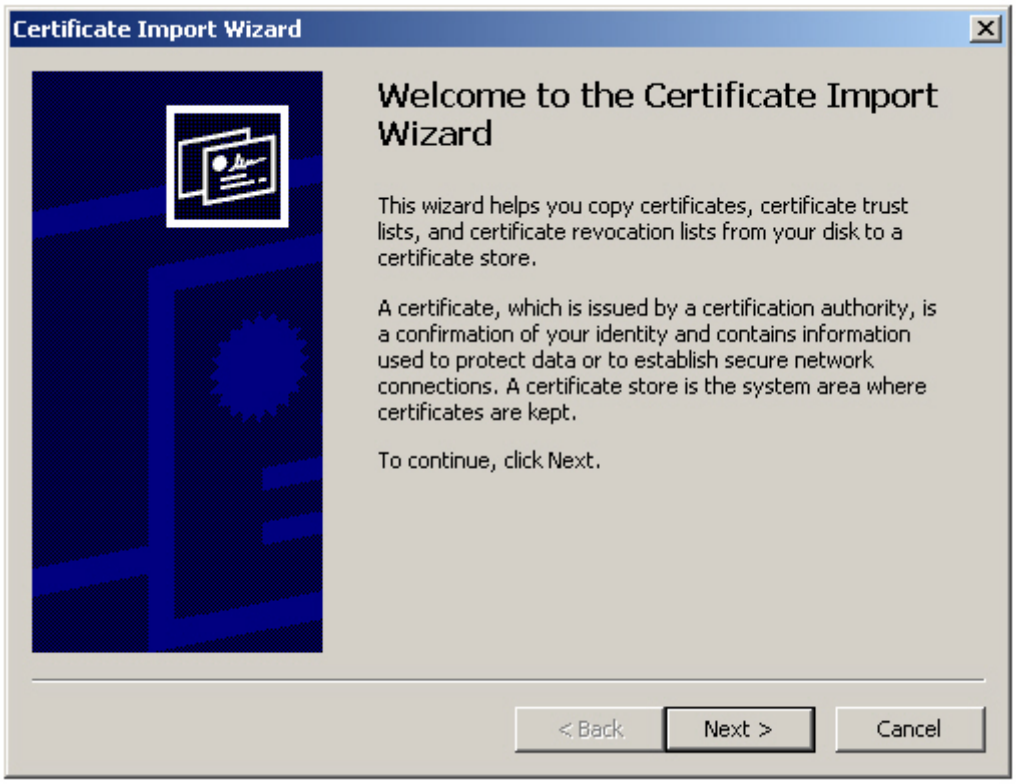


Figure 3-21 Certificate Import Wizard

2. **Click** the *Next* button, the *File to Import* window opens.

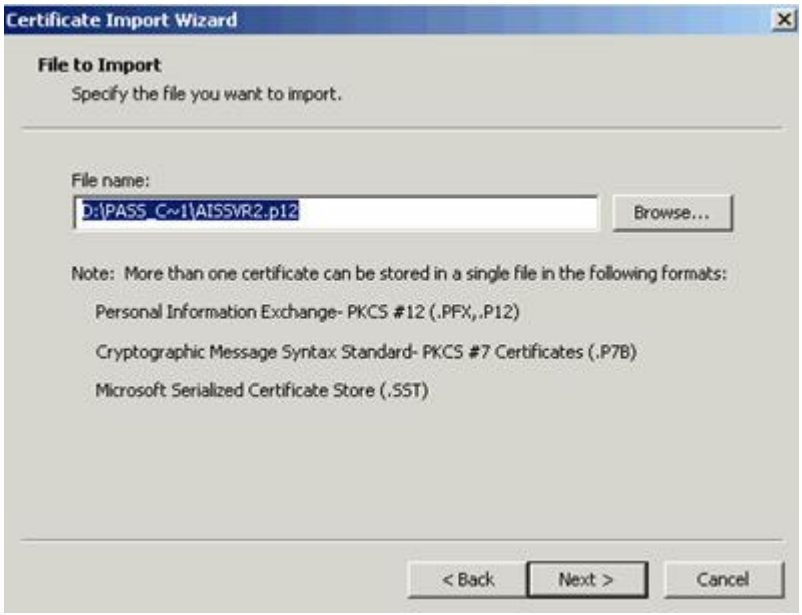


Figure 3-22 Certificate Import wizard screen

3. **Specify** the name of the certificate you want to import. **Click** *Next* to continue, the *Password* window will open.

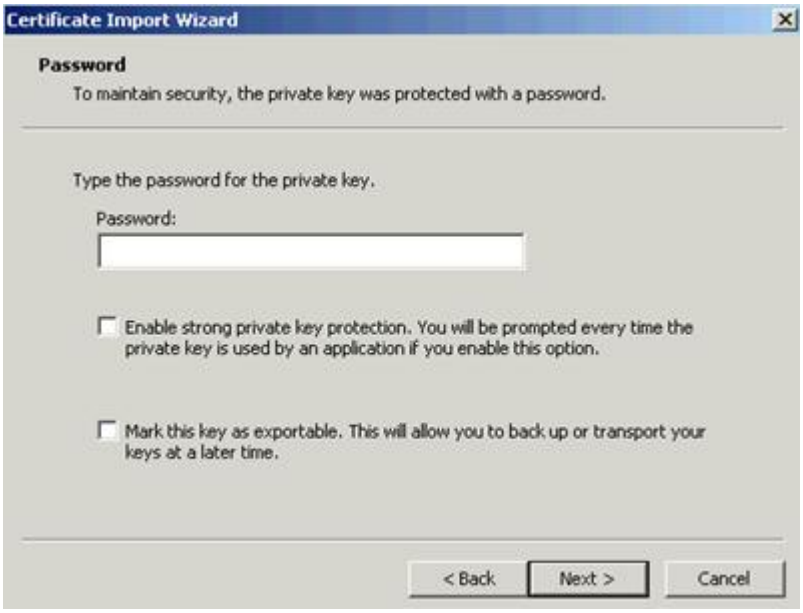


Figure 3-23 Password entry window

4. **Click** *Next* to continue, the *Certificate Store* window opens.

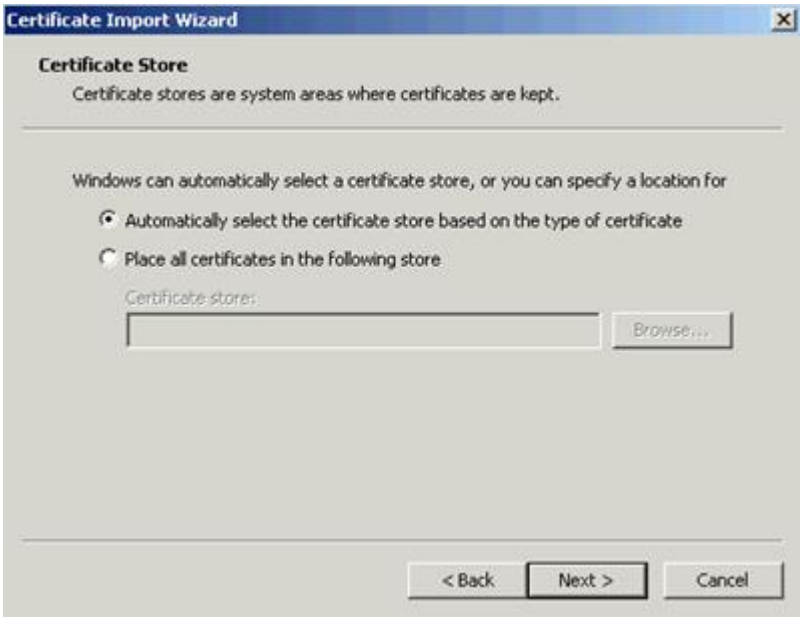


Figure 3-24 Certificate Store window

5. **Select** *Automatically select the certificate store based on the type of certificate*. **Click** *Next* to continue. The setting you selected will be displayed.

Figure 3-25 Certificate setting

6. **Click** the *Finish* button to complete the import. A message displays indicating that the import was successful.

Figure 3-26 Certificate import successful window

3-4.1.3 Installing DoD Certificates for PASS

1. In Windows Explorer, **navigate** to the <drive letter>:\MCS\shared\certificates directory.
2. **Right-click** on the “dod class 3 ca-7.cer” certificate and **select** Install Certificate. This will open the Certificate Import Wizard.

Figure 3-27 Certificate Import Wizard Welcome Screen

3. **Click** *Next*. The *Certificate* Import *Wizard* window opens.

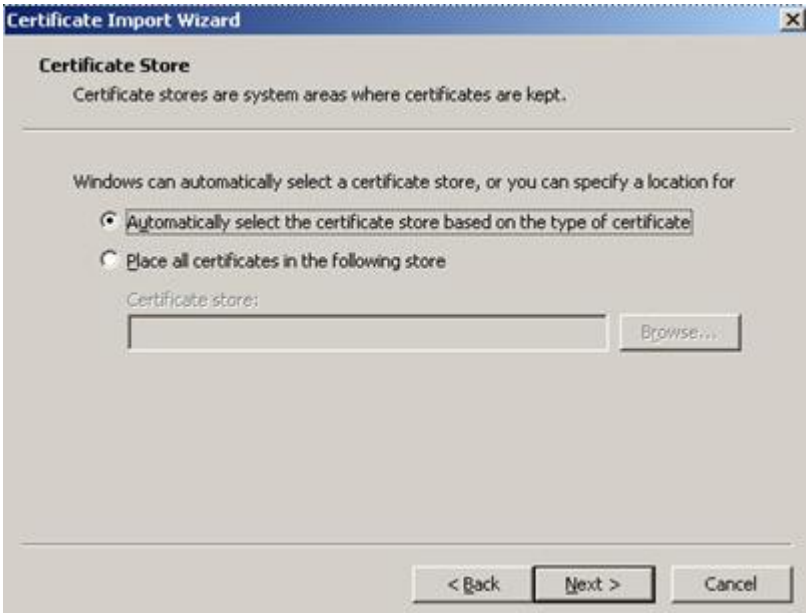


Figure 3-28 Certificate Import Wizard Window

4. **Click** *Next*. The Completing *the Certificate Import Wizard* window opens.

Figure 3-29 Completing the Certificate Import Wizard Window

5. **Click** on *Finish*. The *Certificate Import Wizard* confirmation window opens. **Click** *OK*.
6. **Perform** Steps 2-5 for the "*dod class 3 root ca.cer"* certificate as well.

3-4.2 Manually Starting the PASS Server

1. **Click** on the *Start* button, then **select** *Programs*, *BCS*, *Start PASS*.

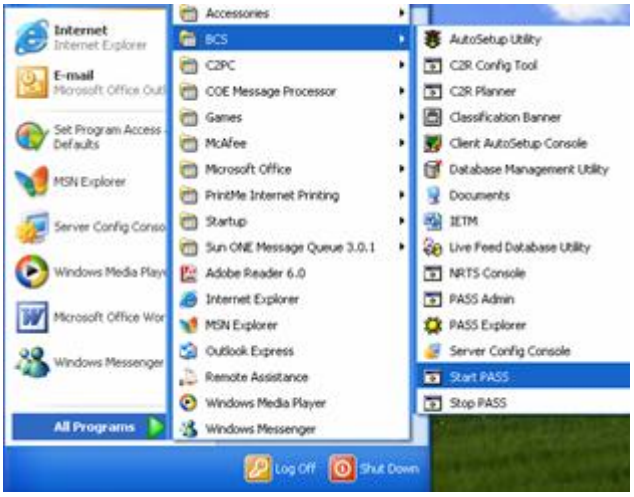


Figure 3-30 PASS Start or Stop

3-4.3 Manually Stopping the PASS Server

1. **Click** on the *Start* button, then **select** *Programs*, *BCS*, *Stop PASS*. See the above figure.

3-4.4 Configure the PASS Server using the PASS Administration Console

NOTE

The PASS Administration window opens automatically when a Server or Gateway that is running PASS is started. Step 1 should be followed if the program must be restarted.

1. **Click** on the *Start* button, then **select** *Programs*, *BCS*, *PASS Admin*.
2. In the Pass Administration window, **select** the Login tab.

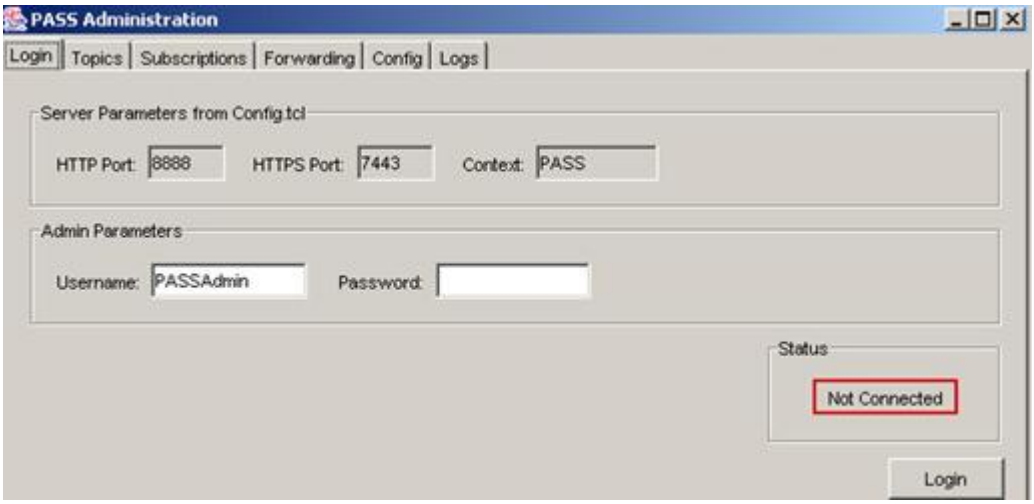


Figure 3-31 PASS Administration Window

3. **Click** *Login* on the *Login* tab. The status changes to Connected, and the frame around it turns green.

NOTE

Closing the PASS Administration window does not stop the PASS Server.

3-4.5 Topics Tab

1. **Click** on the *Topics* tab. The Topics view is presented. The left pane lists topics, and the right pane lists the contents of the selected topics.

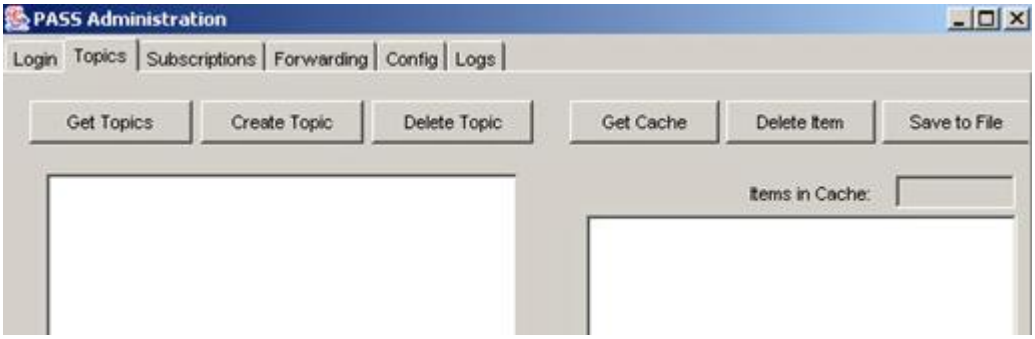


Figure 3-32 Pass Administration –Topics Tab

3-4.5.1 Get Topic List

1. To **get** a list of the currently available topics, **click** the *Get Topics* button and the list of available topics will be displayed in the left pane.

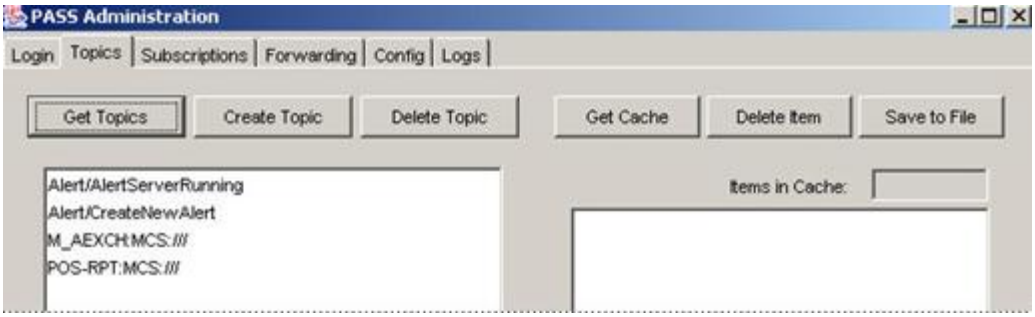


Figure 3-33 PASS Administration - Available Topics

3-4.5.2 Create a Topic

1. To **create** a topic, **click** the *Create Topic* button. The *Create Topics* window opens.

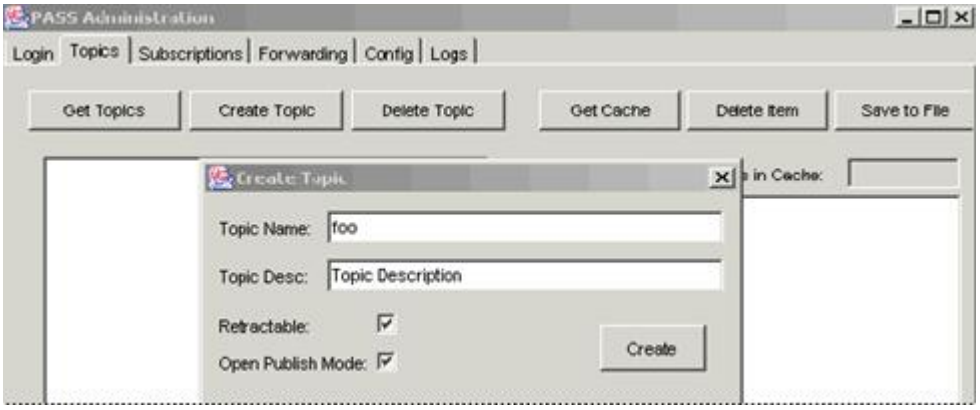


Figure 3-34 PASS Administration - Create Topics

2. **Enter** the name of the topic in the *Topic Name* area.
3. Optionally, **describe** the topic in the *Topic Desc*. area.
4. If *Retractable* is checked, you will have the option of retracting (removing) the topic later.
5. If Open Publish Mode is checked, this enables any BFA to publish to the topic. Without this option set, BFAs can subscribe to the topic but are restricted from publishing to the topic.

NOTE

See the unit SOP for Topic naming conventions.

For example:

- Topic with no subtopics - GRAPHICS:MCS:US/ARMY/3CORPS
- Topic with one (1) subtopic named SUBTOPIC1 - GRAPHICS/SUBTOPIC1:MCS:US/ARMY/3CORPS
- Topic with one (1) subtopic named SUBTOPIC1 that itself has a subtopic named SUBTOPIC1A - GRAPHICS/SUBTOPIC1/SUBTOPIC1A:MCS:US/ARMY/3CORPS

3-4.5.3 View Contents of a Topic

1. To view the contents of a topic, **select** the topic. **Click** the *Get Cache* button. The topic contents are displayed in the right side of the window.

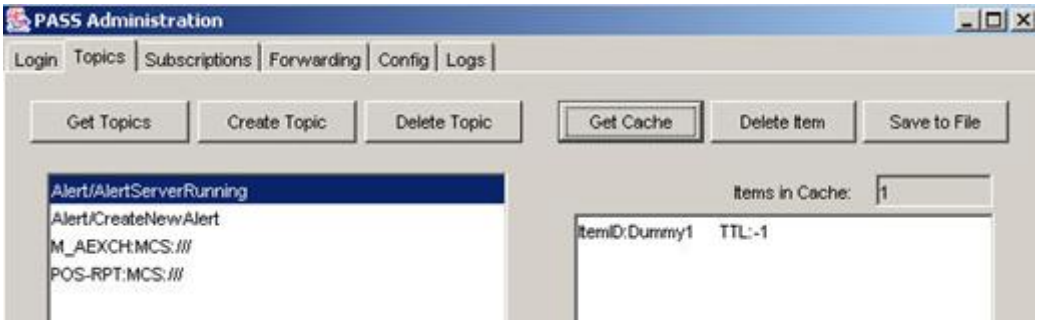


Figure 3-35 PASS Administration - Get Cache

3-4.6 Subscriptions Tab

1. From the PASS Administration window, **click** on the *Subscriptions t*ab to see who is subscribed to a topic.

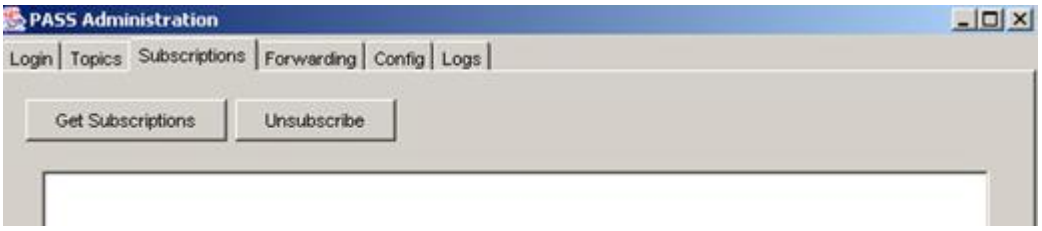


Figure 3-36 PASS Administration - Subscriptions Tab

3-4.6.1 Get Subscriptions

1. **Click** the *Get Subscriptions* button. The current subscriptions to the PASS Server are listed in the subscription field.

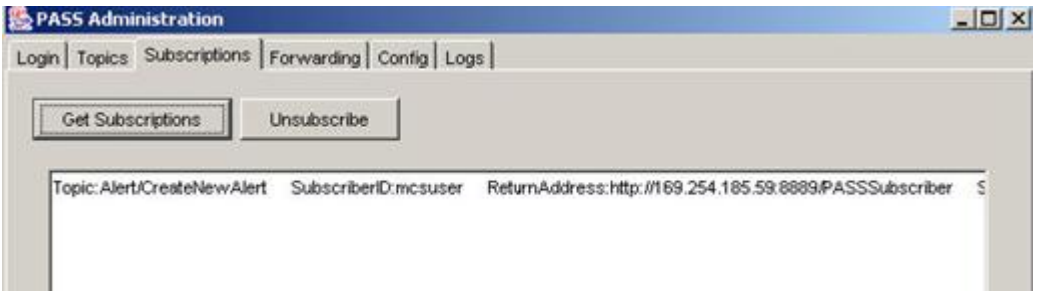


Figure 3-37 PASS Administration - Get Subscriptions

3-4.6.2 Unsubscribe

1. **Highlight** a subscription and **click** the *Unsubscribe* button to terminate a client's subscription to that topic.

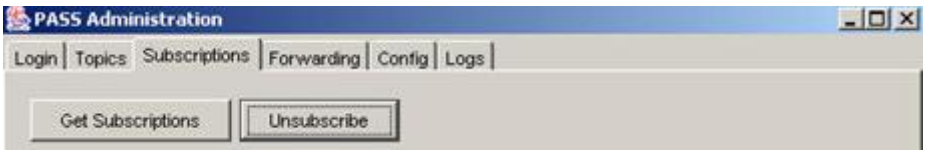


Figure 3-38 PASS Administration - Unsubscribe

3-4.7 Forwarding Tab

Topics available on one PASS Server can be forwarded to another PASS server using the Forwarding Tab.

1. **Enter** the *IP* Address, the *Port* number, *Username* and *Password*, of the PASS server that will be receiving data.
2. **Add** the topics to be forwarded from the local PASS to the remote PASS. **Select** the topic(s) you want to forward from the *Local PASS* list, then **click** the --> button. To remove a topic from the list to be forwarded, **select** it and **click**.
3. When you have completed your list of topics to be forwarded, **click** the *Mirror Remote* button.

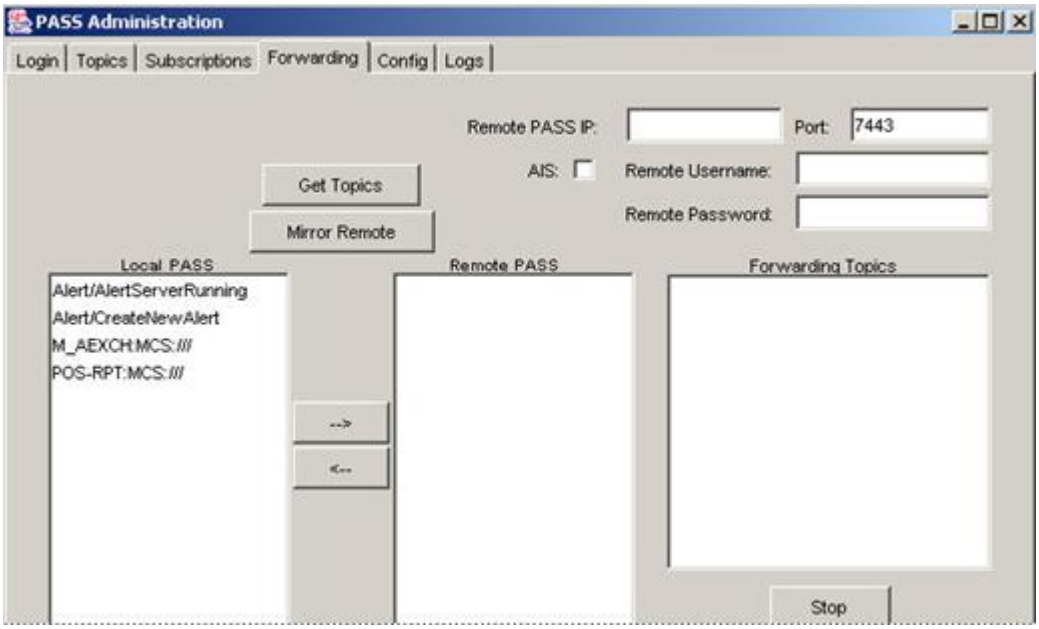


Figure 3-39 PASS Forwarding tab

3-4.8 Config Tab

The *PASS Administration* Window's *Config* Tab allows the user to control the PASS server's ports, memory usage, area of interest, and the JAAS Authentication settings.

The *Java Authentication and Authorization Service (JAAS)* is a set of application development tools that enable services to authenticate and enforce access controls upon users. This section of the *Config* tab determines whether PASS users are authenticated before being allowed to use the server, and which method of authentication is used.

The PASS Administration Configuration options are shown.

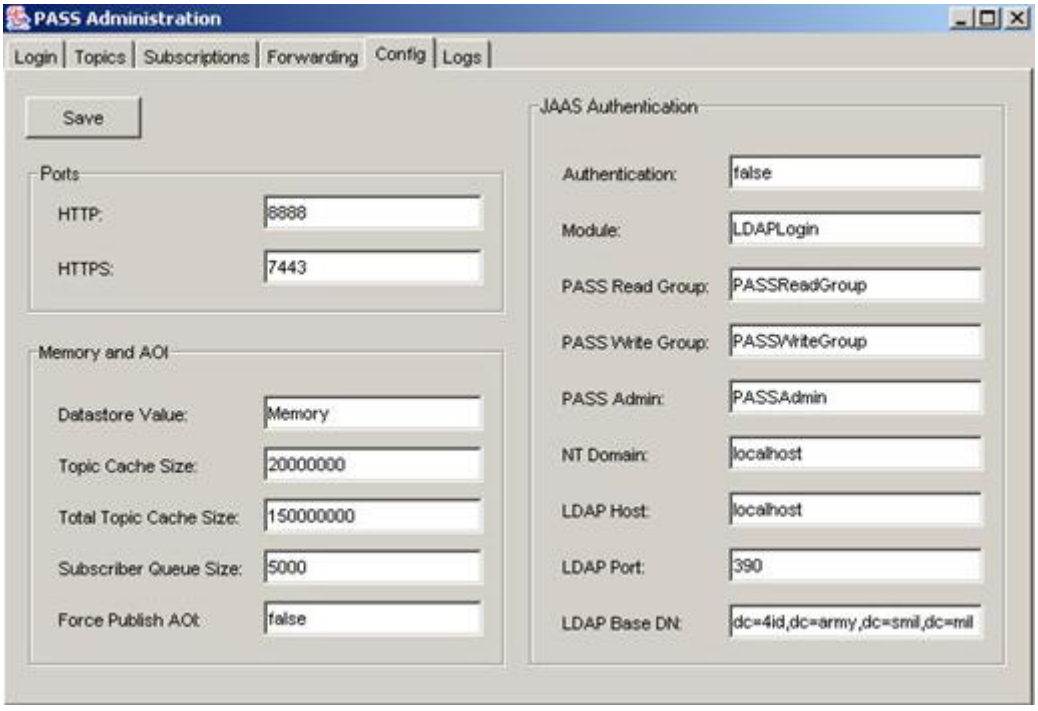


Figure 3-40 PASS Administration Configuration Tab

3-4.8.1 PASS Authentication

NT Logins are supported in the *Config* Tab of the *PASS Administration* application. The following procedure describes the local user and the associated groups necessary to enable NT authentication.

3.4.8.1.1 Local Users and Groups

NT Login requires the user to be a member of the PASSReadGroup and the PASSWriteGroup. Both of these groups must exist before attempting to authenticate using NTLogin in PASS. For full details of creating groups and users within the Microsoft environment, see the *Computer Management* documentation available in the *Microsoft Management Console Help*. The following steps will help to guide you through this process.

1. **Open** the *Start Menu,* then **select** *Settings, Control Panel*, *Administrative Tools*, *Computer Management*.
2. **Select** *Local Users and* Groupfolder. **Select** *Groups* folder. **Create** two new groups: *PASSReadGroup* and *PASSWriteGroup*.
3. **Select** the *Users folder,* **create** a *new user*. **Enter** a user name and password (example: mcsuser, mcsuser).
4. In the new user's *Properties* window, **add** the new user to both of the newly created groups.

3.4.8.1.2 PASS NT Login Authentication

1. To enable NT authentication, **open** the *PASS Administration* application. **Click** the *Config Tab* of the *PASS Administration* application. The PASS Administration window will appear.

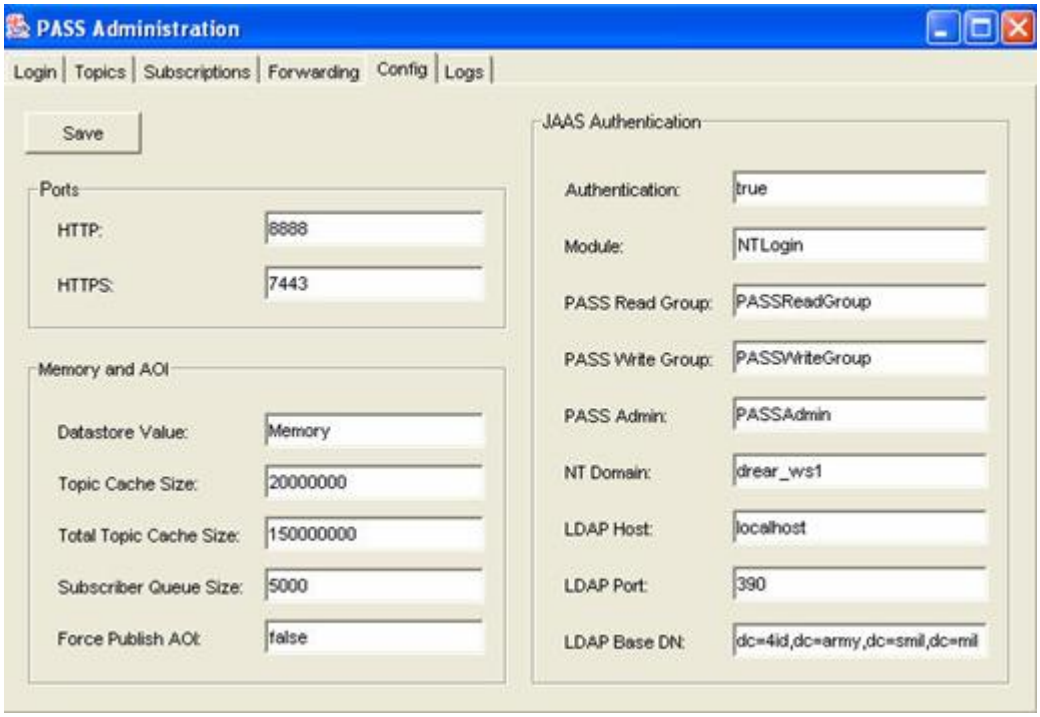


Figure 3-41 PASS NT Authentication

The JAAS area controls how the PASS server authenticates users.

1. For *Authentication,* **enter** *true*.
2. **Set** *Module* to *NTLogin*.
3. Don't change PASS Read and Write Group as shown in the figure above unless directed to do so by the System Administrator.
4. **Enter** the *NT Domain*, either the network name of the Gateway or the *localhos*t.
5. **Click** the *Save* button to save your settings.
6. To apply your changes to PASS, you must Stop and Restart PASS. The next time you try to login to PASS, you will be need to enter the username and password for the user account you created. To stop and restart the PASS server, see Section 3-4.2 .

3-4.9 Logs Tab

The *Logs* tab contains the files that show PASS subscription activity. There are two log files available for viewing: the *PASS Log* and *Audit Logs*.

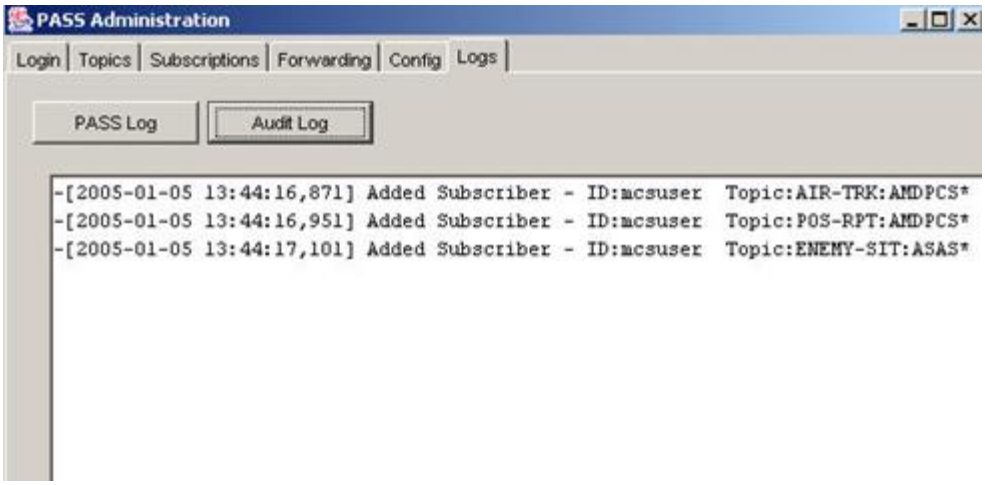


Figure 3-42 PASS Administration Logs Tab

3-4.10 Configure Near Real-Time Server (NRTS)

The NRTS Server Console is the main interface to NRTS. The console provides the means for configuring Data Providers for NRTS, as well as Injectors.

3-4.10.1 Starting the NRTS Server Console

NOTE

The NRTS Server Console starts automatically when an MCS Gateway or Workstation is started. Follow the instructions below to restart it if it has been closed.

1. In Windows Explorer, **navigate** to the *bin* directory in the NRTS folder located in the MCS installation directory; **click** on the *bin* folder to open it.
2. **Double-click** the server_console.bat file to launch *NRTS Server Console*. The NRTS Server Console Window opens.

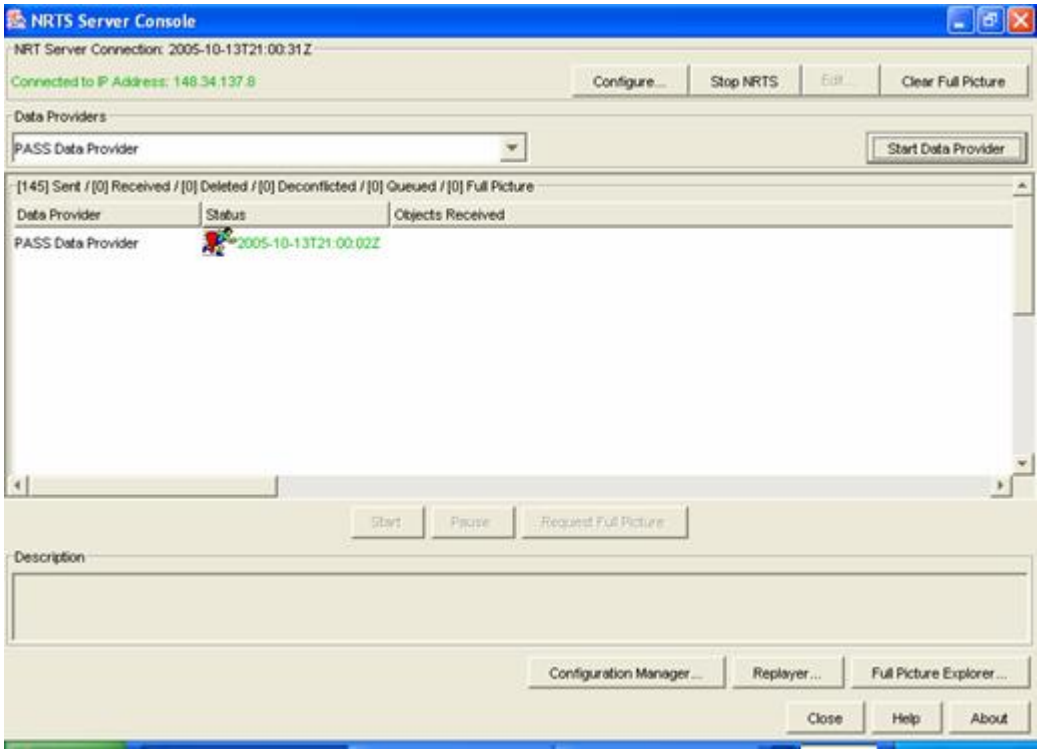


Figure 3-43 NRTS Server Console

NOTE

The Server Configuration Console monitors its connection to NRTS every 5 seconds. Monitoring this connection prevents data from being entered if the connection goes down.

3-4.10.2 NRTS Server Console User Interface

Upon starting the NRTS Server Console Window, the GUI is displayed with all of the message counters (received, deconflicted, queued, and full picture) reset to zero and the sent counter is set to 1.

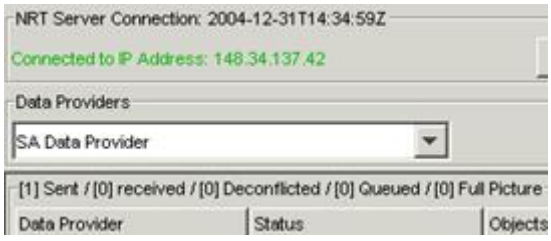


Figure 3-44 NRTS Message Counters

The top part of NRTS Server Console displays the following buttons.

Figure 3-45 NRTS Buttons

- *Configure* - allows user to verify or enter new IP Address from where the NRTS is running.
- *Stop NRTS* - allows user to stop server. Once NRTS is stopped, this button becomes Start NRTS.

- *Edit* - allows user to edit the NRTS properties file but only for local. By default, this button is disabled.
- *Clear Full Picture* - allows user to clear all NRTS objects in the Full Picture.

The middle part of NRTS server console window contains a Data Provider table and several buttons used to manage data providers and NRTS.

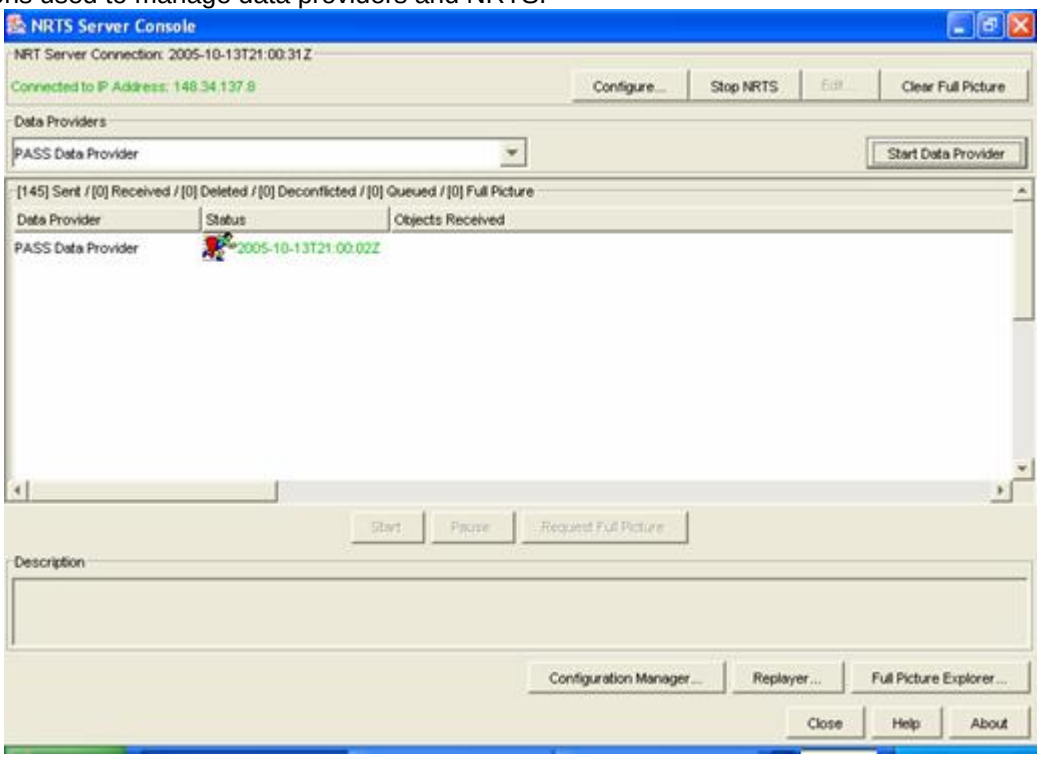


Figure 3-46 NRTS Data Provider Table

- *Data Providers* drop down menu - includes all available data providers.
- *Start Data Provider* - allows user to start each data provider when selected.
- *Stop* / *Start* (dual functions) - allows user to stop the selected Data Provider. *Stop* becomes *Start* when a stopped Data Provider is selected.
- *Pause / Resume* (dual functions) - allows user to pause the selected Data Provider. Pause becomes Resume when a paused Data Provider is selected.
- *Request Full Picture* - is disabled for all Data Providers but GCCS, NRTS, and PASS.

At the bottom of the NRTS server console window are several buttons used to manage NRTS, and a description area, which describes the data provider which is selected.

Figure 3-47 Buttons Used to Manage NRTS

- *Configuration Manager* - used to configure NRTS server, Injection server, and PASS connection.
- *Replayer* - allows a recorded exercise to be replayed at various speeds.

- *Full Picture Explorer* -opens the Full Picture window to view the received NRT Objects.
- *Close* - to close the NRTS server console window.
- *Help* - to launch the Quick User Guide.
- *About* - to open the NRTS version information window.

NOTE

If you close NRTS Server Console without stopping NRTS first, the NRTS Server Console window will be closed and the NRTS application will still be running in the background.

3-4.10.3 Configuring NRTS

Once you have started the *NRTS Server Configuration* window as described above, follow the steps below to properly configure NRTS.

1. From the Server Console window, **click** on the *Configure* button. The *Configure IP Address* window opens.

Figure 3-48 NRTS Configure IP Address

2. **Verify** or **enter** the *IP address* of the NRTS Server.
3. **Click** *OK*. The *Configure IP Address* window closes.

3-4.10.4 Configuration Manager

1. From the *NRTS Server Console* window, **click** on the *Configuration Manager* button to configure the data providers. The Configuration Manager window opens.

Figure 3-49 NRTS Server Console - Configuration Manager Selected

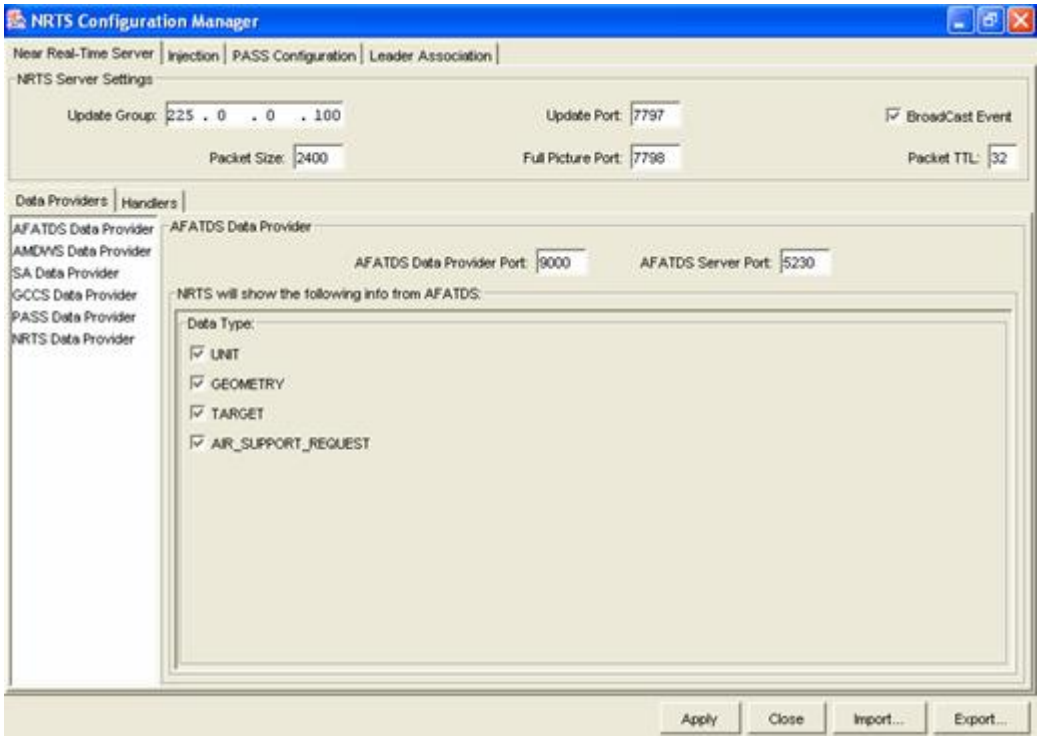


Figure 3-50 Configuration Manager (Near Real-Time Server Tab)

The NRTS Configuration Manager window contains four tabs:

- Near Real-Time Server
- Injection Server
- PASS Configuration
- Leader Association

The following buttons are located at the bottom of this window:

- *Apply* - when this button is clicked, all changes made to NRTS settings in this window take effect
- *Close* - to close the NRTS Configuration Manager window
- *Import* - allows user to load a backup configuration file to replace the current settings
- *Export* - allow user to save the current setting into a file for backup.

3.4.10.4.1 Near Real-Time Server Tab

The *Near Real-Time Server* tab contains the *NRTS Server Settings*.

Figure 3-51 NRTS Server tab

The top area, NRTS Server Settings, is used to configure the NRTS server. Setting the values in these fields configures the NRTS Server for operation.

- *Full Picture Port* -Port receiving data. If the default value is not correct, enter the desired port number.
- *Packet Size* - This field sets the size of outgoing packets. The packet size needs to be acceptable by all network cards. A common packet size used is 2400. Enter the correct size.
- *Packet TTL* - The *time to live* determines the distance, or number of hops the NRTS broadcast can be sent. Leave default value.
- *Broadcast Event* - When checked will broadcast NRTS.
- *NRT_HOME* - Used to identify the NRTS install folder, normally located at: <drive letter>:\MCS\NRTS.
- *Update Group* - IP address used by NRTS to send Multicast messages. Enter the appropriate *Update Group IP address*.
- *Update Port* - Port update multicast is performed on.

NOTE

All the above settings are determined by the System Administrator.

Tab functions:

- *Data Providers - sets up ports and addresses for data providers*
- *Handlers - inject or send data to various servers*

3.4.10.4.2 Data Providers Tab and Description Area

This area provides the ability to select Data Providers, and configure them. Generally you will accept the defaults provided and no change will be needed. If you are instructed to alter a specific setting the following information will guide you through this process.

1. To configure *AFATDS Data Provider*, **highlight** it in the *Data Providers* tab list.

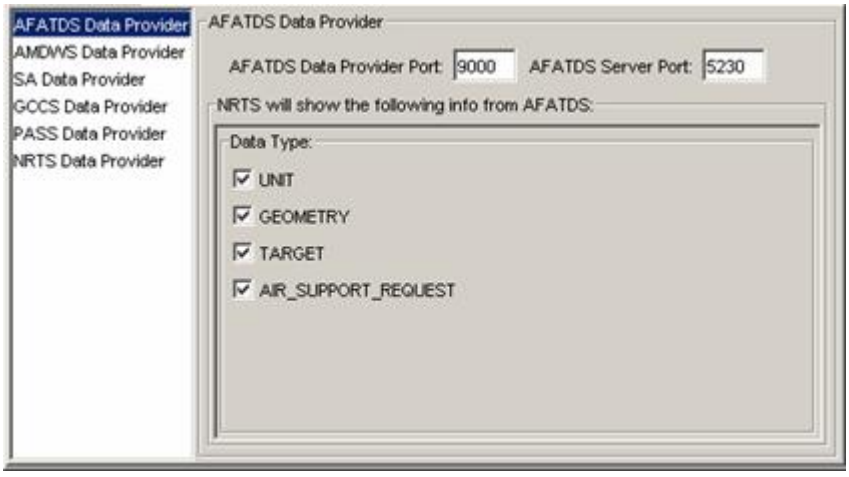


Figure 3-52 Data Provider Configuration - AFATADS

2. **Verify** the *AFATDS Data Provider Port* and *AFATDS Server Port* are correct.

3. If the default port numbers are not correct, **enter** the correct data.
4. **Select (**by clicking the checkbox) the information that you would like to receive in the *Data Type* area.
5. **Click** *Apply* to make any changes take effect. A confirmation window opens. **Click** *Yes*.

AMDWS Data Provider

1. To configure *AMDWS Data Provider*, **highlight** it in the *Data Providers* tab list.

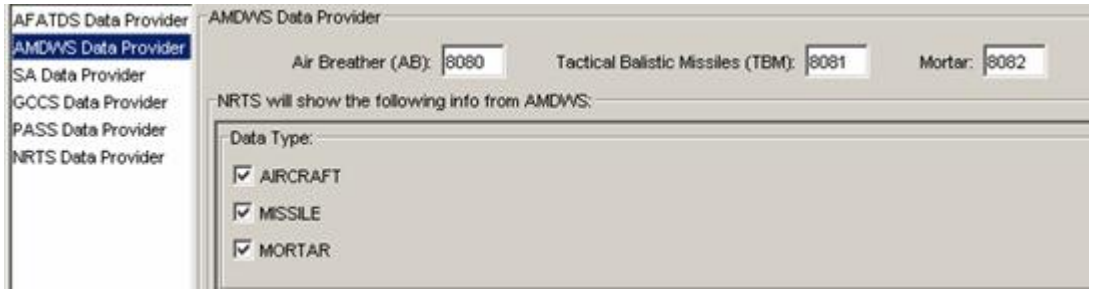


Figure 3-53 Configuration Manager - AMDWS Data Provider

2. **Enter** the *Air Breather (AB)* and *Tactical Ballistic Missiles (TBM)* port numbers, which can be obtained from the AMDWS web page. The URL for this page (and other configuration information) can be obtained from the System Administrator.
3. **Select** the information that you would like to receive in the *Data Type* area.
4. **Click** *Apply* to make any changes take effect. A confirmation window opens. **Click** *Yes*.

SA Data Provider

1. To configure the *SA Data Provider,* **highlight** it in the *Data Providers* tab list.
2. For the SA Data Provider, **enter** the multicast addresses FBCB2 uses.
3. **Use** the *Add* button to add a new *Multicast* address. A new line is opened in the *Multicast Address* frame). **Enter** the necessary data in the appropriate fields of the new line.
4. To **remove** a *SA Data Provider* address, **highlight** the address for removal and **click** the *Remove* button. The address is removed from the *Multicast Address* frame.
5. **Select** (by clicking the appropriate checkboxes in the *Data Type* area) the information that you would like to receive.
6. **Click** *Apply* to accept the changes. A confirmation window opens. **Click** *Yes*.

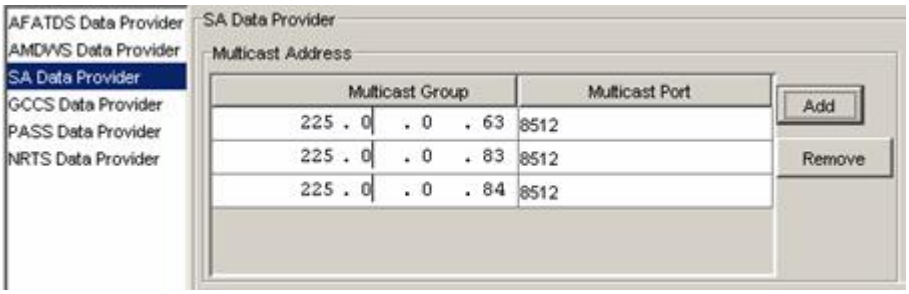


Figure 3-54 Configuration Manager - SA Data Provider

GCCS Data Provider

1. To configure the *GCCS Data Provider,* **select** it in the *Data Providers* tab. The *Data Provider* is highlighted, and the configuration window appears.

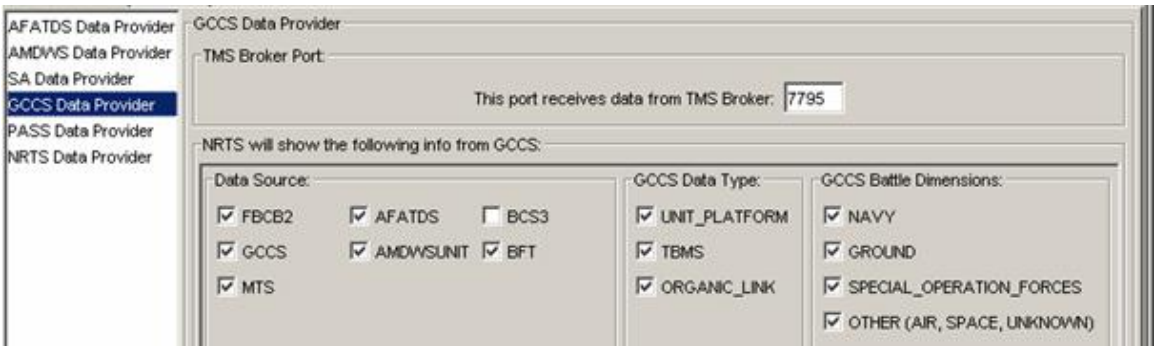


Figure 3-55 *Configuration Manager Window - Configure GCCS Data Provider*

2. **Verify** or **enter** the *TMS Broker* port number.
3. **Select** the information that you would like to receive in the *Data Source*, *GCCS Data Type*, and *GCCS Battle Dimensions* panes located just below the *TMS Broker Port* field.
4. **Click** *Apply* to accept the changes.

PASS Data Provider

1. To **configure** the PASS Data Provider, **select** it in the Data Providers tab. The Data Provider is highlighted, and the configuration window for the Data Provider appears.

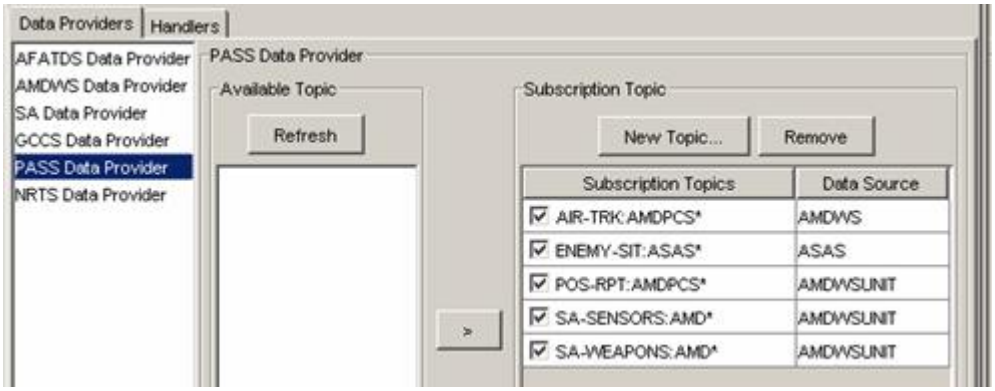


Figure 3-56 NRTS Configuration Manager - Configure PASS Data Provider

2. If connected to PASS, **click** the *Refresh* button to see all topics. If the PASS connection fails, an error message will display. Otherwise, the available topics will be displayed. If no topics are available, nothing happens.

NOTE

PASS must be configured before topics will appear in the Available Topics column.

3. To add a PASS topic to the NRTS feed, **click** on the topic in the *Available Topics*, then **click** the > button. **Repeat** this step as needed to add all the required topics to the *Subscription Topic* listing.
4. **Click** *Apply* to accept the changes. A confirmation window opens. **Click** *Yes*.

NRTS Data Provider

1. To **configure** the *NRTS Data Provider,* **select** it in the *Data Providers* tab. The *NRTS Data Provider* is highlighted, and the configuration window appears.

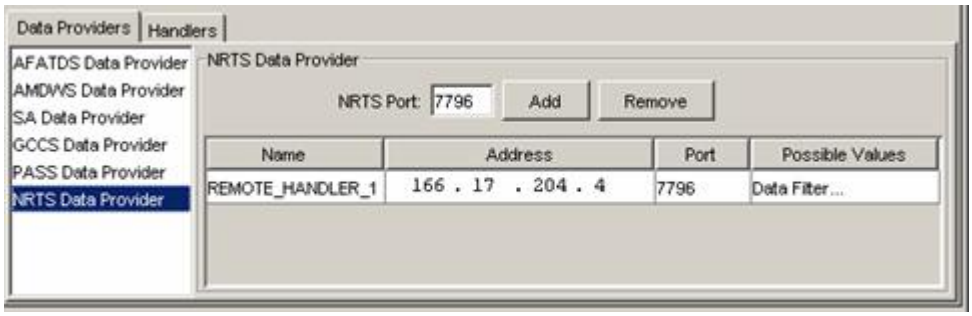


Figure 3-57 Configuration Manager - Add NRTS Data Provider

NOTE

A NRTS data provider can pull data from several NRTS servers.

2. If connecting to a remote NRTS server, **verify** the *NRTS Port, Name, Address* and *Possible Values* fields.

3. If necessary, **use** the *Add* button to add a new *NRTS Data Provider*. A new line is opened in the *NRTS Data Provider* area.

4. **Double-click** on the *Name* area and type a name for the new *Data Provider*. **Enter** the IP *Address* and *Port* number for it as well.

5. **Click** on the words *Data Filter …* in the *Possible Values* area to select what data will be fed from the remote NRTS to this one. The *NRTS Data Provider* window opens.

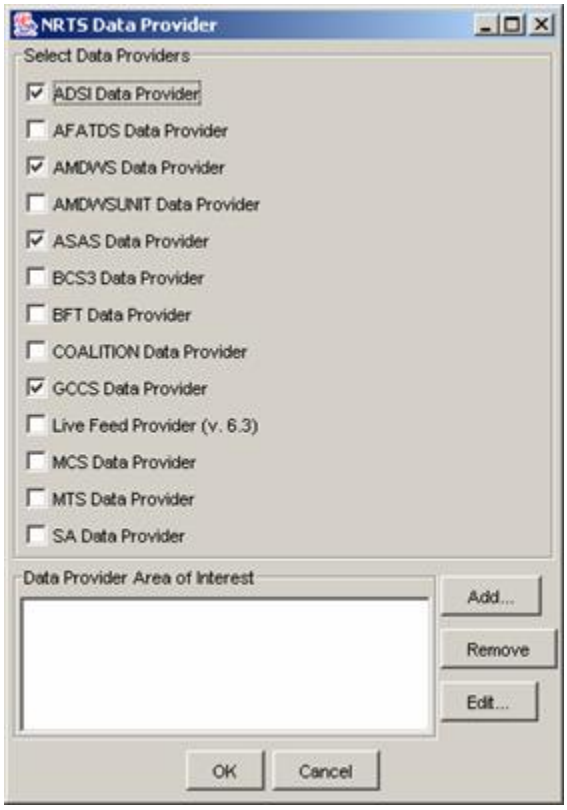


Figure 3-58 NRTS Data Provider Window

6. **Select** the *Data Providers* you wish to feed from the remote NRTS into the server you're configuring.
7. Optionally, **create** one or more *Data Provider Areas of Interest* by **clicking** the Add button, and **selecting** the corners of the AOI.
8. **Click** *OK*.
9. To **remove** a *NRTS Data Provider*, **highlight** the provider and **click** the *Remove* button. The provider is removed from the *NRTS Data Provider* area.
10. **Click** *Apply* to accept changes. A confirmation window opens. **Click** *Yes*.

3.4.10.4.3 Configure Handlers

The *Handler* tab has the settings for communicating with the Injection server.

1. **Click** the *Handlers* tab. The tab is displayed.

Figure 3-59 Handlers Tab

2. For each handler, **confirm** that the values present are correct. Your System Administrator will supply you with the correct data.

3.4.10.4.4 Injection Tab

The *Injection* tab controls the sending of data from this Near Real Time Server to other NRT Servers. It contains two (2) areas:

- Injection - Contains *Injection Port* and *Object Types to Injectors*.
- Injectors - used to configure the listed injectors.

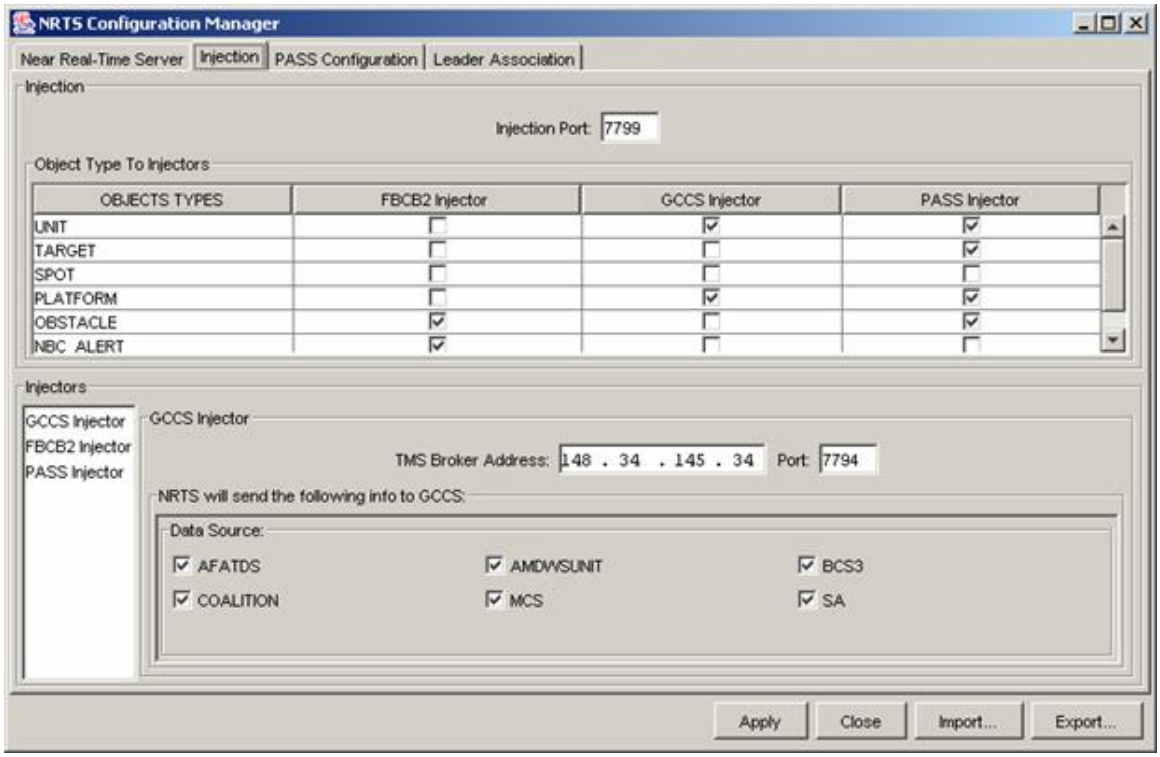


Figure 3-60 Configuration Manager - Injector Server Tab

1. To **select** an object for injection, **click** the box under the injector type column in the row of the object type. A checkmark appears in the box). For example, to inject platform information using the PASS *Injector*, **check** the checkbox below the PASS *Injector column* in the PLATFORM row.

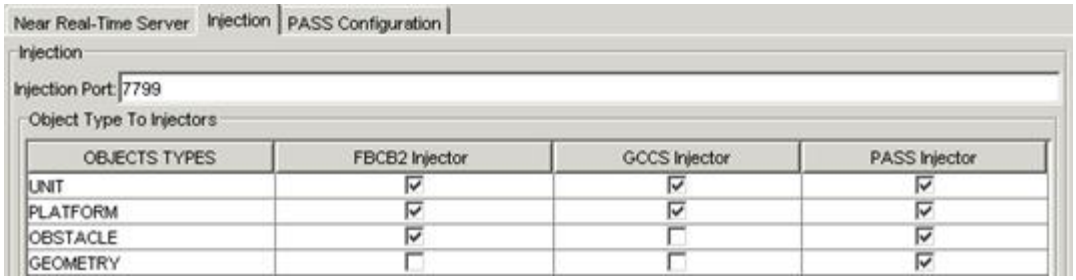


Figure 3-61 Injector Server Tab - Object Type To Injectors

2. **Uncheck** boxes to deselect objects for injection.
3. **Configure** the *Injectors* that will be injected using the bottom portion of the window.

GCCS Injector

a. To have NRTS inject data into GCCS, **select** GCCS. The *GCCS Injector settings* appear.

Figure 3-62 Injector Server Tab – GCCS Injector Settings

b. **Enter** the *IP* address and *port number* of the TMS Broker.

c. **Select** the *Data Sources* to inject into GCCS. **Click** on the checkbox for each *Data Source* you will be injecting into GCCS.

FBCB2 Injector

a. To have NRTS inject back into the *FBCB2* data stream, **click** on *FBCB2*. The *FBCB2 Injection Multicast Addresses* appears. **Select** the *Data Source*s to inject into GCCS. **Click** on the checkbox for each *Data Source* you will be injecting into GCCS.

b. Enter the URN of the machine that is running NRTS into the Originating URN field.

c. Under the *VMF Message Header Type,* **select** the type of message format that is currently in use. However if unsure, it should generally be: MIL_STD_2045_47001C.

d. **Insert** the multicast IP addresses and port information in the *Multicast Group* and *Multicast Port* fields

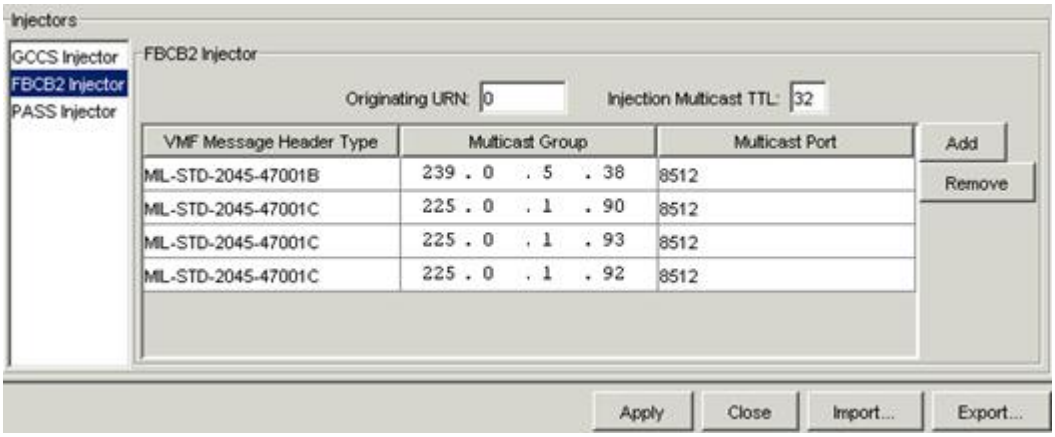


Figure 3-63 Injector Server Tab - FBCB2 Injector

PASS Injector

a. To inject data from NRTS into PASS, **select** PASS Injector. The Pass Injector settings appear.

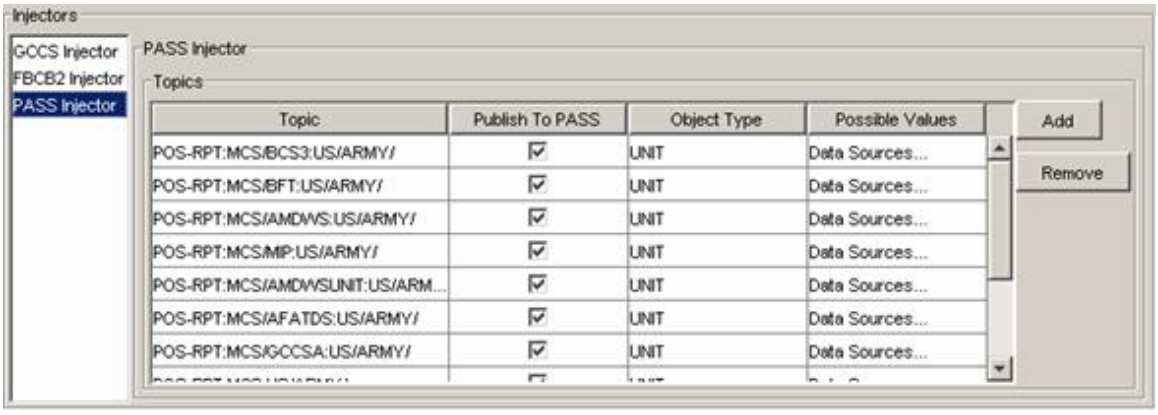


Figure 3-64 Injector Server Tab – PASS Injector

b. The Topic column shows a list of PASS topics that NRTS can inject new information into. To inject data into one of them, **confirm** that the Publish to PASS checkbox for that topic is checked, then **click** on the words *Data Sources* under *Possible Values*, and be sure the appropriate checkbox is checked.

c. To disable injecting a particular type of data into PASS, **uncheck** the *Publish to PASS* checkbox for that topic.

d. **Click** *Apply* to make changes effective. A confirmation window opens. **Click** *Yes*.

3.4.10.4.5 PASS Configuration Tab

The *PASS Configuration* tab is used to configure the NRTS connection to a PASS server.

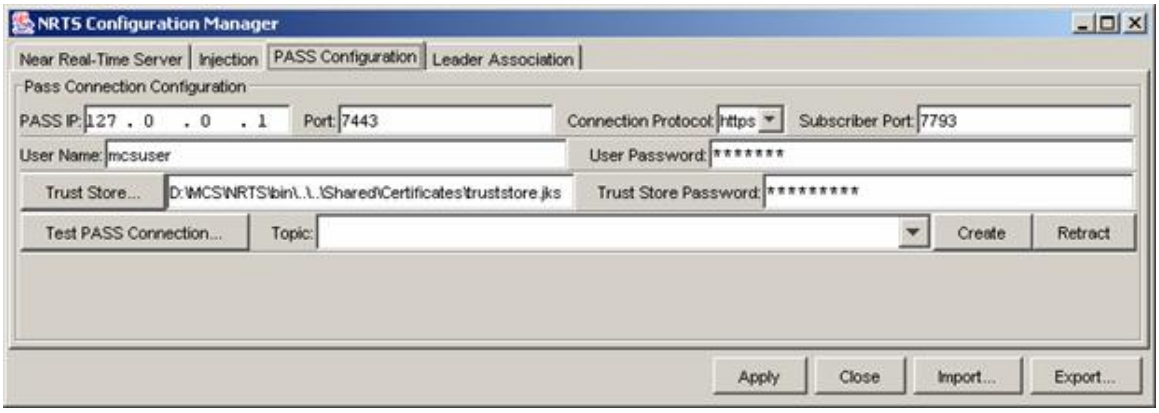


Figure 3-65 PASS Configuration Tab

3.4.10.4.6 PASS Connection Configuration

To configure the PASS connection:

1. In the *PASS IP* field, **verify** or **enter** the IP address of the PASS Servers.
2. **Verify** or **enter** the *Port* number to be used for the PASS Servers.
3. **Verify** or **enter** the *user name*.
4. **Verify** or **enter** *user password*.
5. *Connection Protocol* - **Click** the *down-arrow*, and **select** the appropriate protocol (either non-secured *HTTP,* or secured *HTTPS)*.
6. **Enter** the *port* number the subscriber is listening to.
7. **Click** the *Trust Store* button to verify or **enter** the *Trust Store* location. The default location of the trust store is *<drive letter>:\MCS\NRTS\bin\data\truststore*.
8. **Enter** the *Trust Store password* if necessary.
9. **Click** the *Test PASS Connection* button to confirm the settings are corrected. If PASS is connected and the settings were correct, the PASS Connection Status window opens, displaying a confirmation message.

Figure 3-66 Pass Connection Status

NOTE

The number of available topics (above) will vary.

10. **Click** *OK*. The *PASS Connection Status* window closes.

11. On the *PASS Configuration* tab, **click** *Apply* to save the configuration settings. A confirmation window opens. **Click** *Yes*. The *Confirmation* window closes. **Close** the *Configuration Manager* window to return to the *NRTS Server Console* window.

3-4.10.5 Managing Connections and Data Providers

This section provides the user with the minimum necessary information to successfully execute the NRTS software. The NRTS Server Console is used to start and stop connections and data providers.

NOTE

NRTS must be running in order to start a data provider.

3.4.10.5.1 Starting-Up Connections & Data Providers

1. To **start** the *Near Real Time Server*, from the *Server Console*, **click** on the *Start NRTS* button. The text of the message in the *NRT Server Connection* area turns green, indicating the server is started. The *Start NRTS* button turns into a *Stop NRTS* button.

Figure 3-67 NRT Server Start

2. To start *Data Providers,* **click** the *down-arrow* in the *Data Providers* box. A drop-down list of Data Providers appears. **Select** a *Data Provider*.

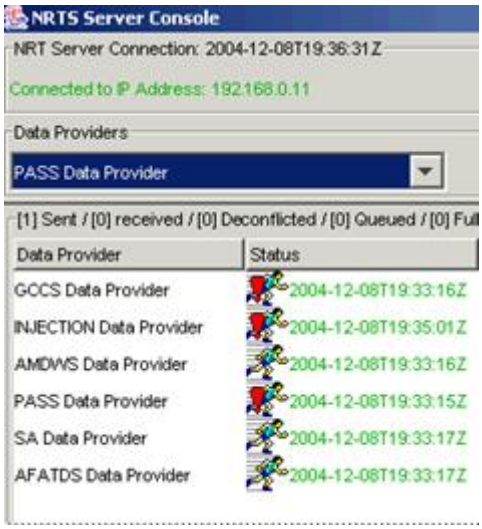


Figure 3-68 Data Providers Drop-Down List

3. **Click** the *Start Data Provider* button. The data provider *Running Man* icon appears in the large pane below.

Figure 3-69 Start Data Provider

4. **Select** all necessary data providers, **clicking** the *Start Data Provider* button for each to start the data provider. A *Running man* icon appears for each.

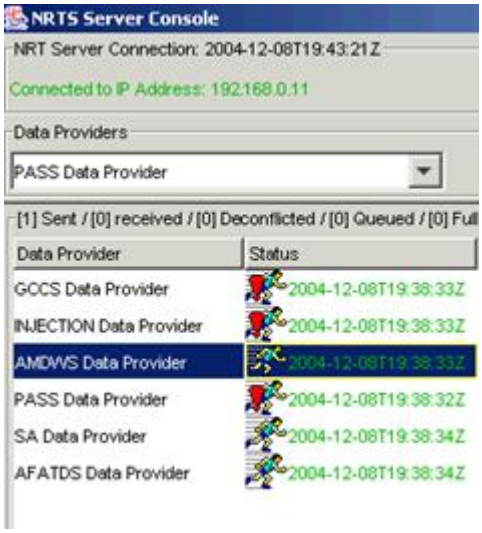


Figure 3-70 NRTS Server Console - Data Providers Started

5. When you **select** a *Data Provider*. Its status appears in the *Description* frame. A *Running Man* with a red exclamation point indicates an error. A *Running Man* icon without the exclamation point indicates the *Data Provider* is running.

3.4.10.5.2 Stopping Connections and Data Providers

1. To **stop** the *NRT Server Connection*, **click** the *Stop NRTS* button. A confirmation window appears. **Click** *Yes*. The *NRT Server Connection* text turns red, indicating the server is being stopped, and the *Stop NRTS* button becomes the *Start NRTS* button.

Figure 3-71 NRT Server Frame - Stopping NRTS

2. To **stop** a *Data Provider,* **select** the Data Provider. **Click** the *Stop* button. A *Stop* icon is placed over the *Running Man* icon.

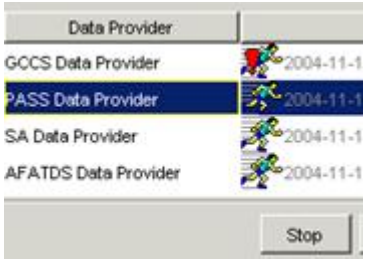


Figure 3-72 Select Data Provider - Stop

Figure 3-73 Data Provider Stopped

3. To **pause** a *Data Provider,* **select** the data provider and **click** on the *Pause* button. A pause symbol is placed over the *Running Man* icon and the *Pause* button turns into a *Resume* button. **Click** the *Resume* button to re-start it.

Figure 3-74 Data Provider Paused

3.4.10.5.3 Leader Association Tab

The Leadership Association tab is used to mark certain platforms as having a leadership role, and to mark command posts. Once associated using this window, a platform's symbol on the map is changed.

NOTE

MCS receives its platform information from systems. The information entered into the Leadership Association tab is used to change the way MCS displays platform information it receives from another BAS, for instance FBCB2.

1. To mark a platform as having a leadership role, first **click** on the *Leader Association* tab of the *NRTS Configuration Manager*.

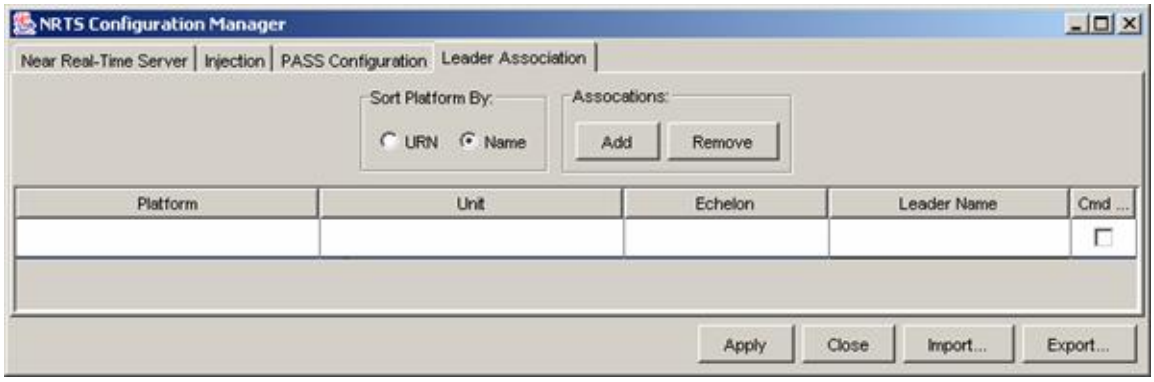


Figure 3-75 NRTS Leadership Association Tab

2. **Click** in the blank space under *Platform*. A drop-down list of platforms appears. **Select** the platform you want to mark as associated with a leader. You can list the platforms either sorted by *URN*, or by *Name.*

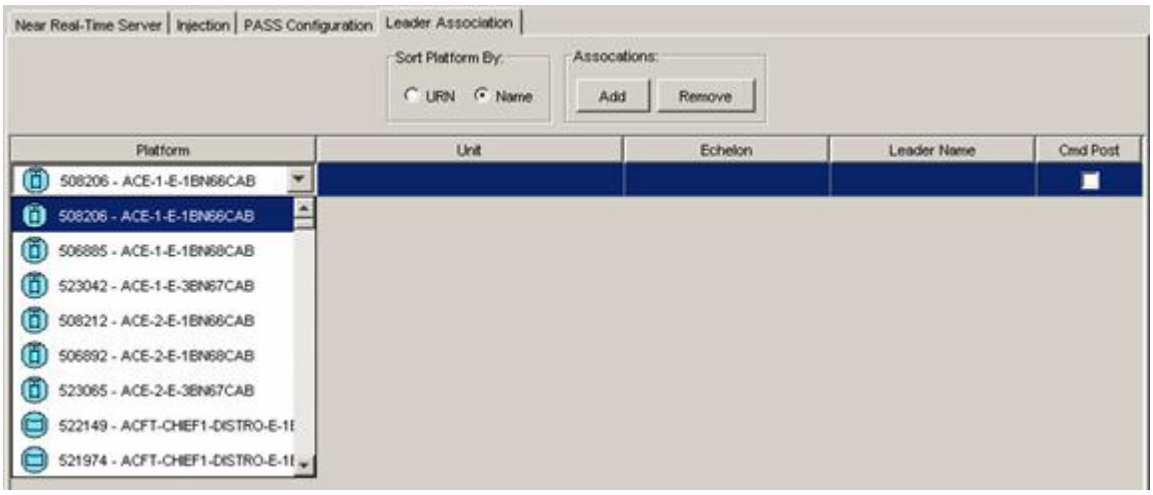


Figure 3-76 Select Platform

3. **Click** in the *Unit* blank space. This also turns into a drop-down list of unit types. **Select** the appropriate unit type.

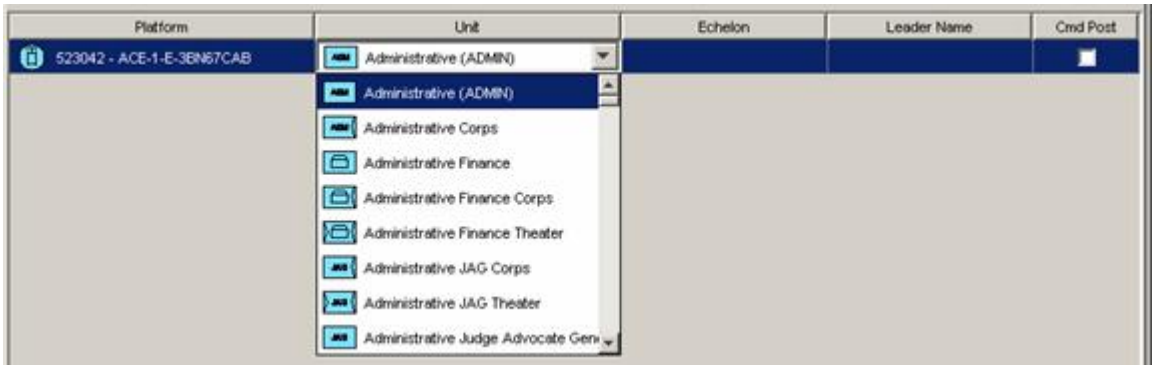


Figure 3-77 Select Unit Type

4. **Click** in the *Echelon* blank, and **select** the echelon of the unit being commanded.
5. Optionally, **click** in the *Leader Name* area and **replace** the default text with the name or other designator of the leader.
6. If the *Platform* being associated is a Command Post/HQ, **check** the *Cmd Post* checkbox.

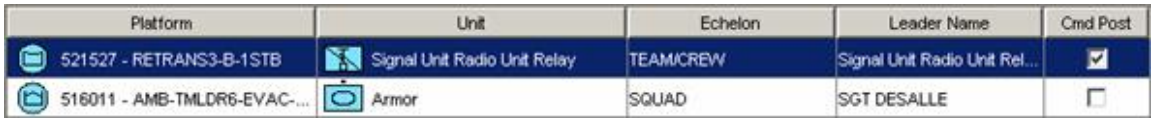


Figure 3-78 Leadership Association Set

7. **Click** *Apply* to make your changes take effect. If the *Platform* you've worked on is in the current Live Feed, you will see its icon in Maps and Overlays change from a platform icon to a leader icon. (The delay before a visible change will depend on NRTS and Live Feed settings.)

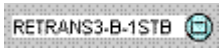


Figure 3-79 Symbol Before Association

Figure 3-80 Leader Associated Platform

8. To **associate** another unit, **click** the *Add* button, and another row is added to the table. **Follow** steps 1-7. **Repeat** as necessary.
9. To **remove** an association, **click** anywhere in that line of the table and **click** the *Remove* button.

3-4.10.6 Help for the NRTS Server Console

1. **Click** the *Help* button to display the Quick User's Guide for the Near Real Time Server (NRTS).

3-4.10.7 Closing the Server Console Window

1. **Click** the *Close* button.
2. As stated before, this will close the Server Console window only. This will not stop NRTS.

3-4.10.8 Stopping NRTS

1. **Click** the *Stop NRTS* button.
2. **Click** *Yes* on the confirmation window.
3. The NRTS application is stopped. **Click** the *Close* button to close the window.

3-4.11 Configure Outlook

Contact the Exchange Server administrator for information on configuring Outlook.

1. **Obtain** the Outlook configuration information from the Exchange Server Administrator.

NOTE

Microsoft Outlook 2003 requires the host name of the Exchange Server and the Mailbox name.

2. **Launch** *Outlook.* The *Outlook Startup Wizard* starts.
3. **Complete** *Wizard* with information provided by the Exchange Server Administrator.

3-5 Workstation Configuration

3-5.1 Prerequisites for Workstation Configuration

Prerequisites: All required Microsoft and other commercial software, and the MCS software must be installed prior to MCS application configuration.

Before starting to configure MCS Workstations, perform the following checklist to ensure you are properly prepared.

- **Review** *Release Notes.*

- **IMPORTANT:** If the required configuration parameters (see MCS Configuration Preparation Check List) were not obtained from the System Administrator at the beginning of workstation installation, obtain them now before attempting to proceed with configuration.
- **Review** the *Installation Security and Troubleshooting Notes* document in the <drive letter>:\MCS\Documents\Admin\ directory. **Perform** the necessary post installation steps.
- Prior to **starting** the *Army C2 Management Console* to configure MCS, **exit** all *MCS* applications.

3-5.2 Army C2 Management Console

The Army C2 Management Console is used to configure a machine to operate as an MCS Workstation, MCS Gateway, or Server.

1. From the *Start* menu, **select** *Programs, MCS, Administration,* and *Management Console*. The *Army C2 Management Console* opens.

NOTE

The Army C2 Management Console opens automatically when the computer is restarted after installing CD# 2.

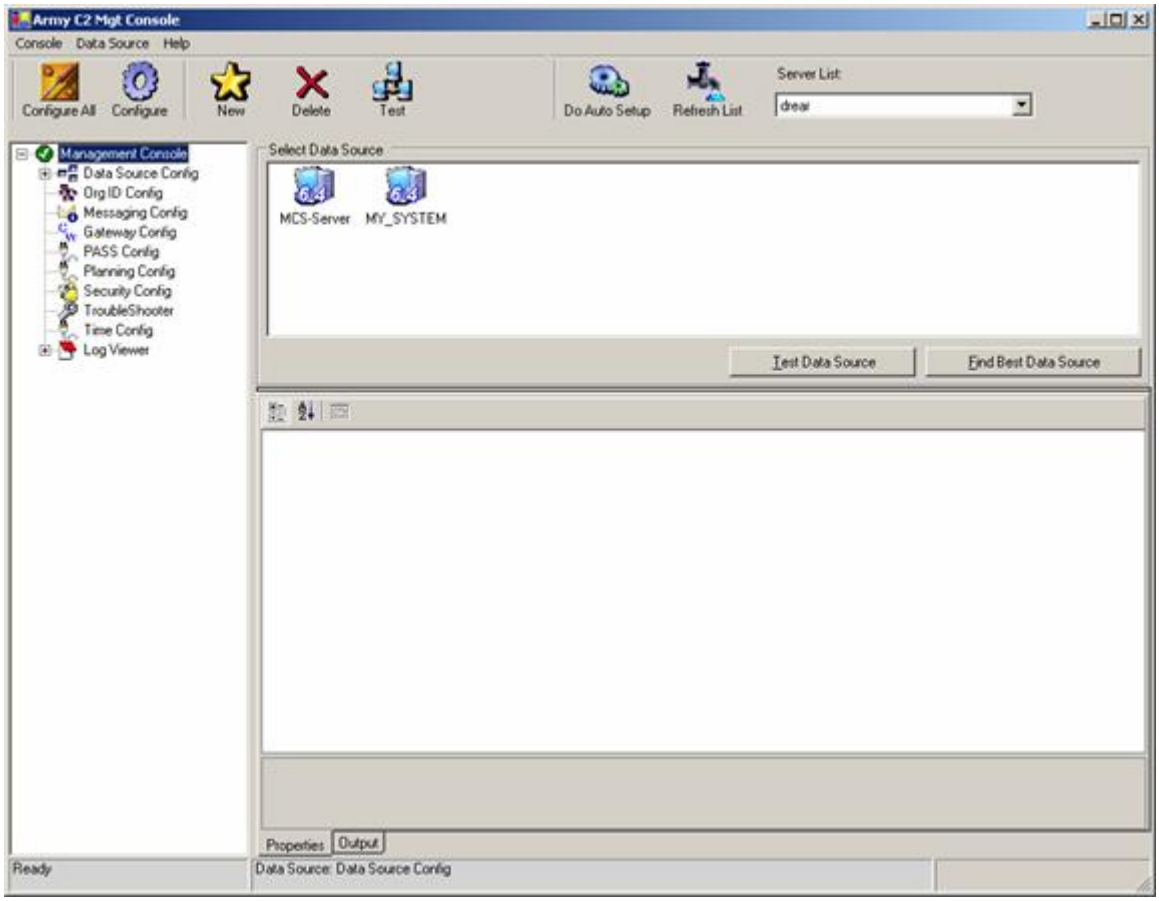


Figure 3-81 Default Army C2 Management Console (Partial)

The default Management Console is divided into four areas: Menu Bar, Toolbar, Treeview and Settings.

The Menu Bar and Toolbar vary (as does the appearance of the window) depending upon which item in the Treeview is selected for configuration.

The default Menu Bar consists of three items: *Console, Data Source* and *Help*.

The default Toolbar consists of the following control icons.

- *Configure All* - Applies all settings that have been changed in the Management Console.
- *Configure* - Applies any specific settings that have been changed in the Management Console.
- *New* - Creates a new data source.
- *Delete* - Deletes an existing data source.
- *Test* - Tests connectivity to an existing data source.
- *Do Auto Setup* - Once an Auto Setup server has been chosen, Do Auto Setup instructs your system to use the settings supplied by the Auto Setup Utility.
- *Refresh List* - Adds all available Auto Setup servers to the Server List.
- *Server List* - Used to pick one an Auto Setup server for this system.

The Treeview lists the various settings that can be configured, as well as the Management Console *Log Viewer* and the *Troubleshooter* function. The default Treeview is shown in Figure 3-81.

The Settings area shows the settings for whichever MCS item is selected in the Treeview.

3-5.3 Configure Data Source

Data Sources are connections to the MCS database, which MCS systems use to store and share data such as overlays, tables of organization, and unit information. The database is stored both on the MCS Workstation, and on the Server.

For workstations, the Data Sources will normally be configured automatically by the Auto Setup Utility. Configuration for MCS Gateways and Servers must be done manually.

1. From the Treeview in the *Management Console* window, **select** *Data Source Config.* The *Management Console* window displays data source configuration settings.

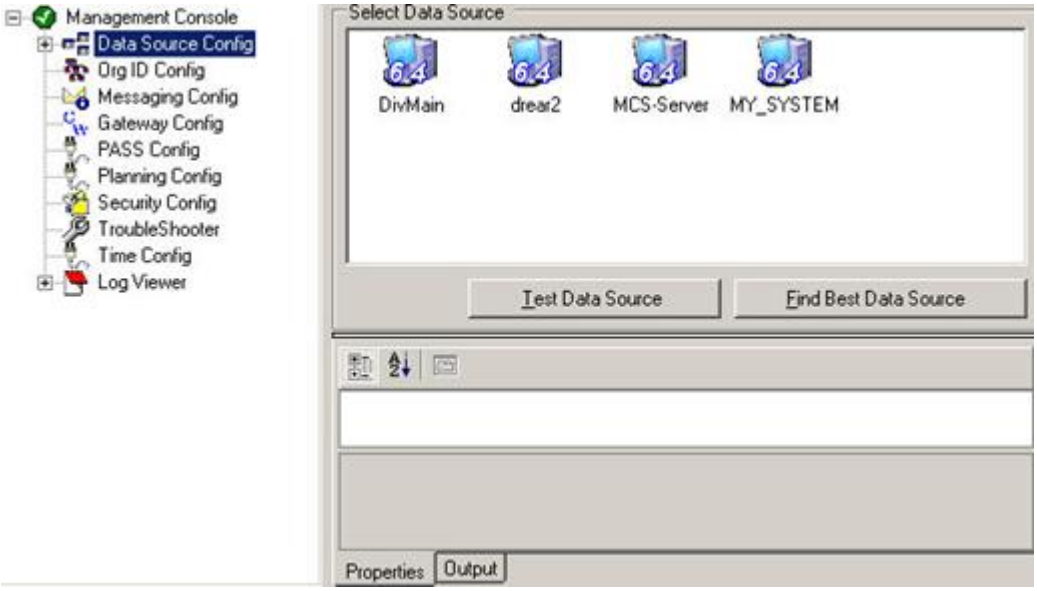


Figure 3-82 Data Source Selected

The *Management Console Menu* shows three functions: *Console, Data Source and Help*. The *Management Console toolbar* shows icons for *Configure, Wizard, New, Delete and Test.* Other features include the *Select Data Source* area and two tabs: *Properties* and *Output*.

- The *Select Data Source* area shows icons for available data sources. It also contains buttons for testing the data source and locating the best data source. The properties of the selected data source are displayed in the *Properties* tab.
- The Treeview lists the available data sources.
- The *Output* tab shows the output of any processes (such as *Test Data Source*) run from the *Data Source Config* screen.

3-5.3.1 Adding a New Data Source

After the initial configuration, if the desired data source is not present in the Management Console window, it can be added through the Data Source selection on the Menu Bar.

NOTE

Usually, Data Source configuration will be handled by the AutoSetup Utility for MCS Workstations. This procedure can be used if the AutoSetup Utility is not available, to connect to servers not configured by the AutoSetup Utility, and for Servers and Gateways acting as AutoSetup Servers.

1. **Launch** the *Army C2 Management Console* from the desktop *Start* menu, **selecting** *Programs, MCS, Administration, Management Console*.
2. **Select** *Data Source* from the menu bar. The Data Source drop-down menu opens.
3. **Select** New from the drop-down menu. The New Data Source window opens.

Figure 3-83 New Data Source

4. **Select** a *SQL Server* template if the database is on the *Battle Command Server.* **Select** the *Access* template if the database is on the local hard drive.
5. **Enter** a name for the new Data Source and **click** *OK*. The *New Data Source* window closes. The new data source appears in the *Management Console* window and the *Properties* tab for the data source appears at the bottom of the screen.
6. In the *Properties* tab, **enter** the *Data Source* details, the *Database Settings* and the *Server Settings* for the new data source.
7. **Click** on any of the *Properties* to display additional information about the property in the gray area at the bottom of the *Properties* tab.

NOTE

Some of the properties apply only to one of the Database Templates. DataSource Location applies only to Access (local) databases. The Server Settings area applies only to SQL Server databases.

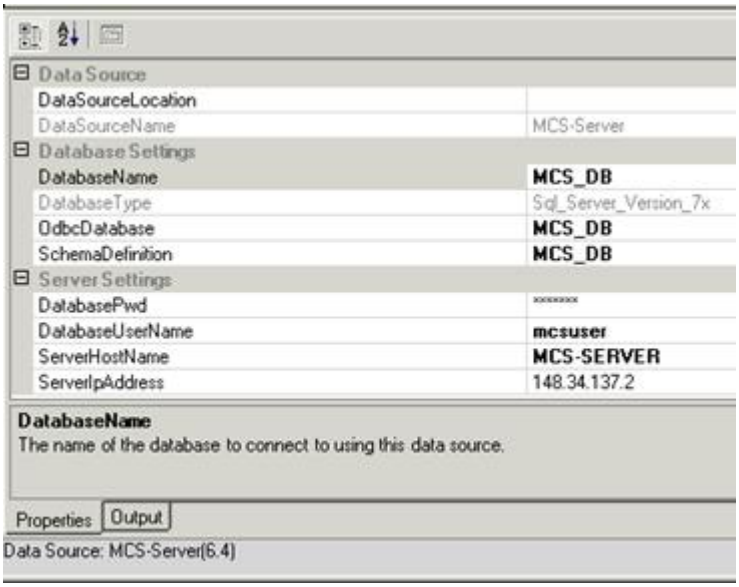


Figure 3-84 Add New Data Source Properties Tab

8. **Select** *DataSourceLocation* (for a database on your hard drive) or *ServerIPAddress* (for a database on a server **Enter** the correct information. This information should be obtained from the System Administrator.
9. For databases on servers, **select** *DatabasePwd*. An *ellipsis* ("…") button appears to the right. **Click** the *ellipsis* to open the *Password Editor* window.

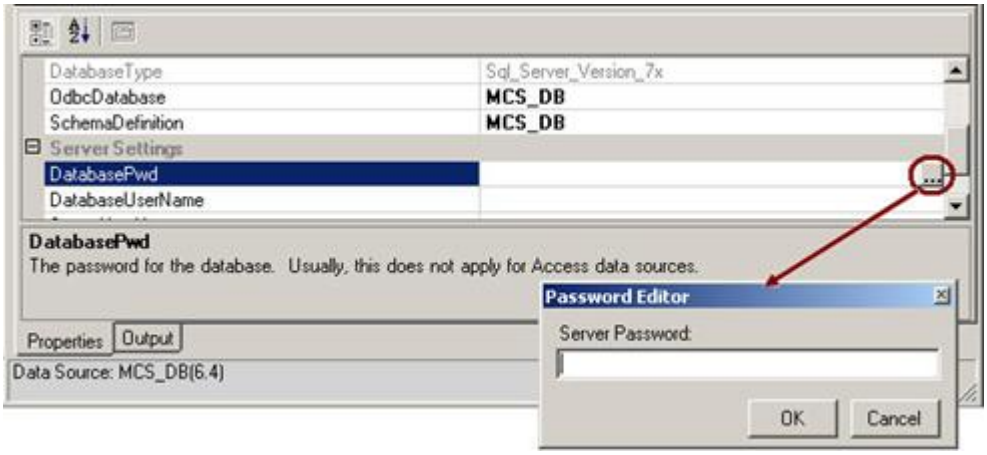


Figure 3-85 Password Editor

10. **Enter** a password. **Click** *OK*. The *Password Editor* closes.
11. To **configure** the datasource for the workstation (save the changes you have made) **click** either the *Configure* icon on the toolbar, or *Console* on the menu bar. If the menu bar *Console* function is used, a drop-down menu appears. **Click** *Configure* on the *Console* drop-down menu. The status bar displays the progress of the configuration, as well as a *Configuration Complete* message when finished.
12. To **view** details of the data source configuration, **click** the *Output* tab of the *Management Console* window.

3-5.3.2 Finding Best Data Source

When multiple data sources are present, the *Find Best Data Source* button in the *Data Source Configuration* window can be used to determine the optimum data source. The *Find Best Data Source* tests only connections to Servers (not to the local MCS database on the same computer).

Figure 3-86 Find Best Data Source

1. **Click** the *Find Best Data Source* button. The best data source is displayed in the *Output* tab.

3-5.3.3 Deleting a Data Source

A data source can be deleted through the Delete selection of the Data Source menu or through the Delete icon on the toolbar.

1. In the Army C2 *Management Console* Treeview or in the *Select Data Source* area, **select** the data source to be deleted.
2. **Click on** the *Delete* icon on the toolbar. A confirmation window appears.
3. **Click** on *OK*. The data source is deleted.

Figure 3-87 Delete Data Source

3-5.4 Configure Org ID

The user's Organization ID determines ownership of folders (groups of overlays), overlays and task organizations.

These Folder and Overlay Ownership Rules apply:

- G3 and CDR can edit all overlays
- S3 can edit an overlay if the overlay owner is the same unit
- A user can take ownership of an overlay owned by the same Battlefield Functional Area
- Only an ENGR can draw or modify engineering symbols on an overlay
- Only CHEM can send certain JWARN messages

The following rule applies to Task Organizations:

- Only G3, S3 and CDR can re-task an organization

To identify your Org ID:

1. From the *Treeview*, **select** *Org ID Config.* The *Management Console* displays the *Organization ID* configuration options and *a Unit Treeview.*

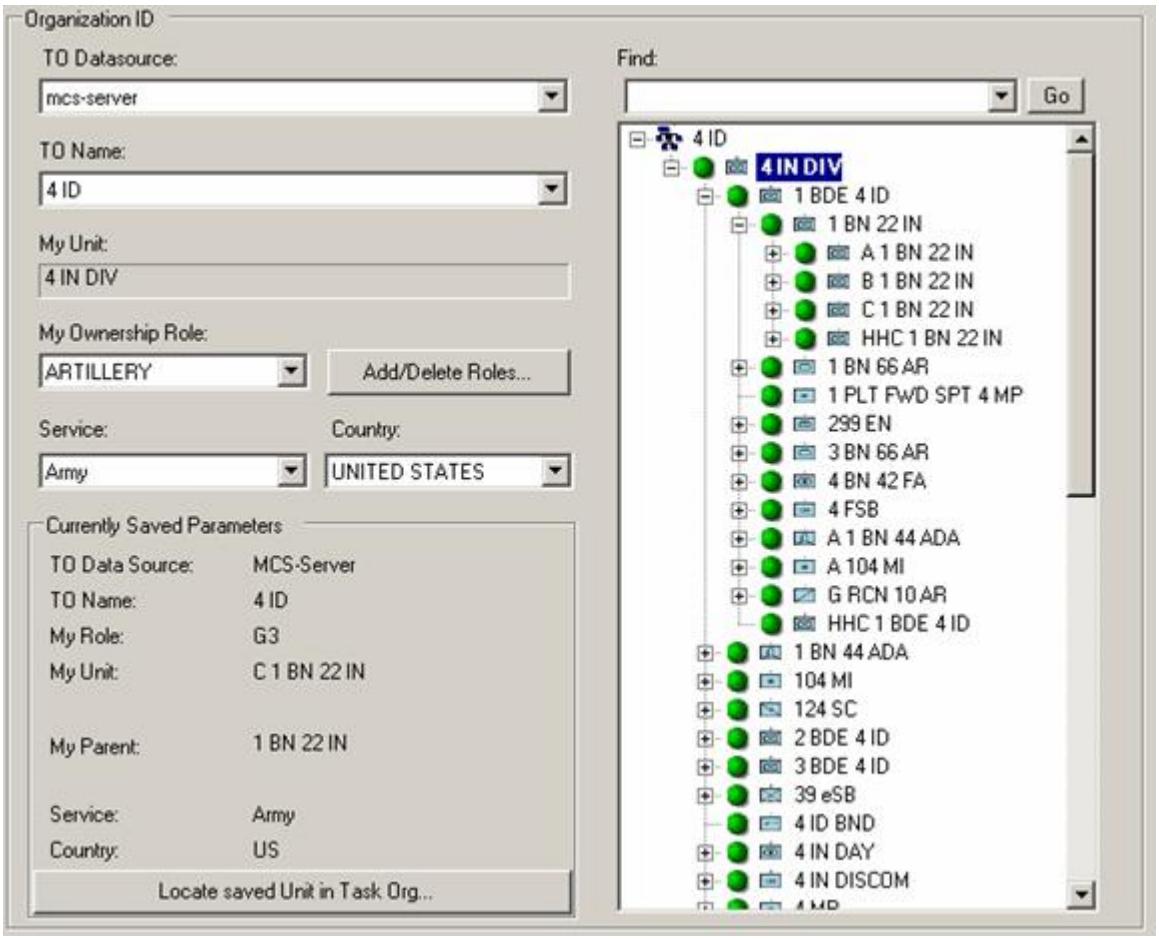


Figure 3-88 Org ID Configuration

2. Open the list of Data Sources by **clicking** the down-arrow in the *TO Datasource* field. **Select** the appropriate *TO DataSource*.

NOTE

At least one Data Source must be configured before selecting an Org ID.

3. **Open** the list of Tables of Organization by **clicking** the *down-arrow* in the *TO Name* field. **Select** the appropriate *TO name*. The selected Unit will appear in the *My Unit* field.
4. **Open** the list of Ownership Roles by **clicking** the *down-arrow* in the *My Ownership Role* field. **Select** the appropriate *ownership role.*
5. **Open** the list of Services by **clicking** the *down-arrow* of the *Service* field. **Select** the appropriate *Service*.
6. **Open** the list of countries by **clicking** the *down-arrow* of the *Country* field. **Select** the appropriate *country.*
7. **Enter** the first few characters of the unit name in the *My Unit* field to locate a unit in the Table of Organization. **Select** *Go* (located to the right of the *My Unit* field). The *My Unit* field will scroll to the first unit whose name starts with the characters you typed. **Select** the appropriate unit from the listing.
8. **Click** the *Locate Saved Unit in Task Org…* button to return the Org ID configuration to the last configure settings.

9. **Click** *Configure* on the *toolbar* and the status bar will show the progress of the configuration and then will display *Configuration Complete* when finished.
10. After configuration is complete, **verify** that the *Currently Saved Parameters* are correct.

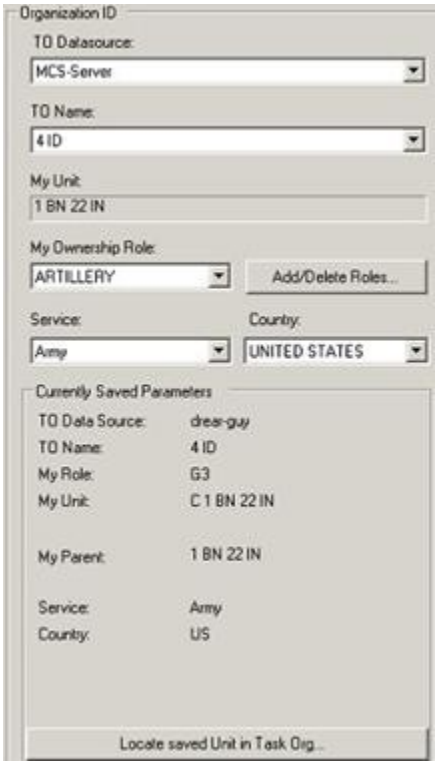


Figure 3-89 Org ID After Configuration

11. After a *Unit* and *Role* have been selected, you can scroll the listing to that unit at any time. **Press** the *Locate saved Unit in Task Org* button to locate the saved unit in the list.

3-5.5 Configure Messaging

NOTE

If configuring a Server or Gateway, skip this section. Messaging cannot be configured on a Server or Gateway.

In order to acquire information and quickly exchange it between appropriate battlefield commanders, shooters, supporters, etc., roles have been assigned attributes which uniquely identify them. The Army C2 Management Console allows a user to assign the appropriate role to the MCS Workstation.

The list of message roles can be found either on the MCS Workstation, or on the C2R server. Role information is stored in a file called hostlist.txt and the hostlist.txt file can be imported from either source.

3-5.5.1 Import Message Roles From a File on the MCS Workstation:

1. **Click** on *Messaging Config* under the *Management Console* item in the Treeview in the left pane and then select *Messaging* from the *Management Console* menu bar. The *Messaging* drop-down menu appears.

Figure 3-90 Messaging Drop-Down List

2. From the *Messaging* drop-down, **select** *Import Hostlist*. The *Import Hostlist File* window opens.

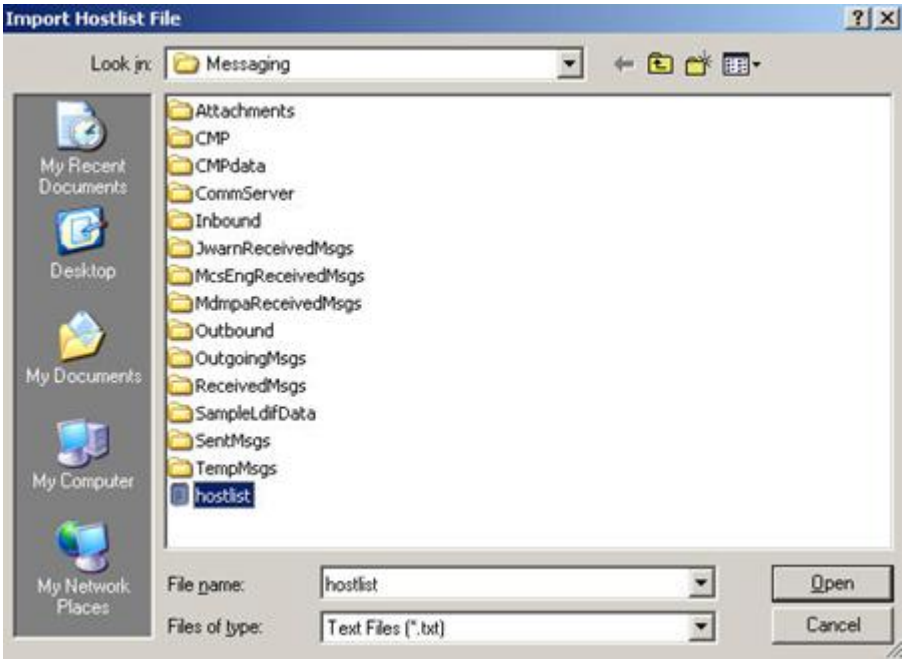


Figure 3-91 Import Hostlist File Window

3. **Select** the *hostlist.txt* file and **click** *Open*. The *hostlist* file is displayed in the *Messaging Role* area of the *Messaging Config* screen.

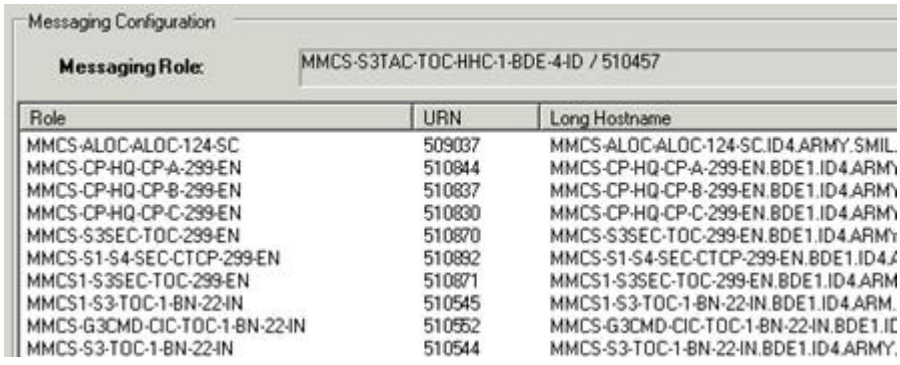


Figure 3-92 Messaging Configuration (Host List File) -2

3-5.5.2 Import Messaging Roles From a Hostlist File on the C2R Server

1. From the *Messaging* drop-down, **select** *Import Hostlist From C2R Server*, as shown in. The file *MCS\Messaging\C2RHostlist.txt* file is imported from the *C2R Server.*

Figure 3-93 Import Hostlist from C2R Server

3-5.5.3 Download Config Files From Server

1. From the *Messaging* drop-down, **select** *Download Config Files from Server* (see above). *The Download Messaging Files* window opens.
2. In the *Download Messaging Files* window, **enter** the *FTP Server Hostname or IP Address*, the *User Name*, and associated *Password* (if any).

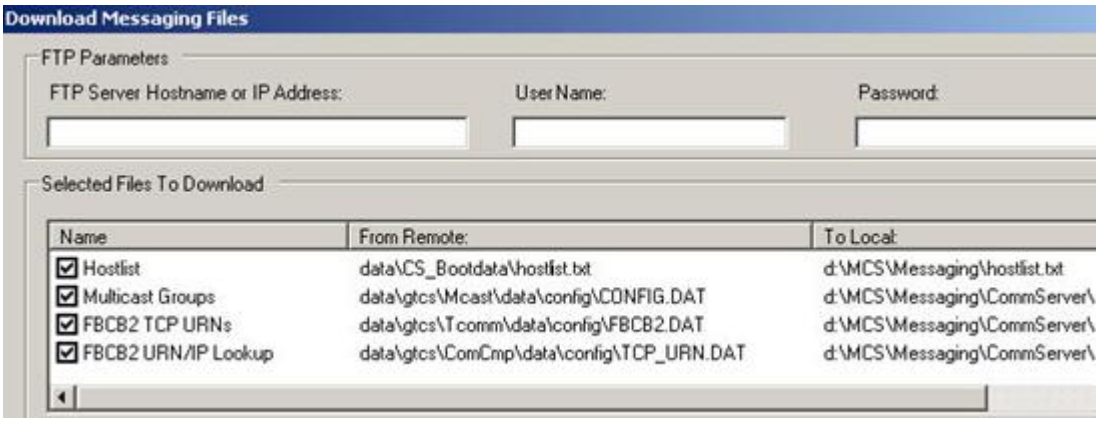


Figure 3-94 Download Messaging Files

3. **Click** the *checkbox* to select or deselect a file for download.
4. **Click** *Download* and the download process starts.
5. **Click** the *Close* button to close the window. The *Messaging Roles* are displayed.

NOTE

All columns can be sorted. Click on the Name column heading to sort the Messaging Roles by Name.

6. **Select** the desired *role* from the list.
7. To **configure** the role for the workstation, **click** the *Configure* icon on the toolbar. The status bar displays the progress of the configuration, as well as a *Configuration Complete* message when finished.

3-5.5.4 CMP Options

1. From the *Messaging* drop-down list, **select** *CMP Options*. The *CMP Options* window displays.

Figure 3-95 CMP Options

2. **Select** the *Message Standard* from the drop-down list.

Figure 3-96 CMP Options – Message Standard

3. **Click** *OK* to save your setting.

3-5.5.5 Use Local Files for Role Selection

1. From the *Messaging* drop-down list, **select** *Use Local Files for Role Selection*.

Figure 3-97 Use C2R for Role Selection

2. The list of roles in the *Messaging Configuration* area disappears and is replaced by *C2R Settings*.

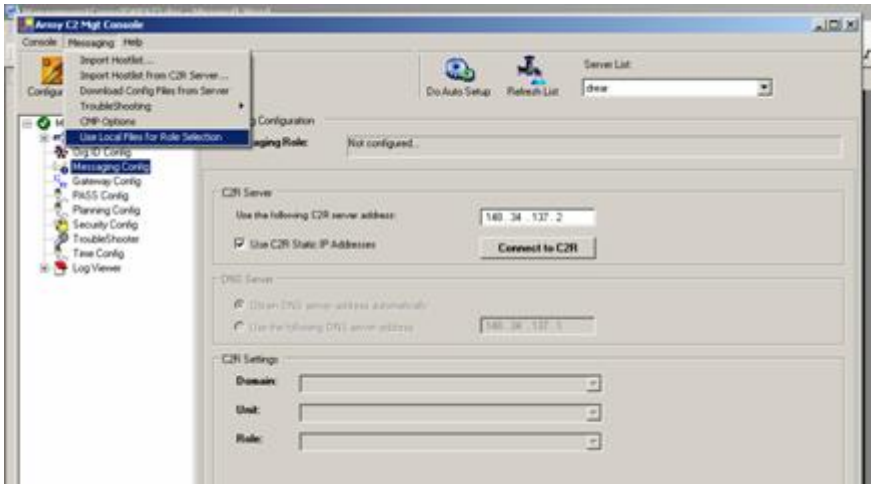


Figure 3-98 C2R Role Selection Settings

3. **Enter** the *C2R Server IP Address* in the space provided. **Click** the *Connect to C2R* button.
4. **Select** *Use the following DNS Server Address*, or take the default option to *Obtain the DNS Server Address Automatically*.
5. **Select** the *Domain, Unit,* and *Role.*
6. To **configure** the Messaging Role for the workstation, **click** the *Configure* icon on the toolbar. The status bar displays the progress of the configuration, as well as a *Configuration Complete* message when finished.

3-5.6 Gateway Config

The *Gateway Config* option in the Treeview of the Management Console is used to configure the workstation's connection to NRTS and to C2PC Gateway (used to connect to GCCS-A).

NOTE

Workstations will normally configure gateways using the AutoSetup Utility. Use the Management Console to configure gateways on Servers and MCS Gateways.

1. From Treeview, **select** *Gateway Config.* The *Management Console* window displays gateway configuration options.

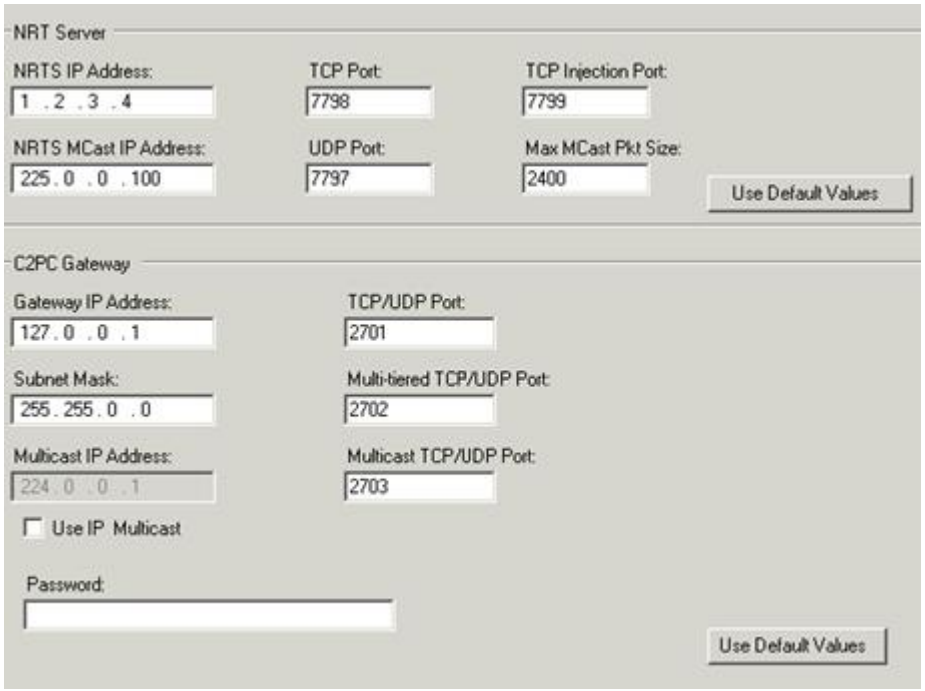


Figure 3-99 Management Console Window - Gateway Config

2. **Verify** or **enter** the correct settings in the *NRT Server* area.
3. **Verify** or **enter** the correct settings in the *C2PC Gateway* area.
4. From the *Management Console* toolbar, **select** the *Configure* icon to configure the connections to the gateways. Site-specific information must be obtained from your System Administrator.

3-5.7 Configure PASS

PASS is an information routing system that delivers data from publishers to subscribers. Publishers publish data to a particular topic without knowledge of which subscribers are

subscribing to this topic. Subscribers subscribe to topics without knowledge of which publishers are publishing information to that topic.

NOTE

Workstations will normally configure PASS using the AutoSetup Utility. Use the Management Console to configure PASS on Servers and MCS Gateways.

NOTE

A Battle Command Server is the primary PASS Server in a TOC, if one is present. If no Battle Command Server is available, a Server or Gateway can be use used as the PASS Server.

1. From Treeview, **select** *PASS Config.* The *Management Console* window shows PASS configuration settings.

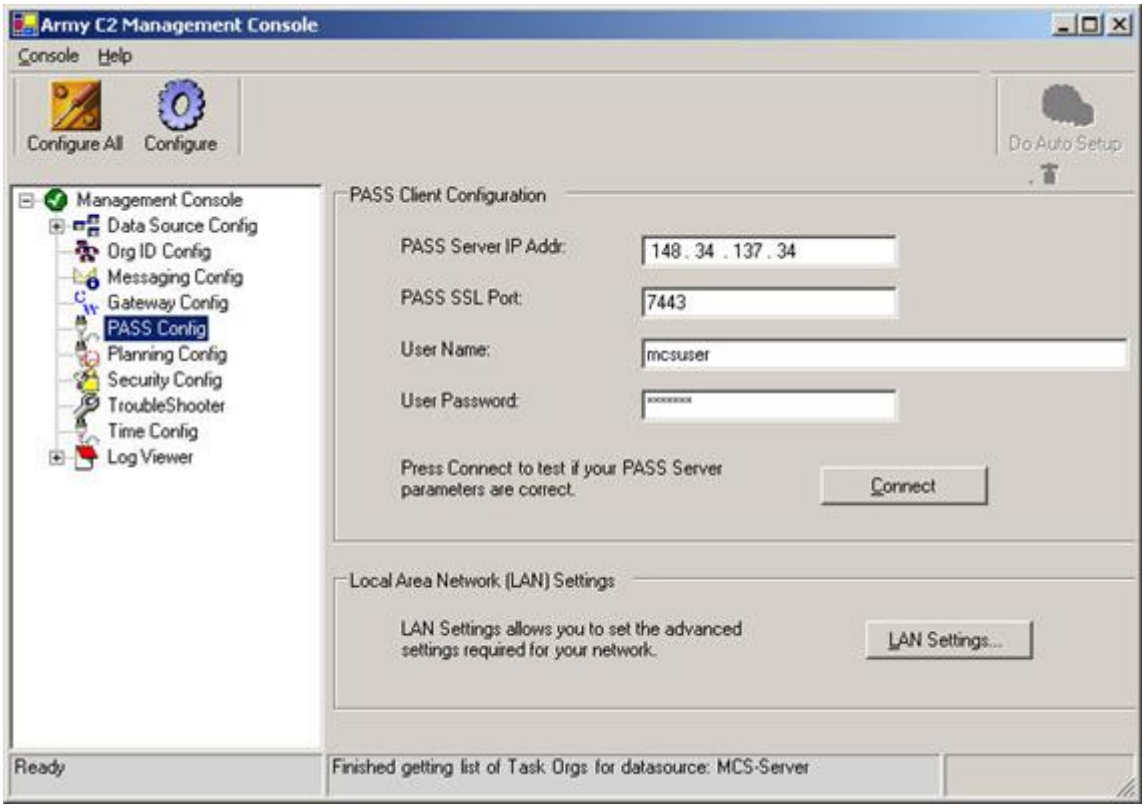


Figure 3-100 PASS Config

2. **Enter** the following data after obtaining site-specific information from your System Administrator:
   - *PASS Server IP Address*
   - *Pass SSL Port*
   - *User Name*
   - *User Password*
3. **Click** the *LAN Settings* button. The *Advanced* window opens.

4. If connecting to a secure socket server, **check** the *Use SSL Authentication* box.

Figure 3-101 PASS LAN Settings Advanced Window

5. If your connection to the PASS Server is through a proxy server, **enter** the necessary information in the *Proxy Server* section. Your System Administrator can tell you whether to use this and what values to enter.
6. **Click** the *OK* button to close the *Advanced* window.
7. **Click** the *Connect* button to validate the connection to the PASS server. A *Connection OK* message appears in the *Army C2 Management Console* window's Status Bar.
8. **Click** the *Configure* button. The workstation connection to the PASS server is now configured.

3-5.8 Planning Configuration

The Planning Config item configures MCS to connect to a web server, which is used to distribute plans.

1. From Treeview, **select** *Planning Config*. The Management Console window displays options for Web Server connection.

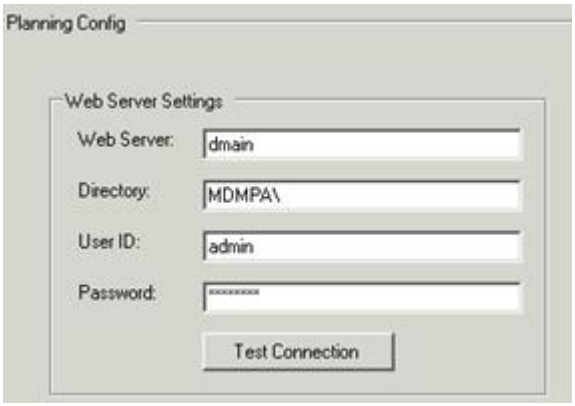


Figure 3-102 Planning Config

2. **Enter** the correct values for the *Web Server* (either IP address or domain name), *Directory* on the server used to store plans, and a valid *User ID* and *Password* required to use the server.
3. **Click** the *Test Connection* button. If connection fails, **confirm** that the correct settings were used, and that the Web Server is up and available.
4. **Click** the *Configure* button on the *Toolbar* to put the new settings in effect.

3-5.9 Configure Security

Following the security policy by adjusting the settings in the Security Access area will help to ensure that information on the system being configured, and on the network, remains secure.

1. From *Treeview*, **select** *Security Config.* The *Management Console* window displays security configuration options.
2. **Check** the *Path* checkbox to set the security level for each of the security settings shown in the *Security Access* area. Green indicates that all users have full security control; Red indicates that only administrators have control. You can obtain the correct settings from your System Administrator.

Figure 3-103 Security Access

3. Under *Set Classification Level*, in the *System Classification* drop-down list, **use** the down-arrow to **set** the appropriate classification level. The text in the Banner Classification Label Text field is updated to reflect the changed classification.

NOTE

For MCS Workstations, the Classification Level is normally set using the AutoSetup Utility. The instructions above would apply to Servers, Gateways, and Workstations unable to use AutoSetup (such as those not on a TOC network).

NOTE

If the Classification Level needs to be increased, obtain the approval of your chain of command.

4. From the *Management Console* toolbar, **select** the *Configure* icon to configure the *Security* settings.

3-5.10 Time Configuration

There are three different roles for time synchronization:

- A Client receives its system time over the network from a time server.
- A Server allows other computers to sync their computer time setting with it.
- A Slave Server does both of these functions. It receives its time from another Time Sync Server, and allows other computers to sync to it.

1. In the *Time Sync Settings* area, **select** a *Time Sync Role*. Normally a MCS Workstation is a *Client*. MCS Gateways and Servers can be any of the roles — consult your System Administrator or unit SOP.

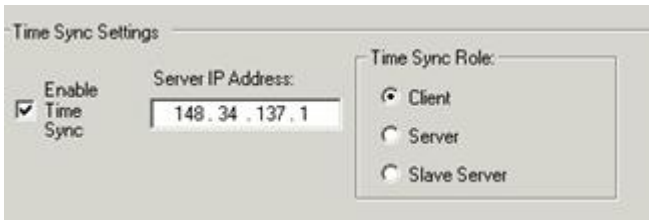


Figure 3-104 Time Sync Settings

2. **Verify** the address in the *Server IP Address box*. The address should be the server providing the time to the workstation. If not correct, enter the correct IP address.
3. **Select** (check) the *Enable Time Sync* checkbox to synchronize this computer's clock with the server.
4. From the *Management Console* toolbar, **select** the *Configure* icon to configure the *Time Sync Settings*.

After completing the configuration, **close** the Management Console by **clicking** the *Close* button at the top right of the window, or **clicking** the *Console* menu and **choosing** *Exit*.

NOTE

For MCS Workstations, the Time Sync Server is normally set using the AutoSetup Utility. The instructions above would apply to Servers, Gateways, and Workstations unable to use AutoSetup (such as those not on a TOC network).

3-6 Additional Army C2 Management Console Functions

3-6.1 Org ID Config-Adding and Deleting Ownership Roles

Ownership roles can be added or deleted by using the *Add/Delete* button on the *Org ID Config* area.

Figure 3-105 Organization ID Configuration Area - Add/Delete Button

3-6.1.1 Add a New Role

1. To **add** a new ownership role, **click** the *Add/Delete* button. The *Add/Delete Roles* window opens.

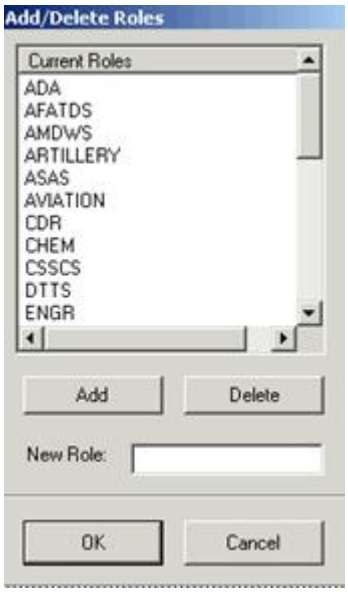


Figure 3-106 Add/Delete Roles Window

2. To **add** a new role to the list in the *My Ownership Role* list in the *ORG ID* pane, **enter** the role name in the *New Role* field of the *Add/Delete Roles* window.
3. **Click** the *Add* button. The new role is added to the list.

3-6.1.2 Delete Roles

1. To **delete** a role, **click** the *Add/Delete* button. The *Add/Delete Roles* window opens (see Figure 3-105).
2. **Select** the role in the *Current Roles* pane.
3. **Click** *Delete.* The role is removed from the list.
4. **Click** *OK* to close the window.

3-6.2 Messaging Troubleshooting

The Army C2 Management Console *Messaging Config* selection includes a troubleshooting tool used to identify messaging failures.

1. **Select** *Messaging Config from the* Treeview. **Select** *Messaging* from the menu bar. The *Messaging* menu opens.
2. From the Messaging menu, **select** *Troubleshoot Message Services* as shown. The Test Messaging Services window opens.

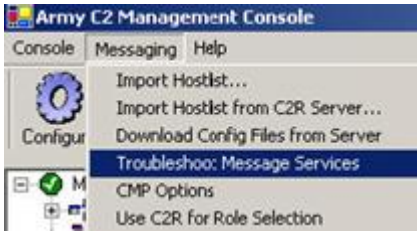


Figure 3-107 Troubleshoot Message Services

3. **Click** the *Test* button in the Test Message Services window to continue.
4. To **view** the test log, **select** the *View Test Log* button. The *test log* opens for viewing.

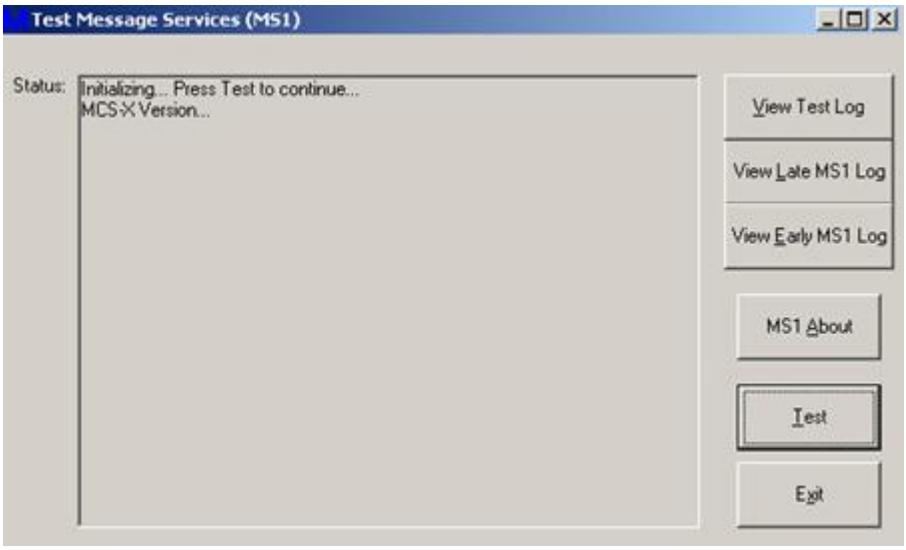


Figure 3-108 Test Messaging Services

5. To **view** the *Late MS1 Log*, **select** the *Late MS1 Log* button. The log opens for viewing.
6. To **start** the *Message Services Troubleshooting* test, **click** the *Test* button.
7. **Click** the *Exit* button to terminate the *Test Messaging Services* application.

3-6.3 CMP Options

The *Common Message Processor* can use one of ten message standards. The message standard which is appropriate varies for each site; refer to site SOP for details.

1. From the *Messaging* drop-down, **click** *CMP Options*.

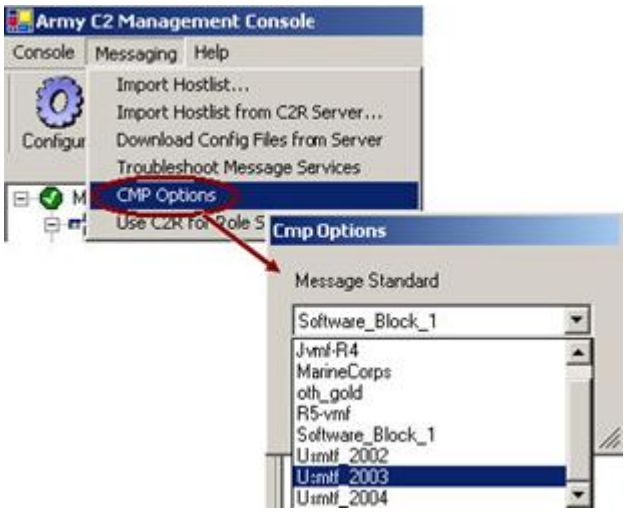


Figure 3-109 Messaging - CMP Options

2. **Click** the down-arrow to display the list of *CMP Options* and **select** the message standard to be used.
3. **Click** the *OK* button to close the *CMP Options* window.
4. From the *Management Console* toolbar, **select** the *Configure* icon to configure Messaging.

3-6.4 AutoSetup Utility

MCS AutoSetup is the fastest, easiest way to configure a MCS Workstation to communicate with a Server. AutoSetup automatically detects AutoSetup Servers on the network and reads settings from them to configure the client system's Data Source, NRTS, PASS, security, and some other settings. The AutoSetup Utility also enables the MAA to change settings for all clients on a LAN in one operation (for instance, to fail over if a PASS server goes off-line).

NOTE

In order to configure an MCS Workstation using AutoSetup, a Server or MCS Gateway must be configured and operational on the TOC LAN.

1. From the Management Console menu bar, **select** the correct server from the *Server List* drop-down list.

Figure 3-110 Server Drop-Down List

NOTE

The System Administrator will define which AutoSetup Server should be used.

2. **Click** the *Do Auto Setup* button.

3. A *Confirm Auto Setup* window opens. **Click** *Yes* to accept the new settings. The workstation is now connected to the AutoSetup Server.

Figure 3-111 Confirm Auto Setup Window

3-7 PASS Failover

3-7.1 Introduction to PASS Failover

Each TOC will be provided with two Battle Command Servers. Each Battle Command Server will run MCS PASS. If one server goes down, PASS failover can be achieved by pointing all PASS clients to the second server. Systems administrators must prepare both machines in advance with the following:

- Common PASS authentication groups (PASSReadGroup, PASSWriteGroup, MCS, ASAS.
- Common PASS users in each group - usually extracted from the ASCIS address book.

If each BCS is joined to the same Active Directory domain, these users and groups can be set in Active Directory Users and Computers.

Unplanned PASS Server Failure assumptions:

- When PASS experiences an unplanned failure, an alternate PASS is available in the TOC or ALOC.
- All BASs must republish data to the secondary PASS server.
- PASS to PASS Server Failover will be refined based on unit needs and organization.
- Two PASSs will be available in Theater, Corps Main and Div Main.

When PASS is configured (personalized) the configuration includes specific activities that must be performed to set up the PASS for a failover.

In the event of a planned or unplanned PASS failure once the configuration has been performed, follow the procedures in the Unplanned Failover Procedures section (below).

NOTE:

Each BAS must develop switchover procedures to available PASS Servers (for example BCS3 checks for server to be up and directs its users accordingly). Primary PASS services that can be used by BASs are: CMP, GTCS, C2R, Alerts, TSAPR, and PASS.

3-7.2 Unplanned Failover Procedures

1. ISYSCON operator notices primary PASS failure on ISYSCON display, or BAS operators notice primary PASS services fail.
2. The G6/S6 gives verbal to TOC to initiate switch to secondary PASS.
3. The G6/S6 is responsible for communicating the secondary PASS IP address to the BASs for redirection purposes.
4. The Commander of that unit rolls over to the identified secondary PASS server.
5. Once the rollover has taken place PASS PUB/SUB service will be handled by the secondary PASS until further notification by the G6/S6.
6. BAS Publishers recreate topics and republish data that has not expired. BAS Subscribers re-subscribe to their topics. All data must be republished by the BASs once connected to the secondary PASS.

3-7.3 Optional: Roll Back To PASS Server (Primary PASS)

1. The Commander of that unit replaces the PASS with the secondary Golden Brick. This brick is already personalized and ready for use.
2. Upon bringing up the secondary Golden Brick, the G6/S6 will then recover the GSALT data from the back up file.
3. The Commander will then verbally notify the BASs to roll back to the original PASS after coming back on line, if necessary. There is the option for the Commander to keep the BASs on the secondary PASS if the situation warrants.

3-7.4 Planned PASS Server Failure

1. The G6/S6 gives a verbal to TOC that the primary PASS Server is going down in 30 minutes (minimum warning time) and for each BAS to initiate switch to alternate secondary PASS.
2. The G6/S6 provides the secondary PASS Server IP address to all BASs.
3. The secondary PASS server is configured to be an active server.
4. **Notify** the BFAs verbally to roll to the secondary PASS.
5. BASs stop interfacing to the primary PASS #1 and switch to alternate secondary PASS in an orderly manner. This includes configuration for PASS and C2R Services.
6. Publishers recreate topics and republish data that has not expired. Subscribers re-subscribe to their topics.
7. The primary PASS server is placed off line.

3-7.5 BAS Reconfigure to Alternate PASS Server

The following procedures are provided as information only and are used by the BASs to connect to the secondary PASS server.

Reconfigure to Resolve Loss of PASS Connectivity.

- A BFA can redirect common software products (C2R, TSAPR, COE Alerts, CMP, GTCS) to use a different PASS Server by updating the server IP in the C2R Configuration GUI.
- **Enter** the IP address of the secondary PASS server in the Server field, then **click** the *Query C2R* button.
- **Click** the *Apply* button then close the application.

Alternatively, a BFA may choose to create its own configuration tool that calls the C2R PASS location configuration API. This will reconfigure Alerts and TSAPR (Time Synchronization and Position Reporting) to point to the new location. APIs are provided for applications to locate the servers. An alert will be generated for notification to use the new PASS server.

NOTE:

Each BAS must republish all Topics and Items to secondary PASS server.

3-7.6 Course Of Action (COA) For TOC BFAs in Unplanned PASS Failure

1. The recommended COA if there is a total PASS server failure.
   - Revert back to the standard Military Messaging.
   - Direct BFAs to connect to MCS in TOC.

Impacts of PASS Becoming Unavailable

Assumptions:

- BFAs were connected with a PASS server to allow initial data to be retrieved.
- Rebooting the PASS server was not successful.
- BFA coordination is required such that all BFA machines move to the same new PASS server back-up together.
- The majority of ABCS 6.4 will operate as described but there are exceptions.
  1. UTR
     - Messages will still get to prior destinations via Unicast if the multicast groups have changed.
     - The PASS server is not required for FBCB2 to reconfigure properly.
  2. ABCS Military Message transmission
     - No impact on transmission. Messages are sent BAS to BAS or BAS to multi BASs. For message transmission, C2R on the PASS server is used for configuration and URN lookups.
  3. Address Resolution
     - Any PASS server in the brigade can be used to obtain multicast data and any PASS server to obtain unicast data.
     - If no PASS server is available, cached multicast groups will still work for destinations within the brigade that have not been effected by a UTR.
  4. PASS
     - Still have messaging and local BAS systems as COP backups.

3-7.7 Detection of PASS Server Failure

1. Loss of PASS server connectivity.
   - It is up to the client applications to recognize the loss of the PASS server.
   - PASS Publishers will detect the loss when they try to publish and get an error condition back.

- PASS Subscribers subscribe to topics with a "time to live" value set. Once this time has passed the subscriber will re-subscribe to PASS. If the PASS server is not available then the client application will get an error condition back.
- C2R API users will get an error condition back.

2. Human Factors
   - CMP GUI users will see an error on the message transmission.
   - The user may notice that updates have stopped for some data.

3-7.8 PASS Server Capabilities

1. Publication and Subscription Services (PASS)
   - Support Information Exchanges
   - Common Input/Output for Disparate Sources
   - SA Over IP XML Translation and to Publish (PASS)
2. WAN Services
   - Ensure Efficient Use of Bandwidth for Data Distribution
3. Master Address Book (C2 Registry)
   - Single Source for Email, Military Messaging, & Web URL
     a. COE Alerts
     b. Time Synchronization and TOC Position Reporting
     c. Communications Server and Message Parser
     d. Military Messaging and Automatic Processing of Situation Awareness Messages in accordance with published BAS Threads

3-7.9 Additional PASS Failover Procedural information

Initial Conditions/Assumptions

1. These procedures are for the PASS functionality to failover from one server to another. BCS supplies functionality in addition to PASS that these procedures do not address.
2. These procedures are an operator/sysadmin initiated manual process. Failover is not an automatic process; see Initial Conditions/Assumptions 3 & 4 below.
3. There are two situations when a PASS failover should be performed: planned and unplanned. In the unplanned situation, the primary PASS node may or may not be operational; however, these procedures are not based on any actions being performed on the machine once it has failed, and so they apply to all situations.
4. The PASS machine that fails will be referred to as the primary or original PASS node; the machine to which the PASS functionality will be moved will be referred to as the secondary or backup PASS node. These procedures cover all of these combinations.
5. If the PASS node encounters connection failures to either publishing or subscribing clients, it will disconnect the offending clients. If the PASS node encounters a "slow" subscriber, it will cancel the subscription and send an unsubscribe message back to the client. Clients should be written to properly handle these situations. If these situations occur repeatedly, the operator/sysadmin/S6 should be notified so that they can initiate the appropriate remedial action, which may be to perform these procedures.

6. No specific method of identifying when the PASS node has failed exists. Upon initial startup, if a client cannot connect to the PASS node, then clearly something is wrong with the PASS node or the network. However, a subscriber cannot tell just from the lack of messages from a PASS node whether the PASS has failed or that a publisher is not publishing. All subscribers may periodically send a PASS command such as "subscribe" or "sync"; no response would indicate that the PASS node had failed; the operator/sysadmin/S6 should be notified so that they can initiate these procedures, when appropriate.
7. These procedures assume that another PASS node exists within the TOC to be used as a backup system.
8. It is assumed that there will be in place a way to keep the primary and secondary (i.e., original and backup) systems in sync with identical user logins and passwords. Refer to the "Set Up the Backup PASS Node" section below for help in performing this function. This procedure must be followed so that all user logins and passwords are on every PASS machine before the failover event; otherwise none of the remaining procedures will work.
9. Each client system (i.e., BAS) must have the ability to change the IP address for its PASS node. In some cases, this may require a BAS system reboot which may be operationally unacceptable; in such cases it is up to the BAS to resolve this issue.
10. It is assumed that all PASS nodes will be configured to use the same Port # for secure communications.
11. There has been no determination of how to decide when to return from the failover configuration to the original configuration. This question must be worked.

Set Up the Backup PASS Node:

1. If PASS authentication is turned off, **skip** to Step 5 (PASS Administration tool). **Export** the PASS node's user/password store into LDIF file format.
    a. Under the Windows 2003 Server operating system, **click** *Start*, then *Programs, Netscape Server Products*, and *Netscape Console 6.x*.
    b. Log on as the Administrator, and give the appropriate password as assigned during installation. Do not change the contents of the Administration URL text box. **Click** OK.
    c. **Navigate** down the tree. As you **single-click** on the desired entry; the next lower level will be displayed.
    d. A series of function tabs will appear. **Click** on *Export Databases*.
    e. To Export User/Passwords, **select** *Subtree*, and then **click** *Browse*.
    f. **Navigate** down the tree. As you **single-click** on the desired entry, the next lower level will be displayed.
    g. At the prompt, **enter** the LDIF file name. **Enter** the desired filename, **click** *OK*, then *OK*, and finally, *Close.*
2. **Email** or **transfer** via floppy or other media the exported *LDIF* file to the PASS node.
3. **Import** the *user/password* stored into the PASS backup node using the *LDIFImporter* tool.
    a. **Run** *d:\bcs\LDIFImporter\bin\runLDIFImporter.bat*.

Figure 3-112 LDIF Importer Window

b. **Enter** the local machine's Netscape Directory Server (NDS) Directory Manager Password, the port that NDS is running on, and the base DN for the machine (domain name in NDS format). (On a default installation of NDS on MCS Gateway the password is mcsuser123, the default port is 390, and Base DN is dc=4id,dc=army,dc=smil,dc=mil.)

c. **Click** the *Browse* button to locate the PASS exported LDIF file on the local machine.

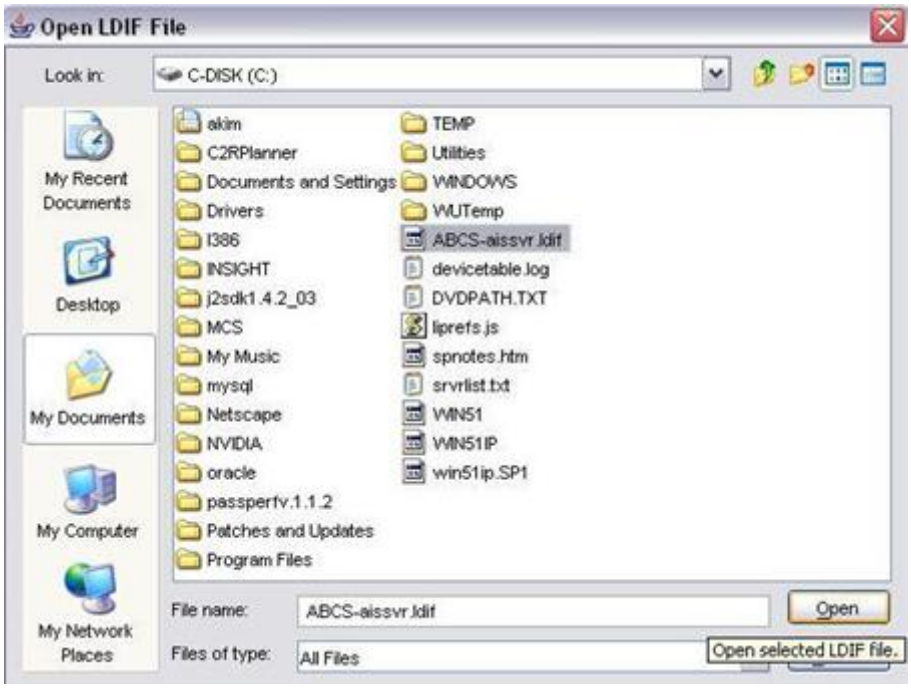


Figure 3-113 Open LDIF File Window

d. After **opening** the LDIF file, **select** the *username/passwords* you want to import into the local Netscape Directory Server and **click** on *Import*.

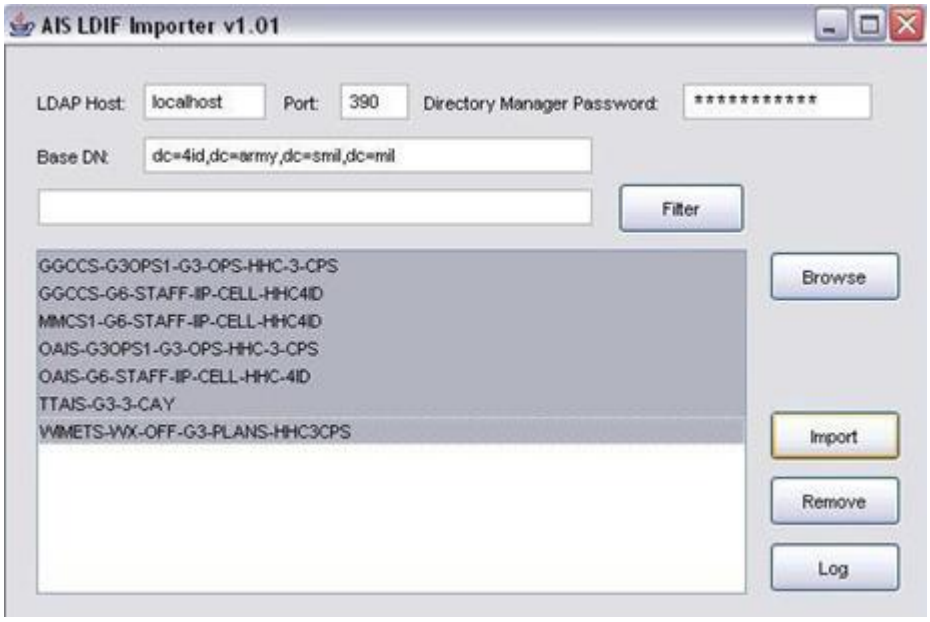


Figure 3-114 LDIF Directory Manager Information Window

e. If done correctly, you should see a message like the following:

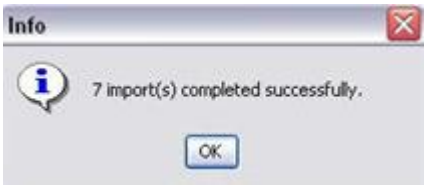


Figure 3-115 LDIF Confirmation Information Window

f. **Close** the LDIFImporter tool after successfully completing the import process.

4. **Set up** the PASS read/write groups through Netscape Directory Server console.

a. **Click** on *Start*, *All Programs*, *Netscape Server Products*, then *Netscape Console 6.x*.

b. **Log on** as admin. (On default MCS gateway install, NDS admin password is "mcsuser123")

c. **Click** on the *Users* and *Groups* tab.

d. **Click** on *Search* with no entered parameters. The imported roles from the previous step are displayed.

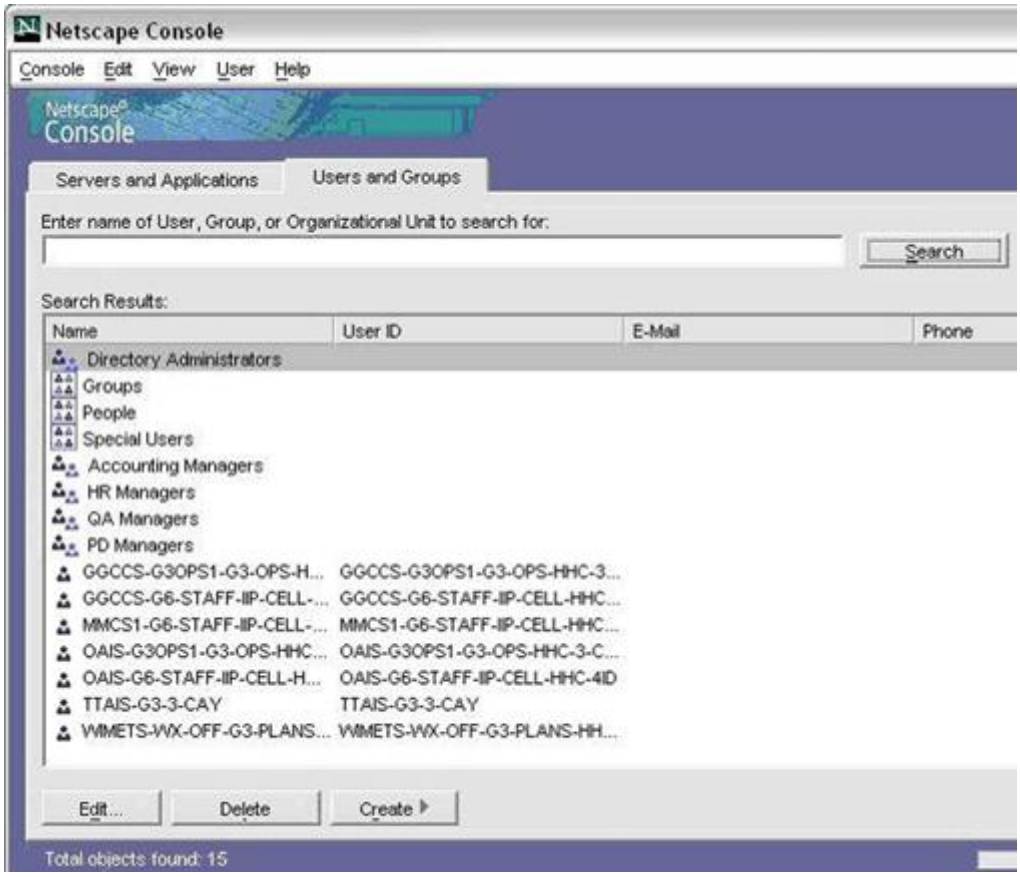


Figure 3-116 Directory Server Console

e. If *PASSWriteGroup* does not exist, you must **create** it. If *PASSWriteGroup* does exist, **skip** to Step e-iv.

i. **Click** on *Create* then *Group*.

Figure 3-117 Select Organization Unit

ii. **Leave** *Base DN* highlighted and **click** on *OK.*

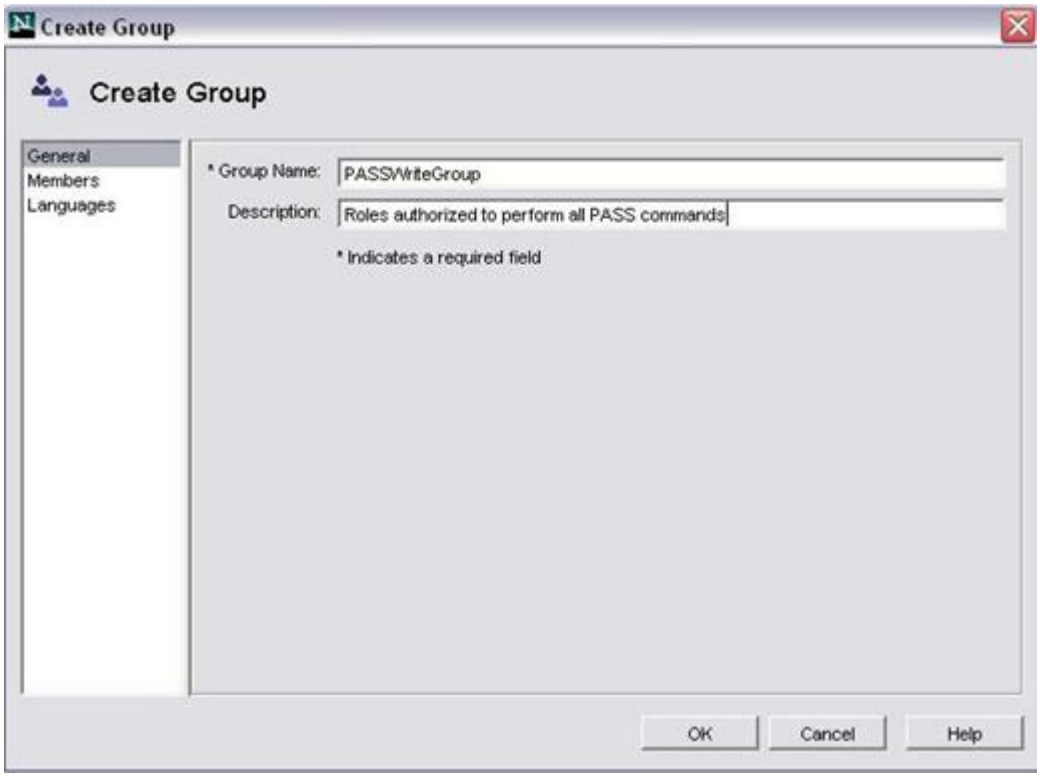


Figure 3-118 Create Group Window

iii. **Type** "PASSWriteGroup" in the *Group Name* field and type "Roles authorized to perform all PASS commands" in the *Description* field.

iv. **Click** on *Members* on the left content pane and then, **click** on *Add,* and the Search users and groups window will be displayed as shown.

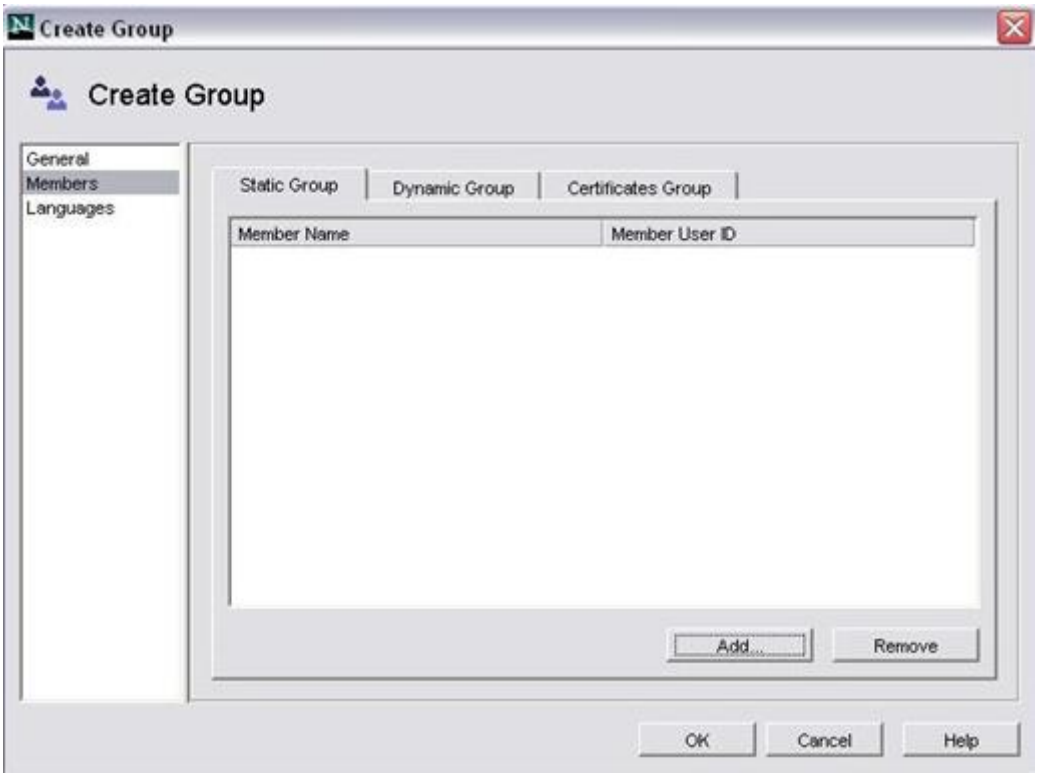


Figure 3-119 Create Members Window

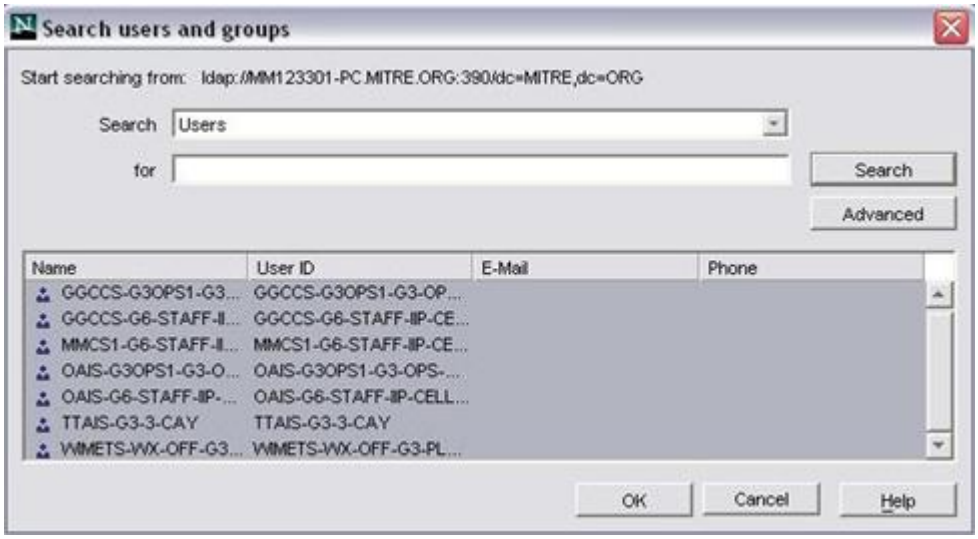


Figure 3-120 Search Users and Groups Window

v. **Click** on *Search* with no parameters.

vi. **Select** the usernames you want added to the *PASSWriteGroup.*

vii. **Click** on *OK* and the Static Group Members window will be displayed.

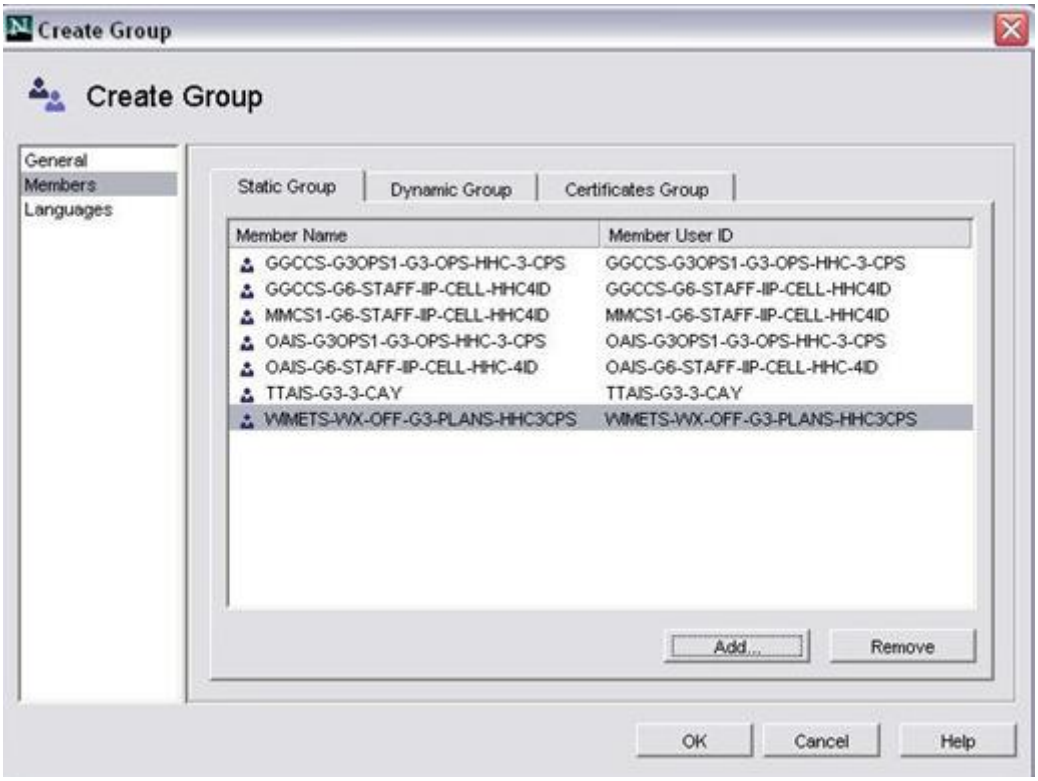


Figure 3-121 Static Group Members

f. If MCS group does not exist, **follow** Steps e-i through e-vi for MCS instead of PASSWriteGroup, adding in only roles that have write access to MCS topics.

g. **Close** *Netscape Console.*

5. On the backup PASS node, **start** or, if already started, **select** *PASS Administration tool*.

a. **Select** the *Forwarding* tab.

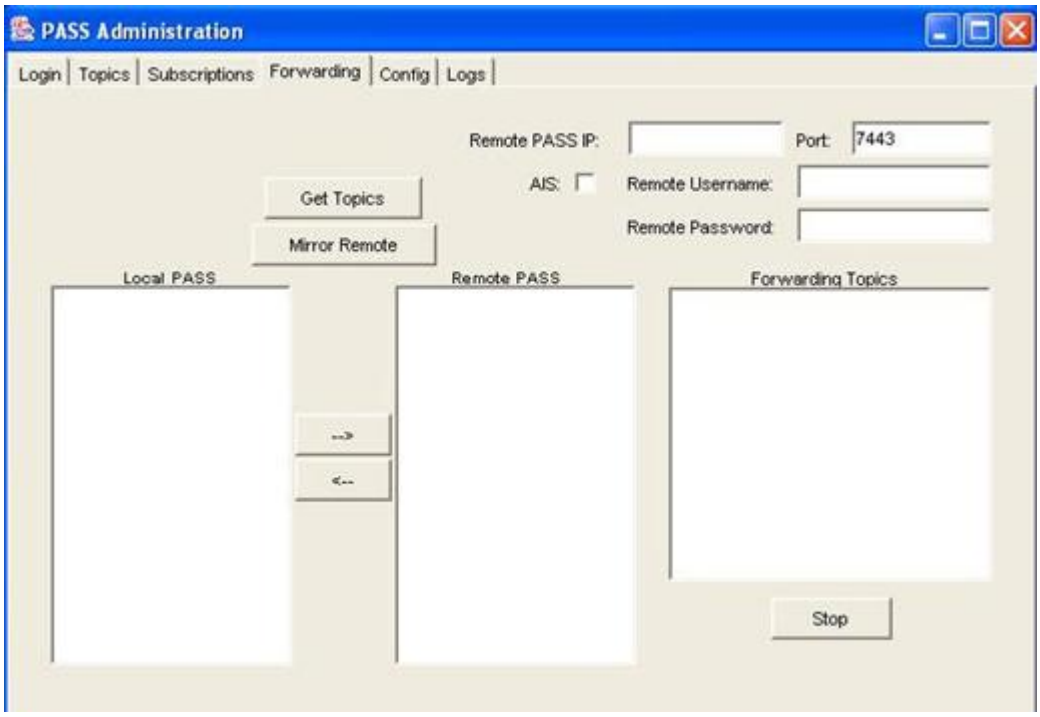


Figure 3-122 PASS Forwarding

b. **Enter** the remote IP address of the primary PASS node.

c. **Enter** the remote port of the primary PASS node. (Default is 7443 for SSL.)

   i. Enter an authorized username/password for access to the primary node.

d. In the *PASS* Administration window, **click** on *Get Topics*.

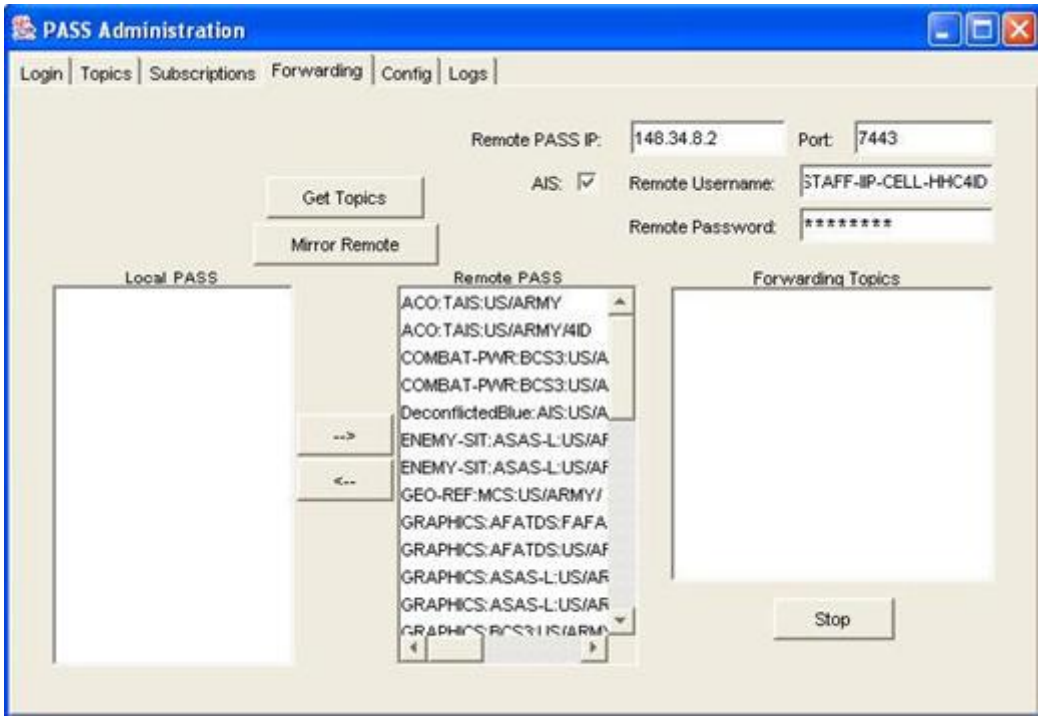


Figure 3-123 Get PASS Topics

e. Then click on Mirror Remote. This gets all topics from the original PASS node, creates duplicates of them on the backup node as open topics, syncs any previously cached items in each topic, and creates subscriptions to the original PASS node topics. Any data entered on the original PASS node will now be mirrored (i.e. duplicated) on the backup node. If at any time new topics are added to the original node or the System Administrator wishes to re-sync the two PASS nodes, click on Mirror Remote.

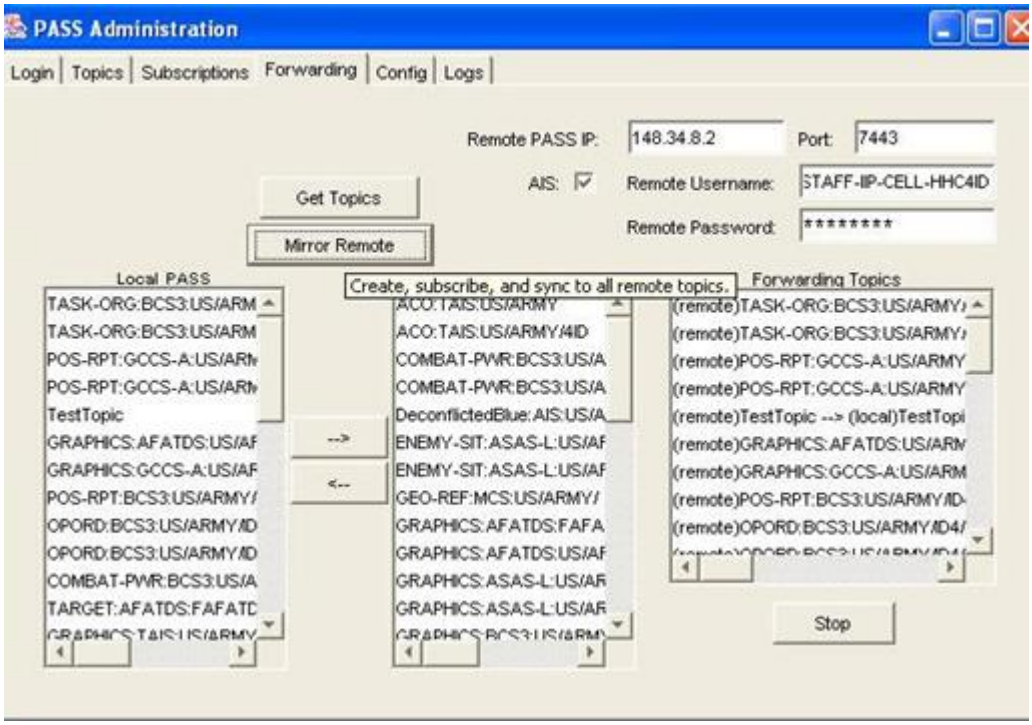


Figure 3-124 PASS Mirror Remote

6. If any new users/passwords are added or changed on the original PASS node, they must also be added to the backup node, or Steps 1-4 must be re-run to get the changes from the primary to the backup.

If the Original PASS Node Goes Down (follow Steps 7-8)**:**

7. Clients and publishers must change to point to the backup PASS node's IP address.
8. All clients must re-subscribe to the topics in which they are interested, and do a "Sync" to these topics in order to obtain any data published since the original node went down and their subsequent re-subscription.

When the Original PASS Node Comes Back Up (follow Steps 9-12):

9. If the user/passwords no longer exist on the original PASS node, or they have changed, they must be manually added into the original node.
10. Clients and publishers must change to point to the original PASS node's IP address.
11. All clients must re-subscribe to the topics in which they are interested, and do a "Sync" to these topics in order to obtain any data published since their switch.

3-8 MCS Auto Setup Utility

3-8.1 Introduction to the MCS AutoSetup Utility

The AutoSetup Utility simplifies the administration of MCS Workstations by letting them read most of their configuration information from a Server or Gateway. This means that setup of a connected Workstation does not include selecting and configuring datasources, NRTS, PASS, Time Server and Planning Server settings, saving the administrator's time. It also allows the

administrator to change settings for all connected workstations from a single central location, without visiting each Workstation.

The utility consists of a tree view listing the DataSources, NRTS, PASS, and other options for Debugging and Instant Messaging. When an item is selected in the tree view, the right pane of the window changes to reflect the options and information associated with the selected item. For example, in Figure 3-125, the *General* item is selected and the right hand pane reflects the General View listing the introduction, legend, and status.
General View

The *Introduction* area describes the AutoSetup Utility.

- The *Legend* describes the color codes used to identify the status of each server, database, etc.
- The *Status* area is a color coded table indicating the availability of a service. Green indicates a connection, yellow indicates a successful ping (without a successful data connection), orange indicates that the connection is currently being automatically tested, blue indicates that the program is waiting for a response and red indicates a broken connection.
- The *Update Status* button makes the AutoSetup Utility re-check the status of all server connections.

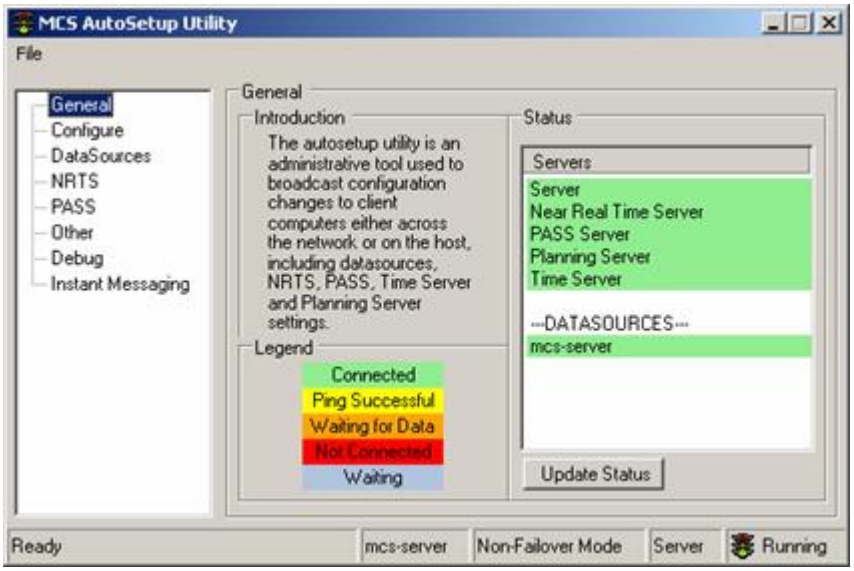


Figure 3-125 AutoSetup Utility General

3-8.2 Starting the MCS AutoSetup Utility

The *MCS AutoSetup Utility* can be started from the *Windows Start* menu.

1. **Click** *Start*, Programs, *MCS*, *Administration*, *AutoSetup Utility*. When the AutoSetup Utility is started, an AutoSetup icon appears in the system tray. From the icon in the system tray, the AutoSetup Utility window can be opened or the user can exit the utility.

Figure 3-126 AutoSetup Utility System Tray Icon

3-8.3 Using the AutoSetup Utility

Each of the settings available within the AutoSetup Utility is described here. To better understand the values associated with each, refer to the configuration checklist.

The appearance of the AutoSetup Utility is the same for both client and server. The difference is that on the AutoSetup Server, many of the settings can be changed, where the client only receives them. All settings not directly set in the AutoSetup Server Utility are set using the Battle Command Server or Gateway's Army C2 Management Console.

Configure

The MCS AutoSetup Configure screen displays the Configuration parameters available. See the figure below. Underlined parameters can be set using the AutoSetup Client.

- *Multicast Address*: The IP address used for multicasting.
- *Multicast Port*: The port numbers associated with the multicast IP address.
- *Broadcast Server*: The Hostname of the server performing the broadcast for service request.
- *Default* button: Used to reset the Multicast Address to the default
- *Apply* button: Used to apply the user settings
- *Communication Status*: The AutoSetup Utility regularly tests its ability to communicate with the AutoSetup Server. It waits *Test Interval* seconds between tests.
- *Update Status*: Used to apply the communication interval setting.
- *Fail Over*: Not implemented at this time.

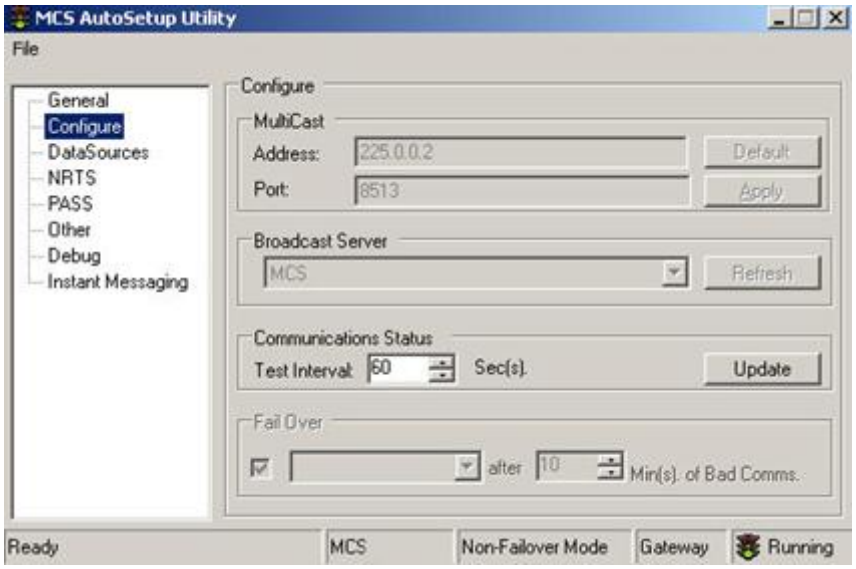


Figure 3-127 AutoSetup Utility Configure

DataSources

The MCS AutoSetup *DataSources* screen displays the DataSource settings available. The following list identifies each of the available options displayed on the screen.

- *DataSource*: List of available MCS databases (including both SQL Server and Access databases).
- *Database*: The name of the database associated with the selected Data Source.
- *Hostname*: The Hostname of the Server.
- *IP Address*: The IP Address of the Server.
- *Test button*: Used to test whether a Data Source is up and running, and can be connected to.
- *Provider*: Type of data base being provided, SQL or ACCESS.
- *server_type_name*: SQL Instance name.
- *Source Name*: Not implemented at this time.
- *Username*: SQL Server User Name required for authentication.

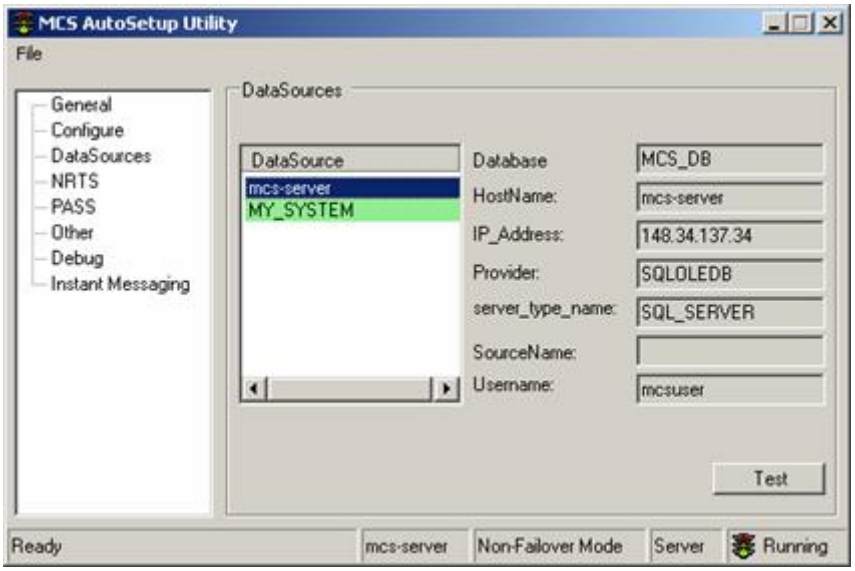


Figure 3-128 AutoSetup Utility DataSources Window

NRTS Primary Server

The MCS AutoSetup NRTS screen displays the NRTS parameters available. The following list identifies each of the available options displayed on the screen.

- *Host IP Address*: IP Address of the NRTS data provider.
- *Full Picture Port*: Port number associated with the NRTS data provider.
- *MultiCast Address*: The multicast IP address used by NRTS to broadcast messages.
- *Injection Port*: Port number used to inject data into other BFA's.
- *Update Port*: Port number used to update NRTS data.
- *Default button*: Used to reset the Primary NRTS setting.
- *Test* button: Used to verify connectivity between the client and the NRTS server.

- *Apply* button: saves and activates changes made to NRTS settings.

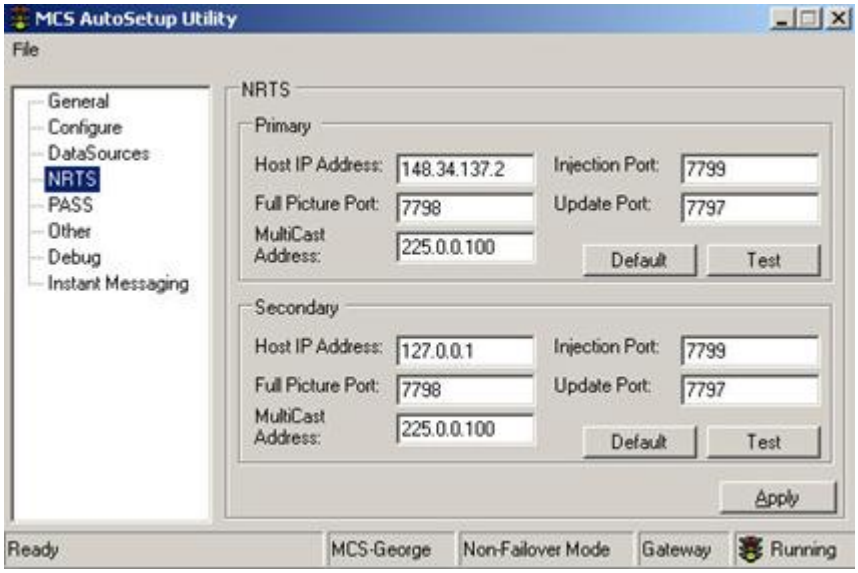


Figure 3-129 AutoSetup Utility NRTS Window

PASS

The MCS AutoSetup PASS screen displays the PASS parameters available. The following list identifies each of the available options displayed on the screen.

PASS Primary Server

- *Host IP Address*: IP Address of the PASS server.
- *HTTP non secure Port*: Port number used to communicate with a PASS server using a non-secure channel.
- *HTTPS secure Port*: Used to communicate with a PASS server if encryption is in use.
- *PASS Authentication* checkbox: Select this box to use Secure Socket Layer (HTTPS), encrypting all communications.
- *Default* button: Used to reset the PASS settings.
- *Test* button: Used to verify the settings for a PASS server.

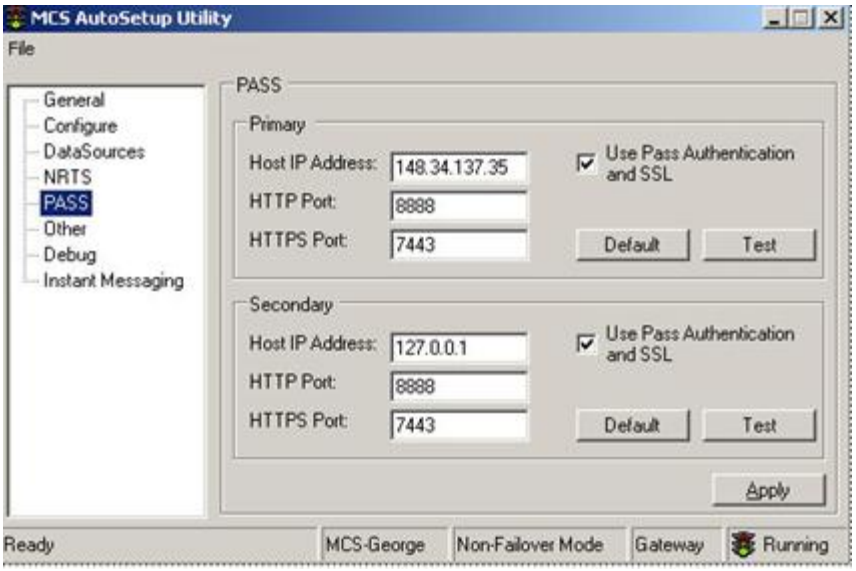


Figure 3-130 AutoSetup Utility PASS Window

Other

The MCS AutoSetup Other screen displays the settings not included in the other categories. The following list identifies each of the available options displayed on the screen.

- *Time Server IP*: IP Address of the Network Time Server, normally the Unit Server or the PASS Server.
- *Web Server*: URL of the Unit's Web Server, normally the Unit Server.
- *Security Classification*: Drop down list, offering Unclassified, Confidential, or Secret.
- *Security Banner Label:* The text here will be displayed in the Classification Banner as the system's Classification Level.
- *Apply* buttons: Use to allow the user to apply the associated selected values.
- *Default* buttons: Used to reset the associated setting.

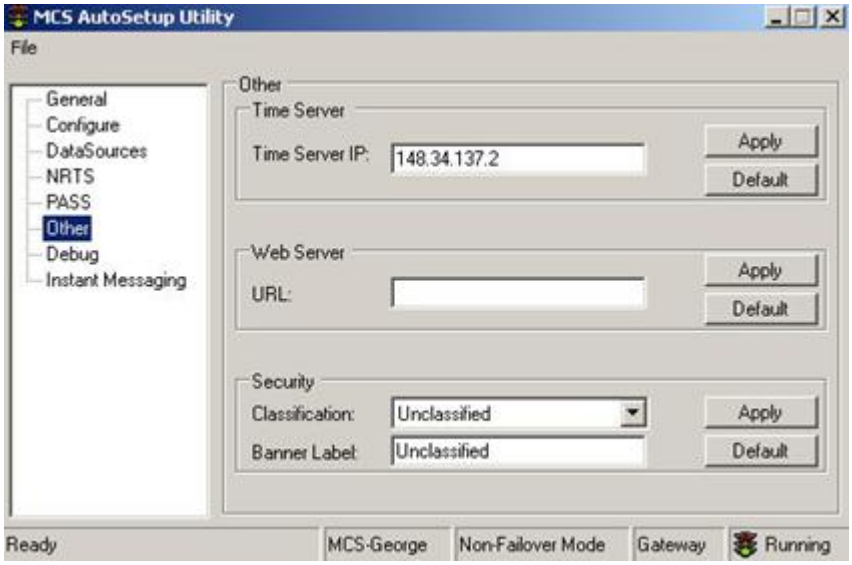


Figure 3-131 AutoSetup Utility Other Window

Debug

The MCS AutoSetup Debug screen displays the various debug tabs. The following list identifies each of the available options displayed on the screen. "Messages" for all these options means messages sent from one AutoSetup Utility program to another AutoSetup Utility on a different computer. The Debug functions are intended for use by the System Administrator in identifying problems.

- *Sent Messages* Tab: Displays the raw text message sent.
- *Received Messages* Tab: Displays the raw text message received.
- *Log* Tab: Displays a log of received, connected, and various status messages.

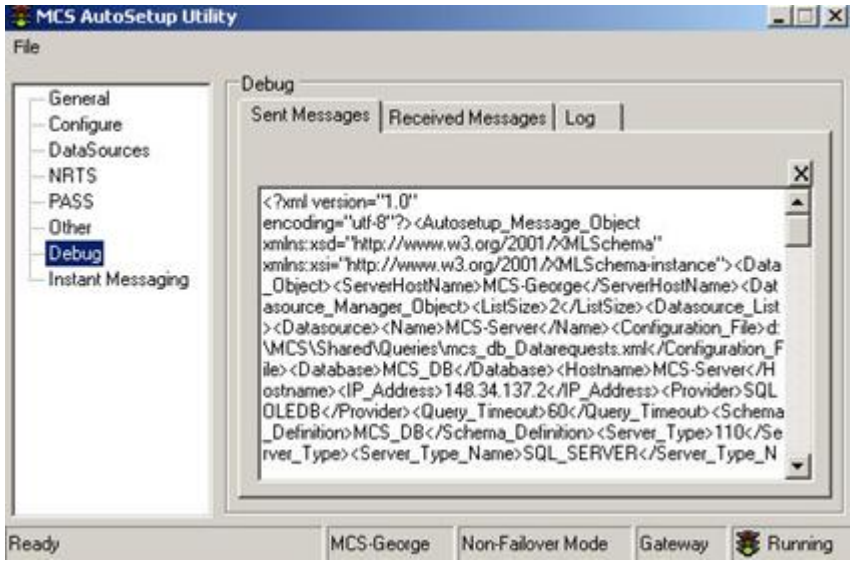


Figure 3-132 AutoSetup Utility Debug Window

Instant Messaging

The MCS AutoSetup Instant Messaging window allows for instant communication between MCS Users. The top portion of the Instant Messaging pane displays the most recent messages transmitted between MCS Users. See the figure below for the location of each of these features.

1. **Enter** text in the lower pane of the *Instant Messaging* window.
2. **Click** the *Send* button to broadcast a message to anyone viewing the MCS AutoSetup Utility on their MCS system.

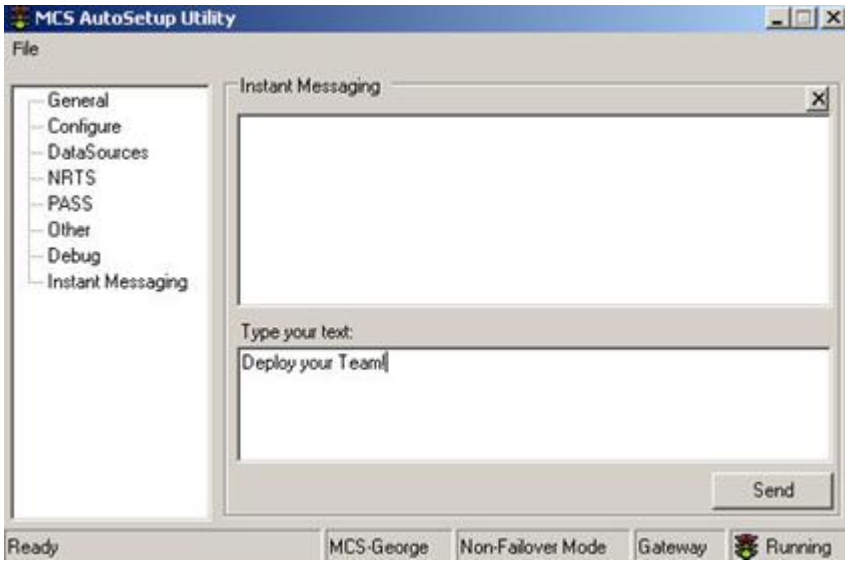


Figure 3-133 AutoSetup Utility Instant Messaging Window

3-9 Internet Relay Chat

3-9.1 Introduction to Internet Relay Chat

Internet Relay Chat (IRC) is a communications tool which allows people to communicate in real-time, sending and receiving text messages.

IRC gained international fame during the Gulf War in 1991, where updates from around the world came across the wire, and most IRC users who were online at the time gathered on a single channel to hear these reports. IRC had similar uses during the coup against Boris Yeltsin in September 1993, where IRC users from Moscow were giving live reports about the unstable situation there.

3-9.2 Installation of Internet Relay Chat

The IRC application can be installed on the Server, Gateway, or Client system. To install the IRC client onto your MCS system, follow the steps below.

1. **Open** the Windows Explorer and locate the folder *<drive letter>:\MCS\Installation Programs\IRC Install*.

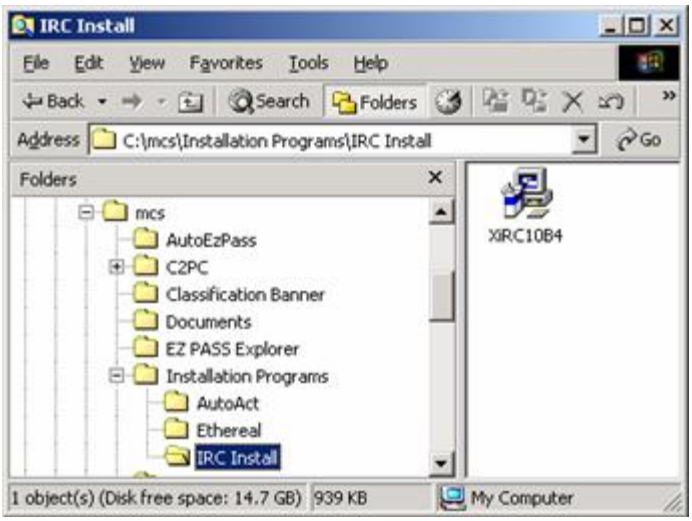


Figure 3-134 Locate IRC Installation Application

2. **Double-click** the installation program file "*XIRC1084.exe*", to start the installation application. The installation script will start as shown below.

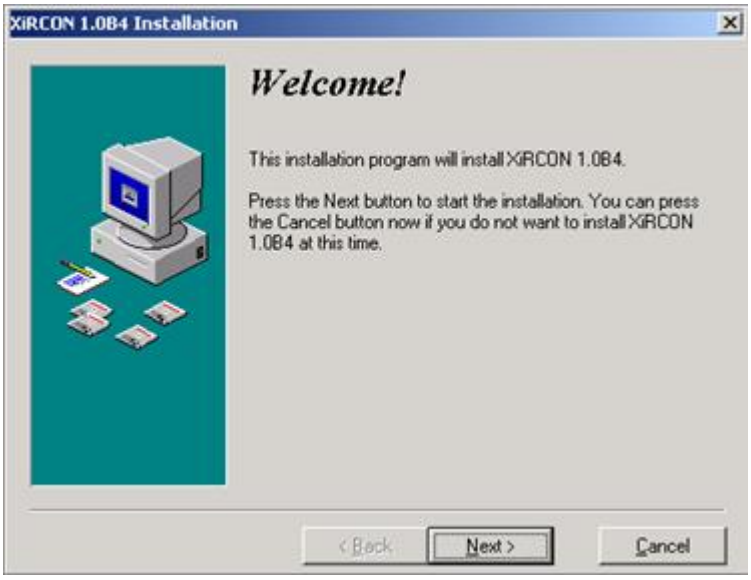


Figure 3-135 IRC Install Wizard – Welcome

3. **Click** *Next* to continue. The *Select Destination Directory* screen will be displayed.

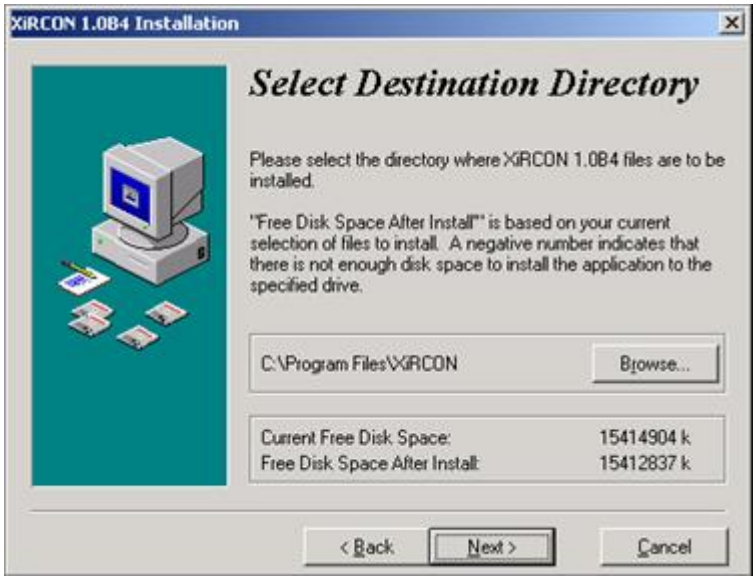


Figure 3-136 IRC Install Wizard - Select Destination Directory

4. Unless otherwise instructed by your Unit SOP, do not change the default installation path. **Verify** there is sufficient disk space to perform the installation as described in the *Select Destination Directory* screen. **Click** *Next* to continue, the *Backup Replace Files* screen is displayed.

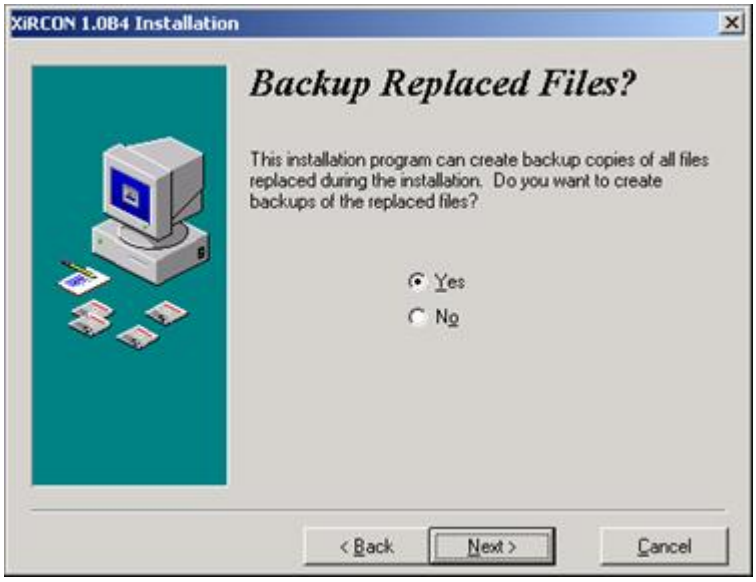


Figure 3-137 IRC Install Wizard - Backup Replaced Files

5. Once you have chosen whether or not to save the replaced files, **click** the *Next* button to continue. The *Select Backup Directory* screen will be displayed if you have chosen to back up replaced files. Otherwise, the Ready to Install screen will appear — go to Step 7.

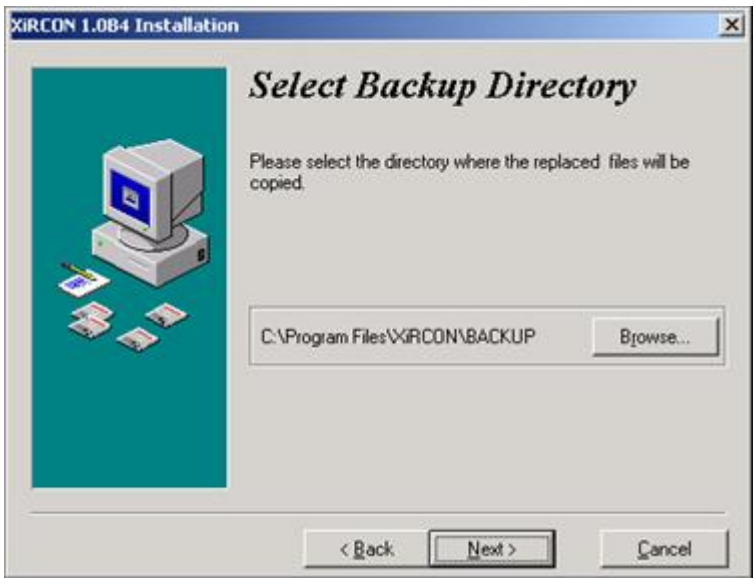


Figure 3-138 IRC Install Wizard - Select Backup Directory

6. **Click** the *Browse* button and **locate** the directory where you would like to install the IRC software. Unless instructed otherwise by your Unit SOP, use the default path. **Click** the *Next* button to continue, the *Ready to Install* screen will be displayed.

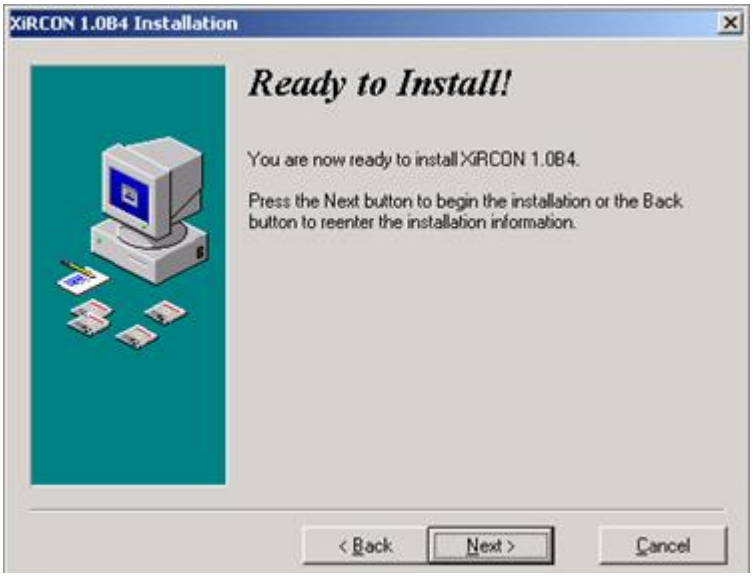


Figure 3-139 IRC Install Wizard - Ready to Install

7. Configuration is complete and you are ready to being the installation. **Click** the *Next* button to begin the installation, or the *Back* button to alter the configuration settings you have previously entered. When the *Next* button is clicked, a progress screen will be displayed, followed by the *Installation Complete* screen.

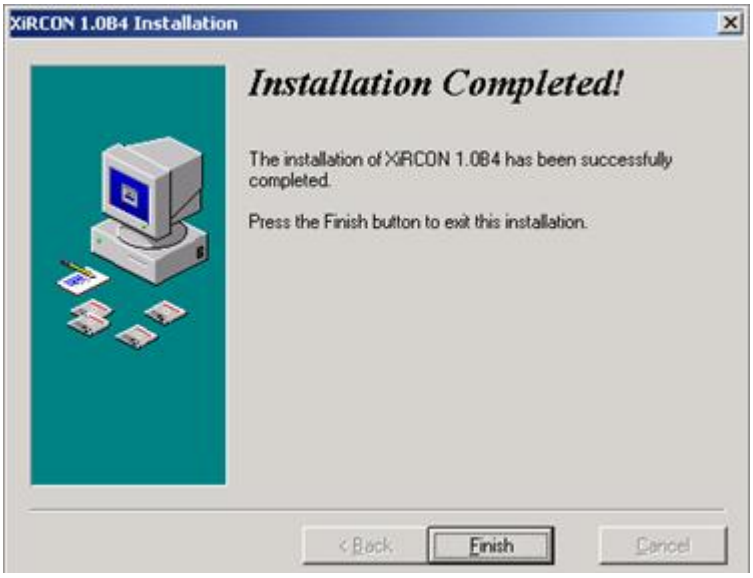


Figure 3-140 IRC Install Wizard - Installation Completed

8. The IRC has been successfully installed. **Click** the *Finish* button to close the Installation Wizard.

3-9.3 Configuring Internet Relay Chat

3-9.3.1 XIRCON Readme File

It is recommended that you look at the XIRCON Readme file before using IRC. To view the file, from the Windows task bar, **click** *Start*, *Programs*, *XIRCON*, *Readme*. The Readme file will be displayed using the Notepad.

3-9.3.2 XIRCON

XIRCON can now connect to an IRC server. Contact your System Administrator for information on available IRC servers. For each server, you will need its network name and hostname.

The following steps describe how to configure the IRC Client.

1. From the Windows Task Bar, **click** *Start, Programs, XIRCON, XIRCON*. XIRCON starts.

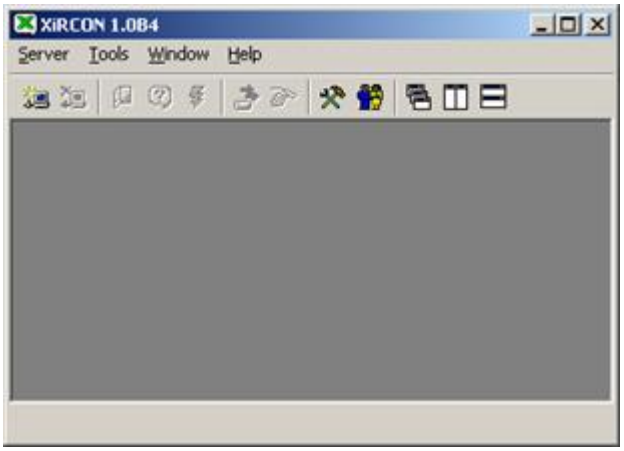


Figure 3-141 XIRCON

2. To connect the application to an IRC Server, **click** *Server*, *Connect* in the menu bar. The XIRCON *Connect* window opens.

Figure 3-142 XIRCON Menu Bar

Figure 3-143 XIRCON Connect Window

3. To add a server to the list in this window, **right-click** in the *Servers* area and **select** *Add*. The *Add Server* window opens.

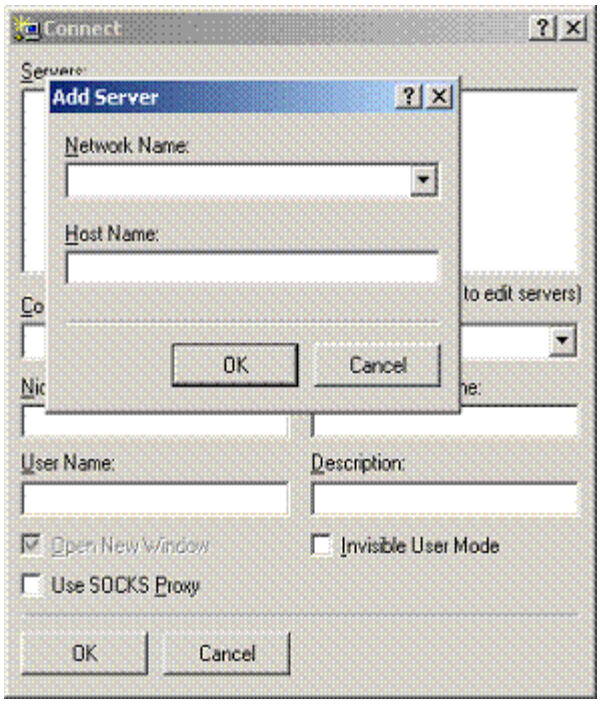


Figure 3-144 XIRCON Add Server Window

4. **Enter** the information supplied by your Unit System Administrator, then **click** *OK*.
5. For additional information about the XIRCON application for IRC **visit** *www.xircon.com*.

Chapter 4 Troubleshooting MCS Software

4-1 Resources for Troubleshooting MCS Software

4-1.1 Introduction to Resources for Troubleshooting MCS Software

CAUTION

Workstations and Gateways must be rebooted every 24 hours.

Servers must be rebooted every 72 hours.

The following resources are available when troubleshooting the MCS software:

- MCS release notes.
- Online help is available with each of the MCS applications.
- Log files for each of the software applications.

In addition to these resources, the MCS Management Console contains a built in troubleshooting utility. This utility can be used to perform the following tasks:

- Reinstall MCS Path
- Re-register the COM components (RegArmy)
- Perform minor registry repairs (RegClean)
- Remove each instance of a specified component (RegPurge)
- Utility for testing messaging connectivity
- Utility for testing C2R connectivity

Terms

- TTL (Time To Live) - tells a network router if the packet has been in the network too long and should be discarded. Each router that receives a packet subtracts one from the count in the TTL field. When the count reaches zero, the router detecting it discards the packet.
- HTTP (HyperText Transfer Protocol) – HTTP is the set of rules for transferring files on the internet. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols.
- SSL (Secure Sockets Layer) - SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. The “sockets” part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system.
- HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) – HTTPS is a Web protocol developed by Netscape that encrypts and decrypts user requests as well as the data that is returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

4-1.2 Release Notes

The Release Notes included with MCS provide the user with valuable last minute information which may not have been included in the final MCS documentation. The content of the release notes varies from release to release, however, the following information is normally available.

- A brief introduction to describe the information included in the release notes.

- The Release History, listing the date of each release, a short description to identify the purpose of the release, and a numeric value indicating the version of each release.
- Installation instructions which describe the steps necessary to install the release. A full release will be installed on all MCS systems (Workstation, Gateway, Server) computers. A patch release will identify which MCS systems are effected by the patch release.

4-1.3 Online Help

MCS includes online help to assist the user with operating and supporting MCS. Each of the applications available in MCS provides the user with online help to assist using the program. Online help is an interactive application, which allows you to locate valuable application information through a variety of methods (i.e. Help by Contents, Index, and Search by Keyword). The following steps describe how to access online help from within the Management Console.

1. From the Management Console, **click** *Help* on the menu bar. A Help drop-down menu opens.

Figure 4-1 Management Console Help down-arrow Menu

2. **Click** *Management Console Help*. The MCS *Management Console Help* opens.

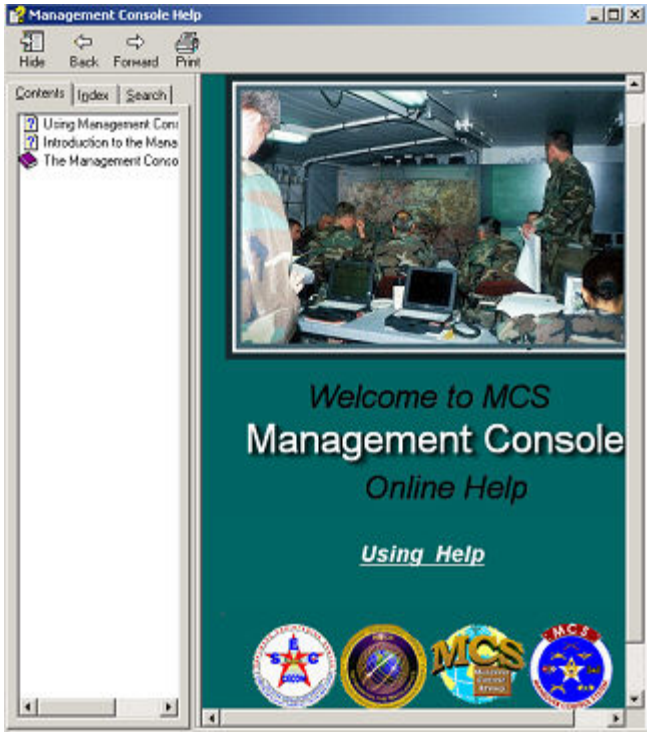


Figure 4-2 Management Console Help

There are three tabs on the *Management Console Help* screen: *Contents, Index and Search.*

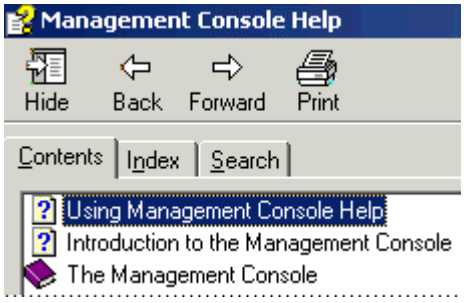


Figure 4-3 Management Console Help Tabs

- To **locate** information by topic, **select** the *Contents* tab.
- To **locate** information by index, **select** the *Index* tab.
- To **locate** information by keyword, **select** the *Search* tab.

4-1.4 Log File

Log files provide important information, which can be used to locate and identify a failure during installation or the operation of the MCS Software.

The Army C2 Management Console provides two ways to view log files:

- View Log File option on the Console menu
- Log Viewer in the Management Console treeview.

To view a log file using the View Log File option, follow these steps:

1. **Select** *Console* from the *Management Console* menu bar. The Console drop-down menu opens.

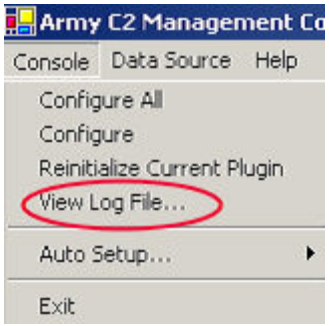


Figure 4-4 Management Console down-arrow Menu

2. **Select** *View Log File* from the *Console* drop-down menu. The Management Console log file is displayed in an Internet Explorer window.
3. **Use** the *scroll bars* on the side and bottom of the window to move through the entire log file.

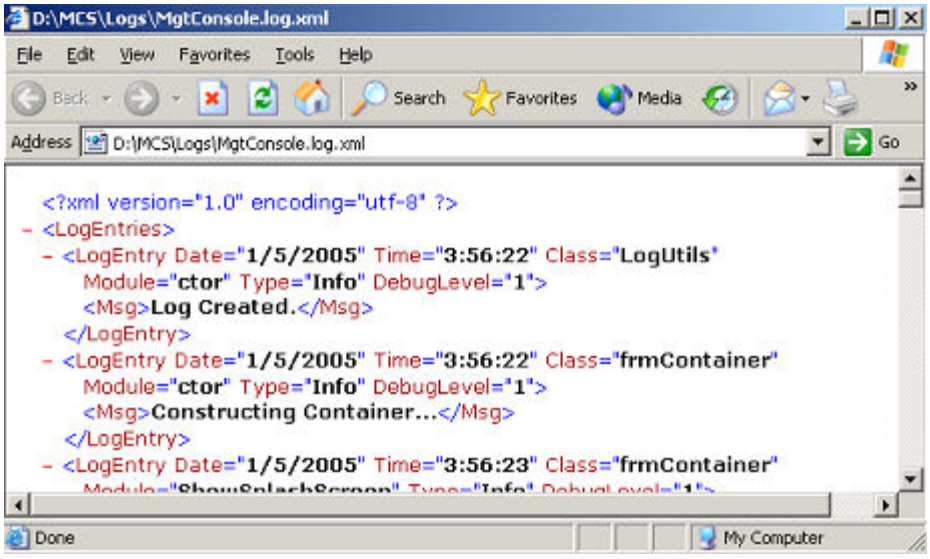


Figure 4-5 View Log File

4. To **exit** the log file viewer, **click** the *X* in the upper right corner of the window, or **select** *Close* from the *File* drop-down menu.

   To **view** log files through the Management Console Explorer Log View, **follow** the steps below:

CAUTION

Never open more than one (1) instance of the DAS Viewer

5. In the treeview area, **click** *Log Viewer*. Icons for each of the log files appear in the pane on the right side and in the treeview.

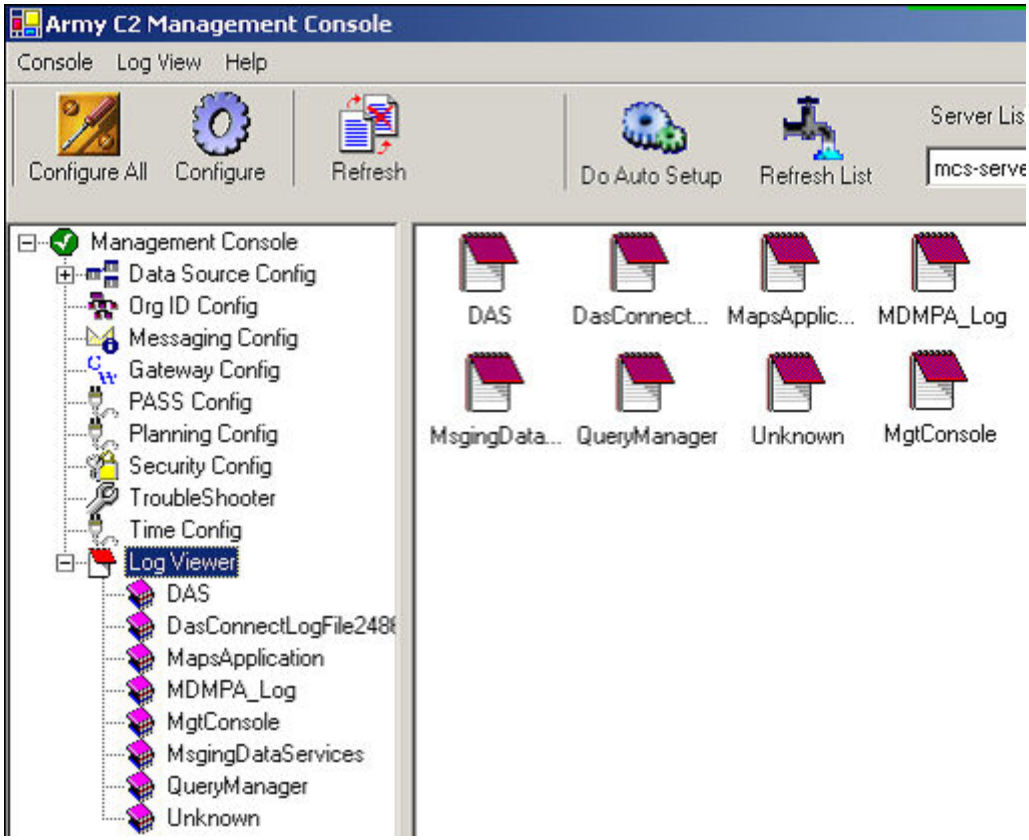


Figure 4-6 Management Console Log Viewer

The following files may be available depending on system usage:

- Data Transaction Viewer or Data Acquisition System (DAS)
- MDMPA configuration
- MDMP Log configuration
- Management Console configuration
- Messaging Data Services configuration
- Message Wrapper
- Query Manager

6. **Select** the desired log file from the treeview area or **double-click** the desired icon from the right side area. The log file opens in a new window. A section of a log file is shown.

Type	Message	Class	Module	Date	Time
Info	Log Created.	LogUtils	ctor	6/16/2004	12:54:20
Info	Constructing Container...	frmContainer	ctor	6/16/2004	12:54:20
Info	Exiting constructor...	frmContainer	ctor	6/16/2004	12:54:20
Info	Checking ActiveX registrations.	InstallUtils	RegisterComponents	6/16/2004	12:54:20
Info	Registering Msging type lib...	InstallUtils	RegisterComponents	6/16/2004	12:54:20
Info	Registering McsLight type lib...	InstallUtils	RegisterComponents	6/16/2004	12:54:20
Info	Getting global variables...	InstallUtils	GetGlobalVars	6/16/2004	12:54:21
Info	MCS Install Dir: c:\mcs\	InstallUtils	GetGlobalVars	6/16/2004	12:54:21
Info	Searching for PlugIn XML files...	Plug_Ins	FindPlugIns	6/16/2004	12:54:21
Info	Adding found plugins:	Plug_Ins	FindPlugIns	6/16/2004	12:54:22
Info	Data Source Config	Plug_Ins	FindPlugIns	6/16/2004	12:54:22
Info	Gateway Config	Plug_Ins	FindPlugIns	6/16/2004	12:54:22

Figure 4-7 Management Console Log View Sample

In addition to viewing the Management Console log files, additional log files are available and can be viewed using the Microsoft Notepad application. Below are a few samples of additional log files available for viewing:

- C:\McsInstall.log
- C:\McsMessaging.msi.log
- C:\taskorg.log
- C:\VLSTrack.msi.log
- C:\MCS\Classification Banner\Banner.log

4-2 Management Console Troubleshooting Utility

4-2.1 Introduction to Management Console Troubleshooting Utility

The MCS Management Console Troubleshooting Utility provides a variety of tools to assist in locating and correcting problems within MCS.

The following steps describe how to execute each of the troubleshooting tools available within the MCS Troubleshooter Utility.

CAUTION

These troubleshooting utilities should be used with care by experienced system administrators.

1. From the *MCS Management Console*, **select** the *TroubleShooter* icon in the left side area. The *TroubleShooter Selections* appear in the treeview area of the MCS Management Console.

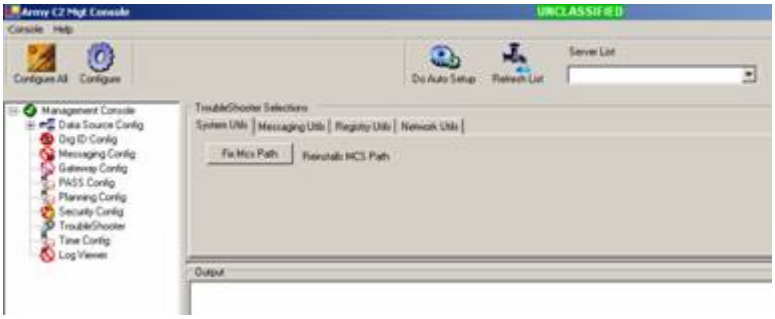


Figure 4-8 Troubleshooter icon

The *Troubleshooter Selections* window consists of four tabs: System Utils, Messaging Utils, Registry Utils, and Network Utils. Each of the tabs contain one or more tasks used to troubleshoot MCS.

- The System Utils tab contains the Fix MCS Path utility.
- The Messaging Utils tab contains utilities for testing messaging and C2R: the MS1 utility tests messaging connectivity and the WS1 utility tests C2R connectivity.
- The Registry Utils tab contains three utilities: RegArmy, RegClean, and RegPurge.
- The Network Utils tab provides a couple of tests to determine if the network is operational.

4-2.2 System Utils

To correct problems with the MCS path, follow these steps:

4-2.2.1 Fix MCS Path

1. **Click** the *Fix MCS Path* button on the *System Utils* tab. The Output window displays the results of running the Fix MCS Path utility.

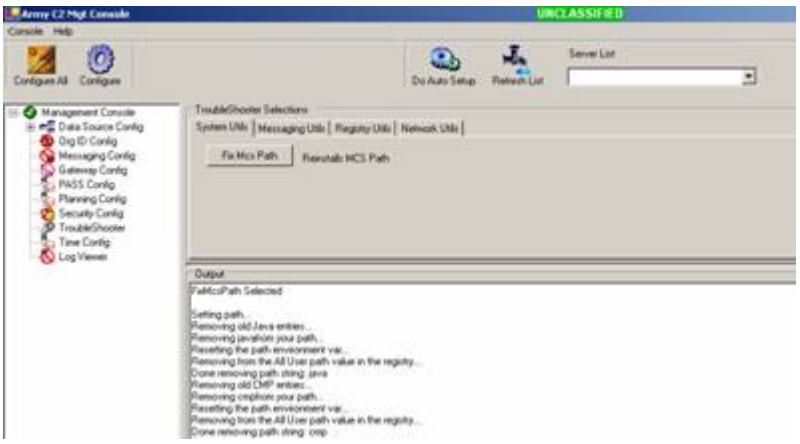


Figure 4-9 System Utils – Fix MCS Path Output

4-2.3 Message Utils

The *Messaging Utils* tab contains two utilities for testing messaging:

- MS1 - the messaging utility for testing messaging connectivity.

- WS1 - the messaging utility for testing C2R connectivity.

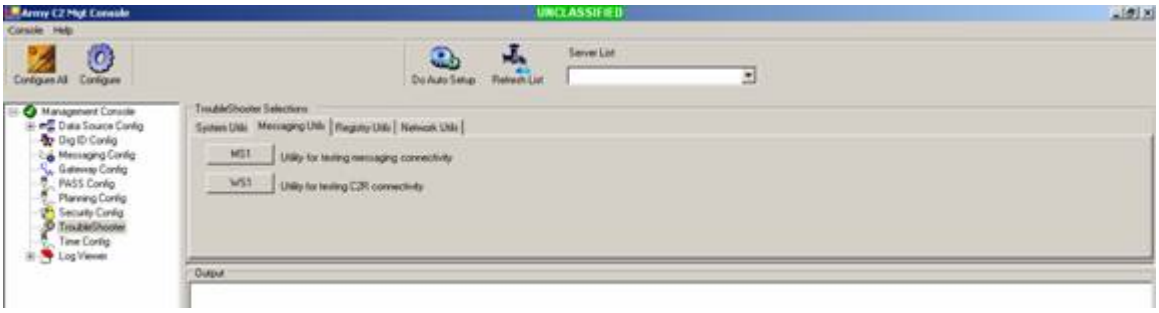


Figure 4-10 Messaging Utils Tab

4-2.3.1 MS1 Messaging Utility

The *MS1* button launches the test of messaging connectivity. Follow these steps to run MS1 messaging utility:

1. To **test** messaging connectivity, **click** the *MS1* button. The *Test Message Service*s window opens.

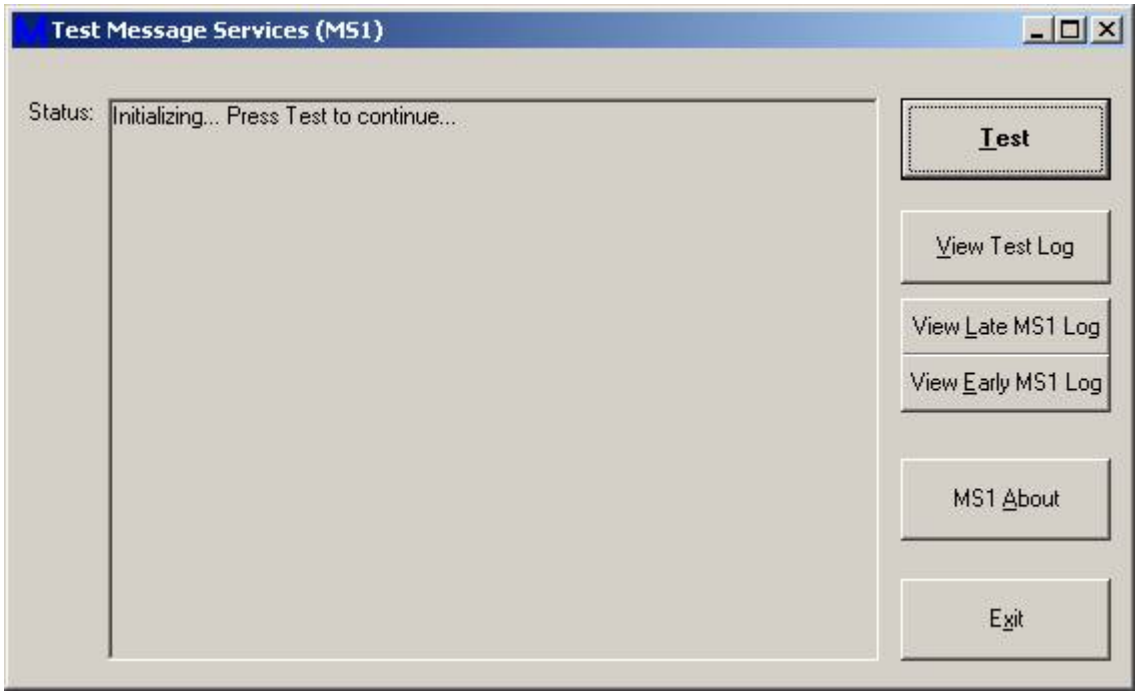


Figure 4-11 Test Message Services Window

2. **Click** the *Test* button in the Test Message Services window. The test results are displayed in the Status area.
3. When testing is completed, **click** the *Exit* button to close the Test Message Services window.

4-2.3.2 WS1 Button

1. To **test** C2R connectivity, use the WS1 button on the Messaging Utils tab.
2. **Click** the *WS1* button in the *Messaging Utils* tab and the C2R utility window is displayed.

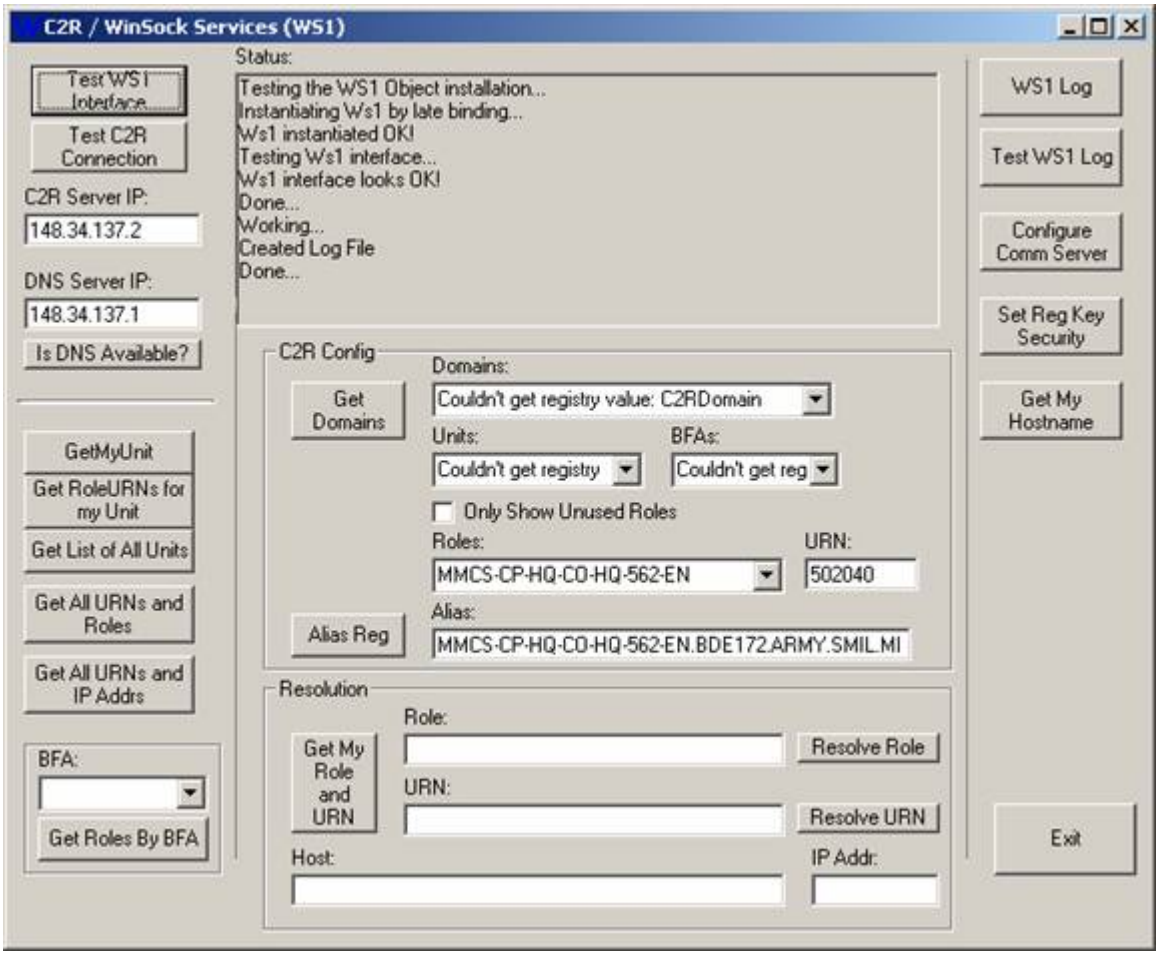


Figure 4-12 C2R Connectivity Test

3. **Click** the *Exit* button to close the WS1 utility

4-2.4 Registry Utils

To run one of the three registry utilities, follow these steps:

1. To **run** registry utilities, **click** the *Registry Utils* Tab in the *TroubleShooter Selections* area. The *Registry Utils* tab opens.

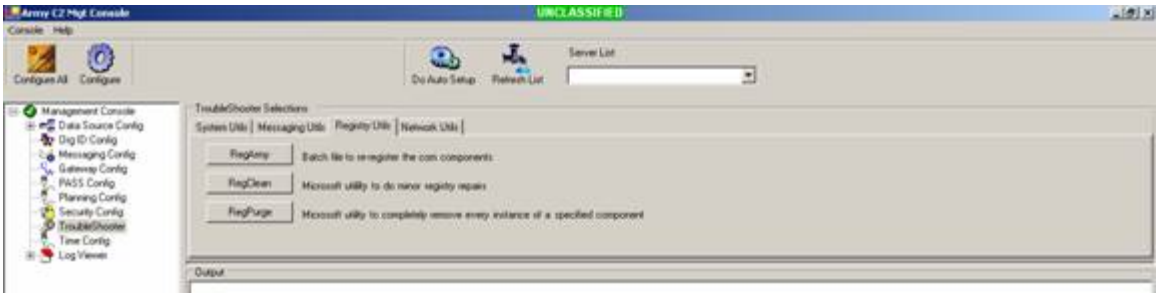


Figure 4-13 TroubleShooter Selections - Registry Utils Tab

4-2.4.1 RegArmy Button

1. To **re-register** the *COM components* of MCS, **click** the *RegArmy* button. The utility is launched. The results of the RegArmy utility are displayed in the command window.

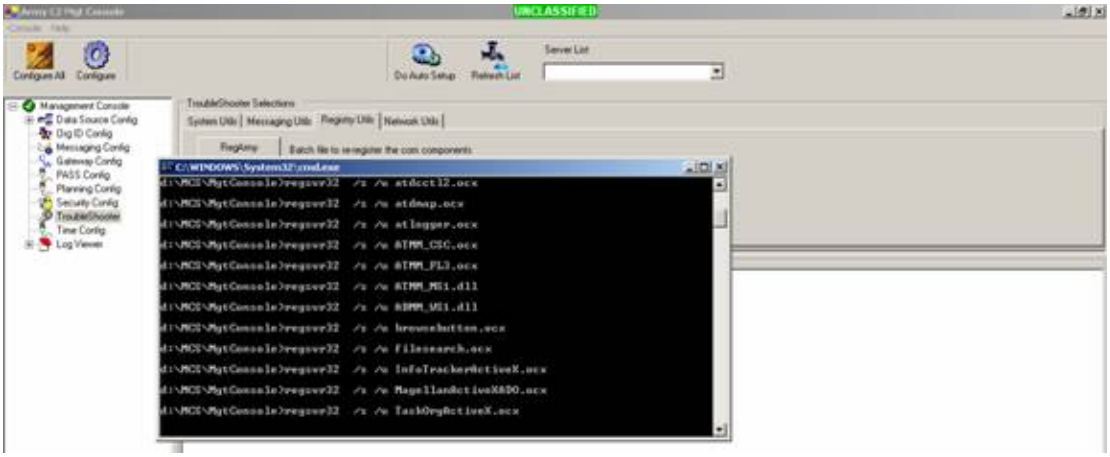


Figure 4-14 RegArmy Utility Output Display

4-2.4.2 RegClean Button

1. To **run** the *Microsoft RegClean* program, **click** the *RegClean* button on the *Registry Utils* tab. The RegClean window opens.

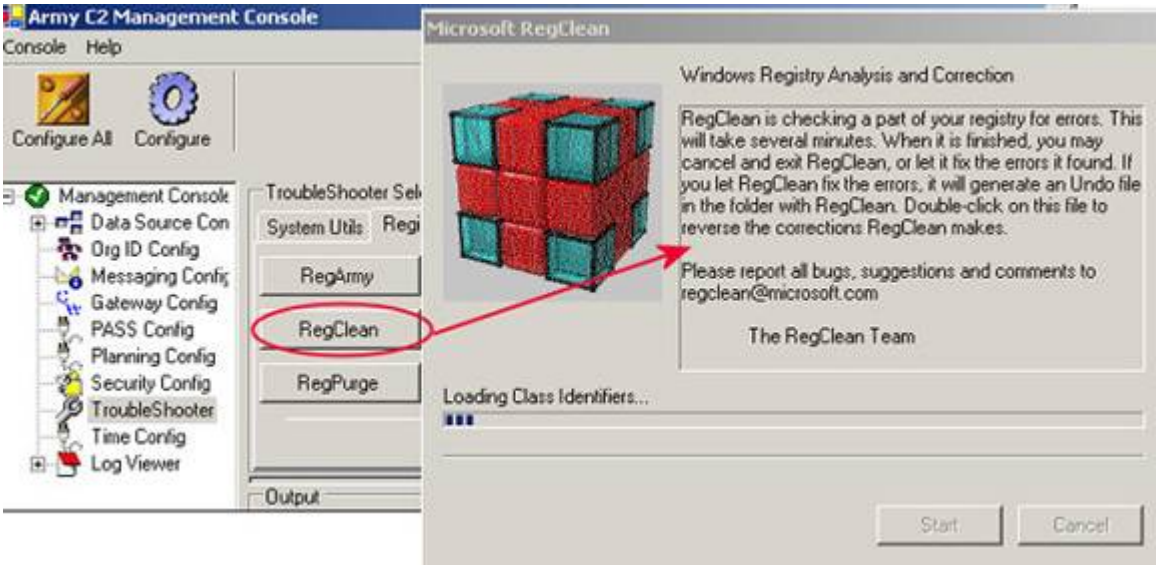


Figure 4-15 Microsoft RegClean Window - Clean in Process

2. Once the utility is completed, **click** the *Exit* button of the *RegClean* window. The *RegClean* window closes.

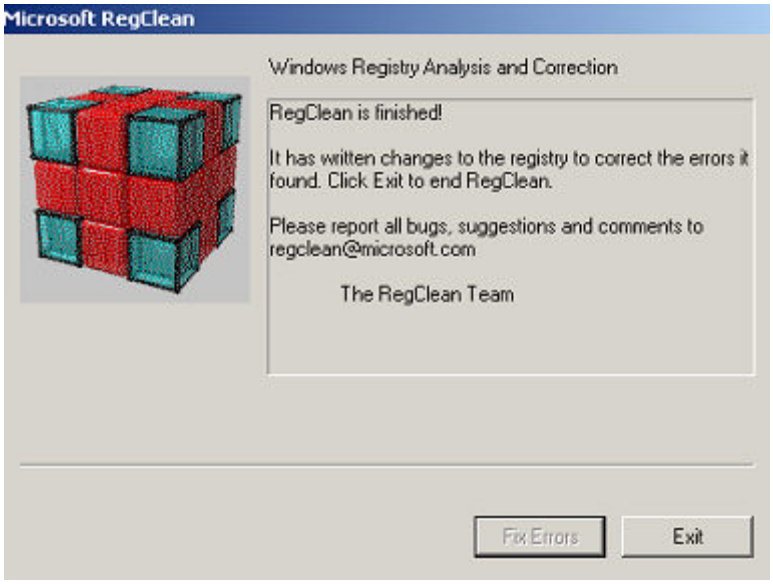


Figure 4-16 Microsoft RegClean Window - Clean Finished

4-2.4.3 RegPurge Button

1. To **run** the RegPurge utility, **click** the *RegPurge* button. The *Registry Cleaner* window opens.

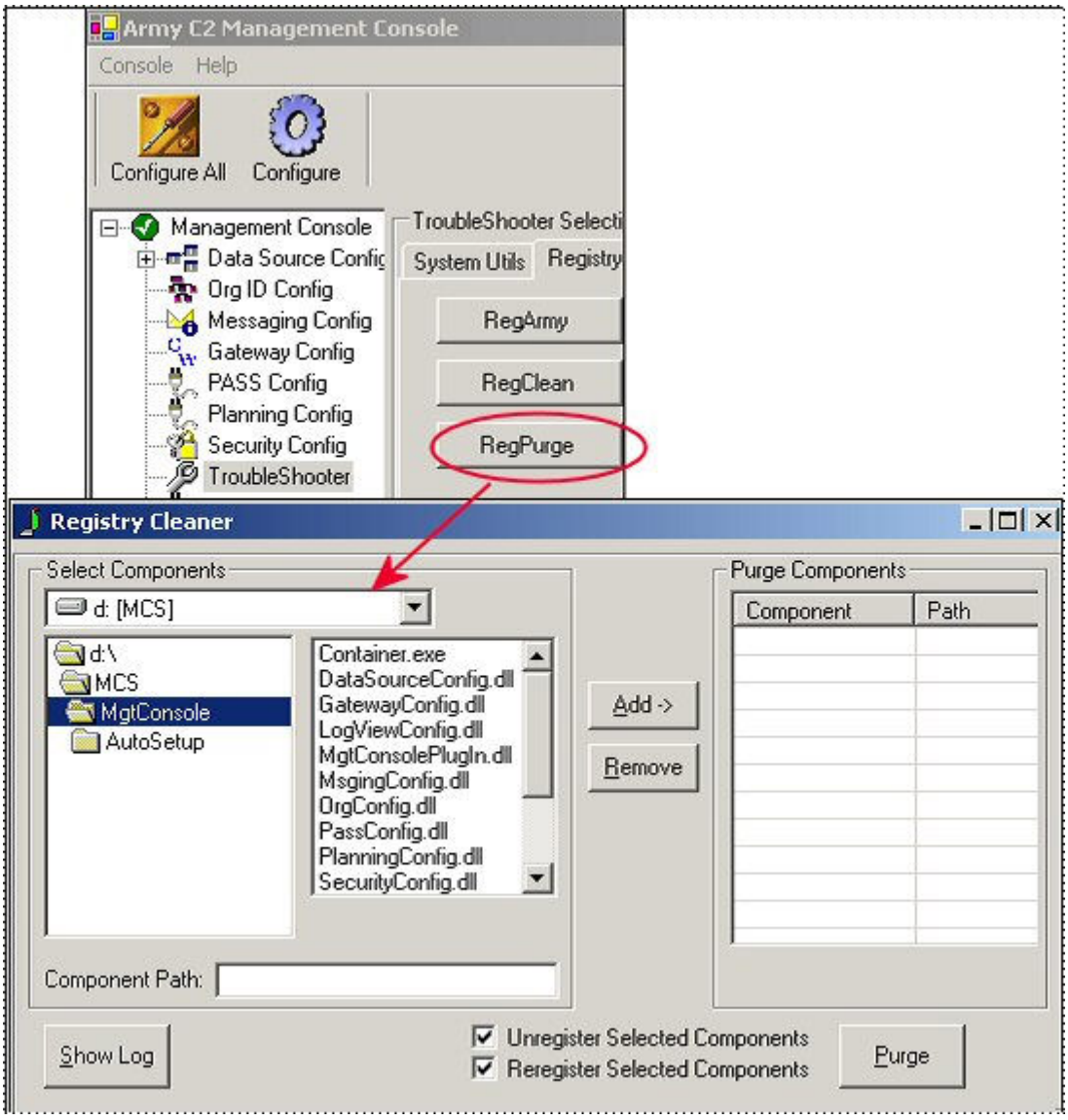


Figure 4-17 Registry Cleaner Window

2. To completely **remove** every instance of a selected component of MCS, **click** the *Purge* button.
3. **Select** the *component(s)* to remove, and **click** the *Add* button. The component(s) is added to the *Purge Components* list. Continue selecting components, if desired.
4. When all components have been selected, **click** the *Purge* button.
5. Click the *X* in the upper right corner to close the *RegClean* program.

4-2.5 Network Utils

To run the Network Utilities, **click** the *Network Utils* tab. The *Network Utils* tab contains two utilities.

Figure 4-18 Network Utils Tab

4-2.5.1 Ping Button

1. **Click** the *by IP Address*, or *by HostName* radio button, and **enter** the IP address or hostname accordingly for the machine you wish to ping.
2. **Click** the *Ping* button. Ping is performed, and the results are displayed in the *Output* box.

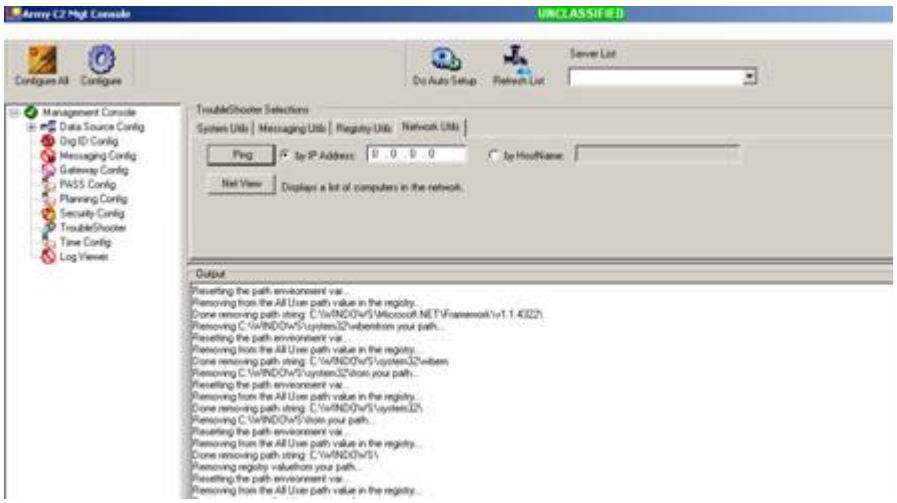


Figure 4-19 Network Utils Tab - Ping Results

4-2.5.2 Net View Button

The Net View button launches a utility that lists the servers associated with a particular MCS workstation.

1. **Click** the *Net View* button. The *Net View* process is launched and the results of the Net View process are displayed in the Output pane.

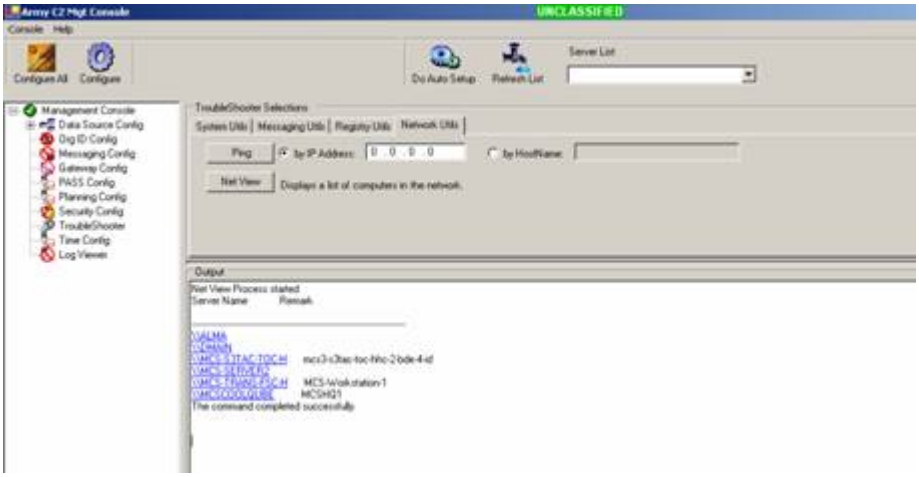


Figure 4-20 Net View

4-3 MCS Software Troubleshooting Scenarios

4-3.1 Troubleshooting the MCS Installation

If an error occurs during the installation of MCS, perform the following steps:

1. **Record** the error message. If the error has instructions. (i.e.: GSD did not install please install GSD after installation completes), follow these instructions.
2. **Verify** the user has Local Administrator Rights.
3. **Verify** the computer meets all the prerequisites. (i.e.: Hard Drive Space).
4. **Complete** the current install and, then, **reinstall** MCS.
5. If the error re-occurs or a new error occurs, **check** the CD for dirt or scratches.
6. **Clean** the CD or use a known working CD.
7. If unable to correct the fault, **contact** the S6/G6.

4-3.2 Troubleshoot Lost Connection

In the event of losing network connectivity, the following steps will provide guidance in locating the failure:

1. **Record** the error. If the error has instructions, **follow** these instructions.
2. **Verify** the *LAN* cable is connected at the computer and at the HUB/Switch.
3. **Verify** that there are no breaks or worn spots on the cable.
4. **Connect** or **replace** cable as needed.
5. **Verify** the *IP* address and port settings to the server are correct.
6. If necessary, **correct** *IP* address and port settings.
7. If unable to **correct** the fault, **contact** the S6/G6.

4-3.3 Troubleshooting Lost Files

1. **Click** *Start*, point to *Search*, and then **click** *For Files or Folders*.

2. **Click** *Pictures, music, or video* or *Documents (word processing, spreadsheet, etc.)*, depending on the type of file you want to find.
3. **Click** the appropriate search criteria, **type** all, or part of the name of the file (if you know it), and then **click** *Search*.

   A wildcard character is a keyboard character such as an asterisk (*) or a question mark (?) that is used to represent one or more characters when you are searching for files:

   Asterisk (*)

   Use the asterisk as a substitute for zero or more characters. If you are looking for a file that you know starts with "OPORD" but you cannot remember the rest of the file name, **type** the following:

   OPORD*

   This locates all files of any file type that begin with "OPORD" including OPORD Eagle.txt, OPORD Eagle.doc, and OPORD Fox.doc. To narrow the search to a specific type of file, **type**:

   OPORD*.doc

   This locates all files that begin with "OPORD" but have the file name extension .doc, such as OPORD Eagle.doc and OPORD Fox.doc.

   Question mark (?)

   Use the question mark as a substitute for a single character in a name. For example, if you type OPORD ?ox.doc, you will locate the file OPORD Fox.doc or OPORD Box.doc but not OPORD Eagle.doc.

3. If unable to **locate** the file, **copy** the file from another MCS Workstation.

4-3.4 Troubleshoot Broken Maps & Overlay Bookmark

A broken link in the Maps & Overlay bookmark will cause the loss of map data to the MAU. The following steps will provide guidance in locating this type of failure:

1. **Verify** the map bookmark is being applied correctly.
2. **Open** *Map Manager* and verify the bookmark still exists.
3. **Verify** that the *Map* associated with the bookmark is linked to Map Manager. **Relink** to all required maps if needed.
4. **Verify** the map is available on the hard drive. **Copy** maps to hard drive and relink map as needed.
5. If unable to **correct** the fault, **contact** the S6/G6.

4-3.5 Troubleshoot Lost UTO Using the TO Tool

A missing UTO using the TO Tool can be corrected by the following:

1. **Verify** proper data source is selected. If data source has changed, **open** the desired *UTO*.
2. If the UTO is still not available, **provide** *UTO* though the server or other media source.
3. If the UTO is still not available, **import** *UTO*.
4. If unable to **correct** the fault, **contact** the S6/G6.

4-3.6 Troubleshoot UTO Not Displaying When Selected from the Tools Menu in MDMP-A

1. **Verify** *UTO* is listed on the *Products* tab.
2. **Verify** *UTO* has been added using the *Identify friendly forces/troops available Essential Process Step.*
3. **Verify** *UTO* is available using Troubleshoot Lost UTO using the TO Tool procedures.
4. **Add** *UTO* using *Identify friendly forces/troops available Essential Process Step*.
5. **Click** *Tools* from the *Menu* bar, then **select** *Task Organization*. The *UTO* should appear on the *MDMP-A.*
6. If unable to **correct** the fault, **contact** the S6/G6.

4-3.7 Troubleshoot MCS Messaging Unable to Send Message

1. **Verify** message has been completed properly.
2. **Verify** *Multicast* and *UniCast* are started. **Start** *Multicast* and *UniCast* as needed.
3. **Verify** network connectivity.
4. **Send** a *message.*
5. If unable to **correct** the fault, **contact** the S6/G6.

4-3.8 Troubleshoot Unable to Receive Live Feed data

1. **Verify** *Auto Update* is turned on and *Live Feed* is selected.
2. **Verify** *Live Feed* providers are checked on the *Live Feed* tab.
3. **Verify** *Units* and or *Geometries* are checked within the providers.
4. **Verify** network connection.
5. **Confirm** *Live Feed* options are correct.
6. **Verify** *IP* address and *Port* settings are correct in the *Management Console*.
7. If unable to **correct** the fault, **contact** the S6/G6.

4-3.9 Troubleshoot EOB displaying wrong Mission Specialty symbols on TO Tool

1. **Select** the *Unit* and **open** *Unit Properties.*
2. **Verify** *Mission Specialty*. **Correct** as needed. **Click** *OK*.
3. **Open** *Unit Properties* and **verify** the change.
4. If unable to **correct** the fault, **contact** the S6/G6.

4-4 Query Database Using the Search Engine Tool from Desktop

4-4.1 Description of Search Engine Tool

The Search Engine provides the user with the capability to query and analyze the contents of the MCS database. The Search Engine supports the MCS mission by enabling the user to:

- **Search** and **view** database content identified by operator specified criteria.
- **Create** and **save** the specified criteria as an MCS filter which can be used to display map feature geometries, friendly units, and/or enemy units on an overlay.

4-4.2 Search Engine Menu Bar and Toolbar

1. From the *Start* menu, **click** *Programs, MCS*, *Administration*, then **choose** *Search Engine*. The *Search Engine* window opens.

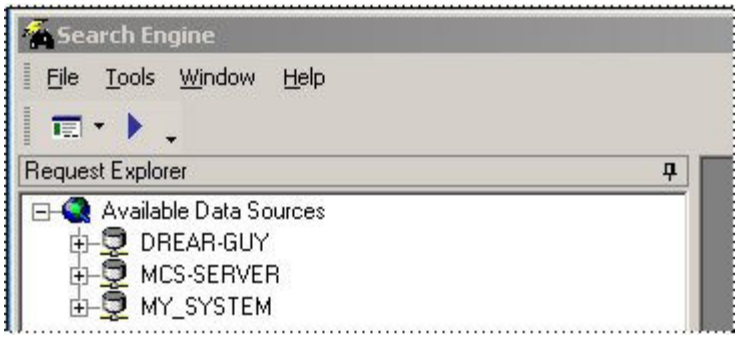


Figure 4-21 Search Engine Window

The functions of the Search Engine Menu Bar are: File, Tools, Window and Help.

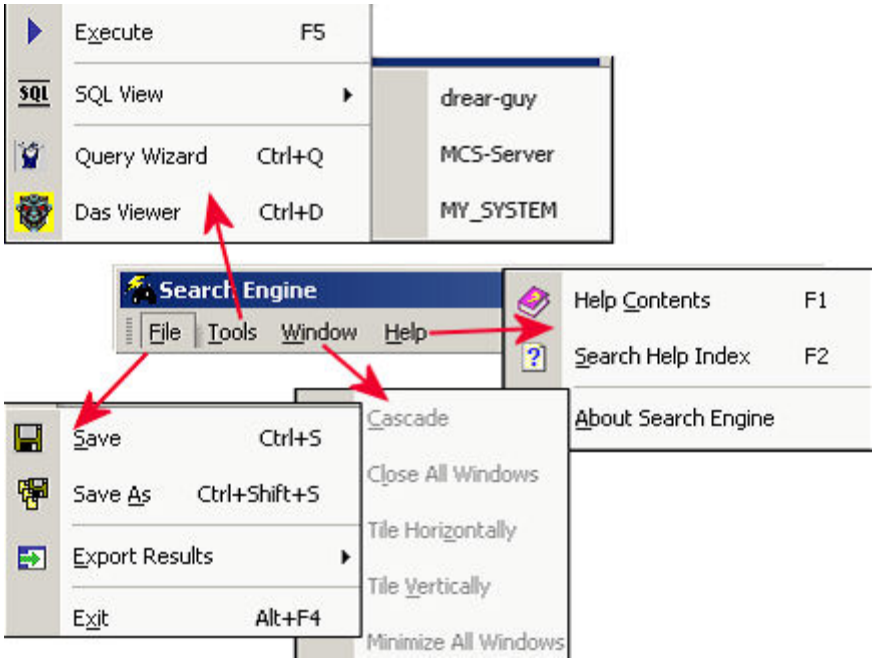


Figure 4-22 Search Engine Menu Bar

The functions of the Search Engine Toolbar are:

- View Type Selection Icon - Used to select the *SQL, Advanced,* or *Wizard* views.
- Run Query Icon - When selected runs a query from the query window.
- Find Form Button Icon - Opens Unit Filter Wizard window.
- Toolbar Options Icon - From the Custom option opens the Customize window used to modify the toolbar.
- Customize Window - Used to customize the toolbar.

These functions are:

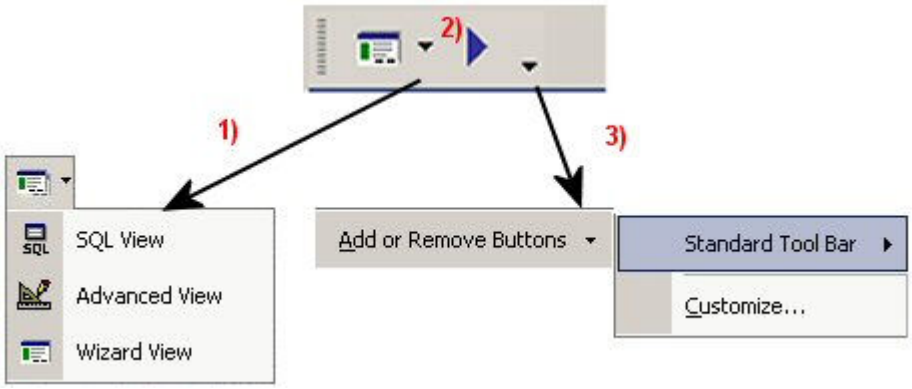


Figure 4-23 Search Engine Toolbar

4-4.3 Create a Filter with Wizard

Filter Wizards are Graphical User Interface (GUI) windows used to create and customize unit filters. The Search Engine provides two Wizards, the Correlated Hostile Unit Filter, and the Friendly Unit Filter wizard. Wizards can create and customize friendly and hostile filters.

1. From the *Search Engine's* toolbar, **click** the *View Type Selection* icon down-arrow and *Wizard View* .

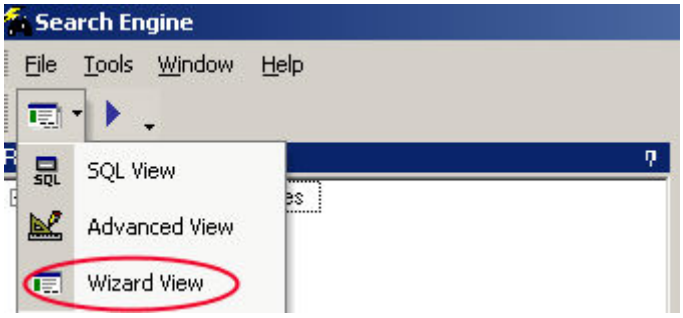


Figure 4-24 Wizard View Icon

2. *In* Request Explorer, from the *Create MCS Filter* branch, **double-click** on the desired filter icon (i.e., friendly or correlated hostile icons). The *Unit Filter Wizard* opens adjacent to Request Explorer.

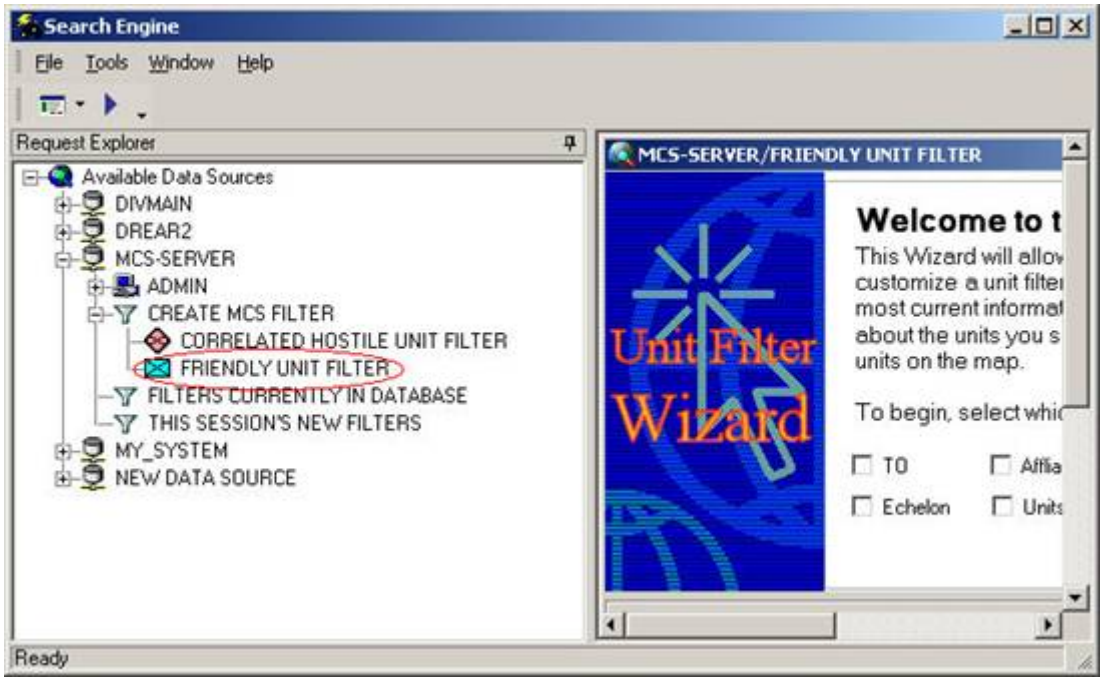


Figure 4-25 Request Explorer: Friendly Unit Icon Selected

3. **Select** the overall criteria for the filter. These choices determine the flow of the wizard.
4. **Click** *Next*. The next criteria window opens.

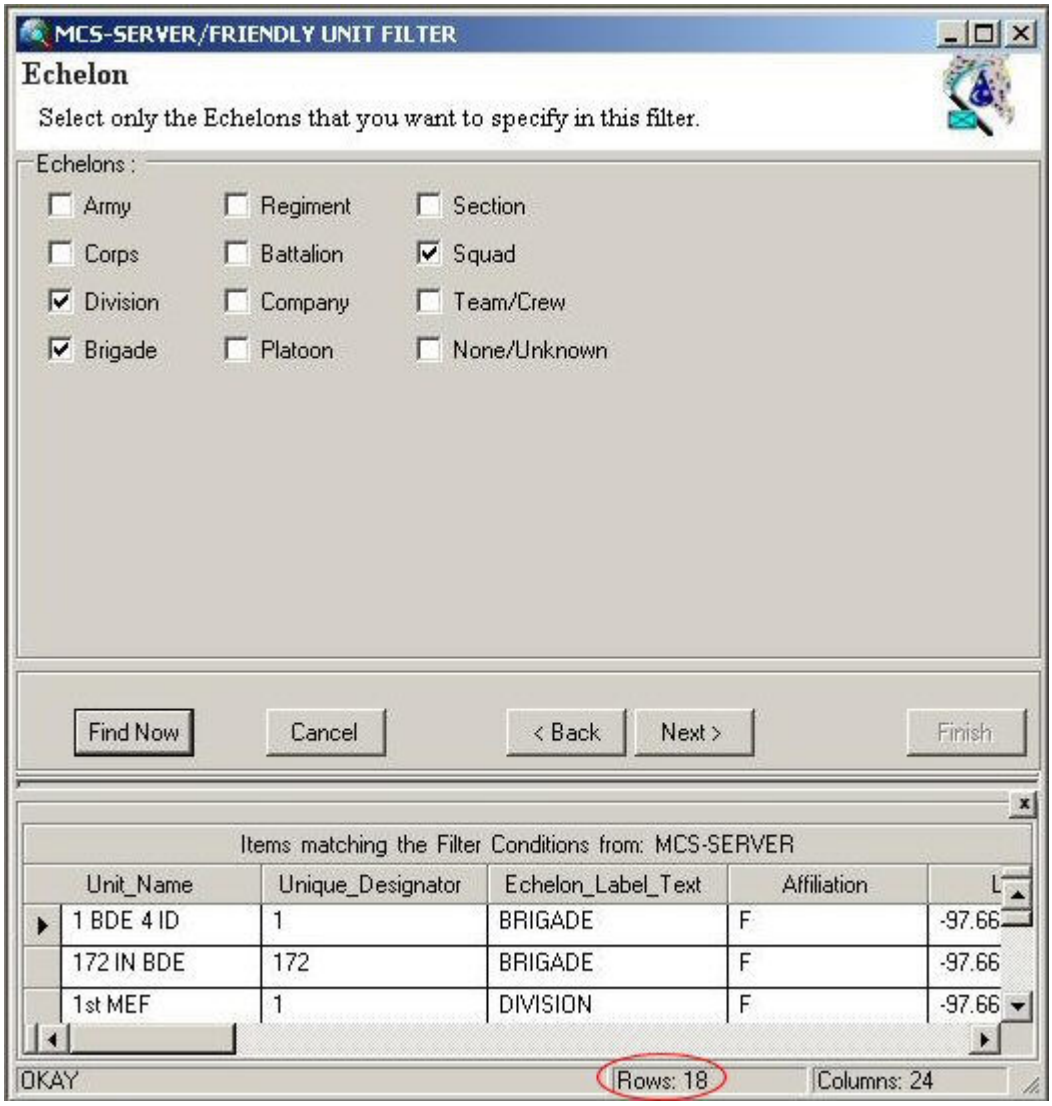


Figure 4-26 Echelon Window

NOTE

Criteria windows will vary depending on the overall criteria selected.

5. **Click** *Find Now* or, from the menu bar, **click** the *Run Query* icon. Results are displayed in the bottom area of the window (see above figure).
6. **Click** *Next*. The next criteria window opens.
7. **Select** the *Affiliation*(s). A check mark appears in the associated box(es).

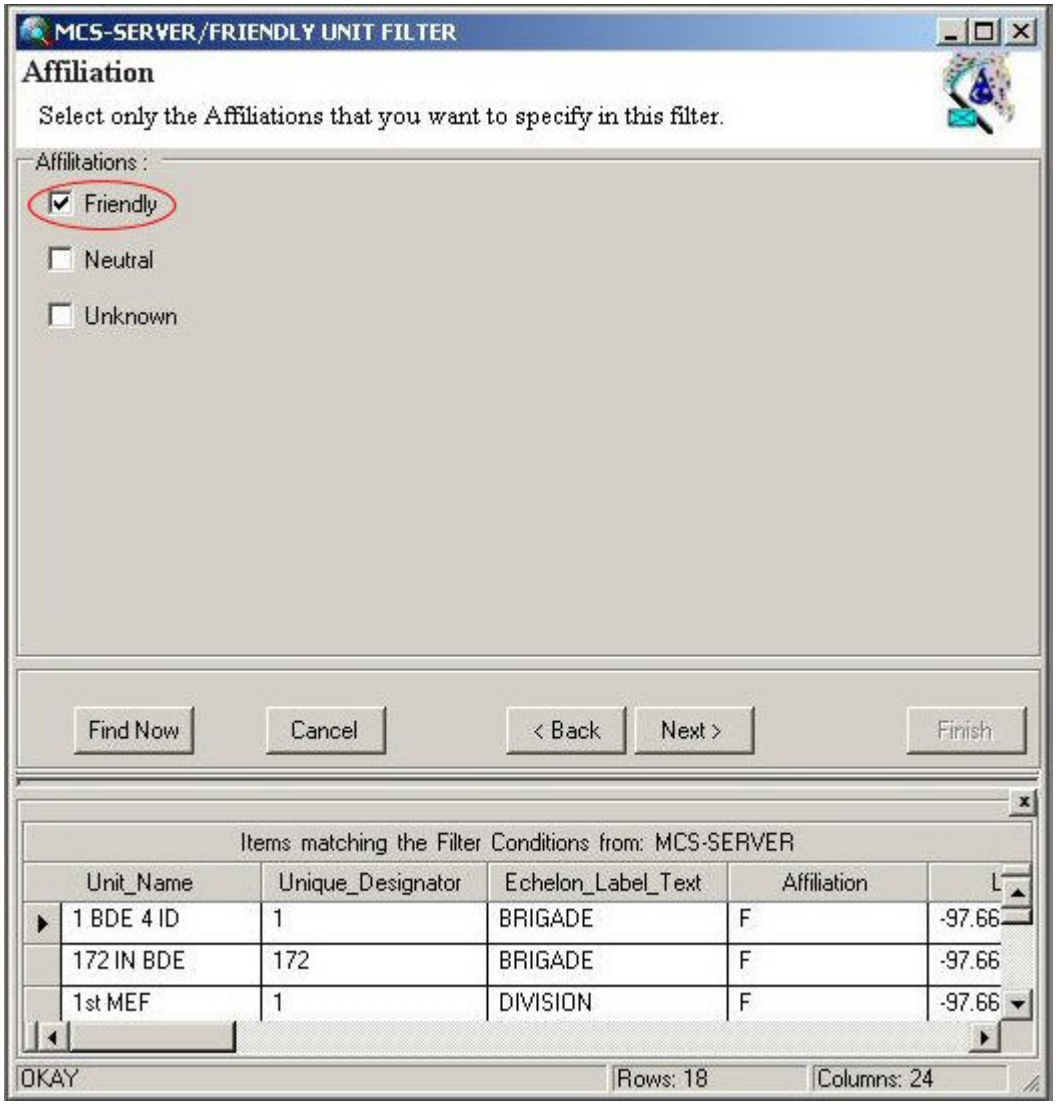


Figure 4-27 Affiliation Window

8. **Click** *Next* to continue without executing the query; or **click** *Find Now* or the *Run Query* icon on the toolbar to run the query.
9. **Click** *Next.* The *Description of your Filter* window opens.

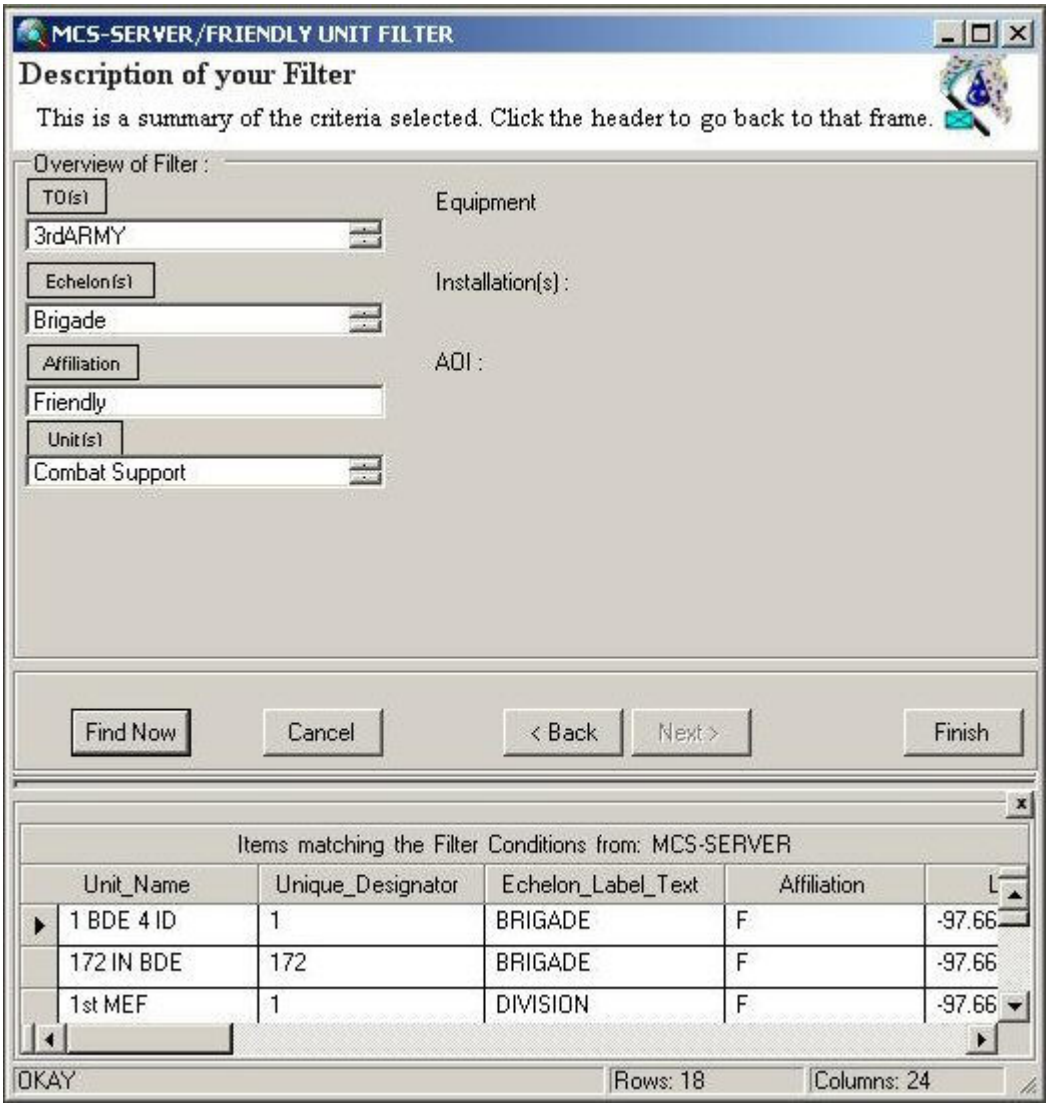


Figure 4-28 Description Of Your Filter Window

10. In the *Overview of Filter:* area, **verify** the criteria.
11. If a change (i.e., add, deletion) of a criterion is necessary, **click** *Back* until the *Welcome to the Unit Filter Wizard* window opens, and make the necessary change. **Click** *Next* to return to the *Description of your Filter* window.
12. **Click** *Finish*. The *Filter Name* window opens.

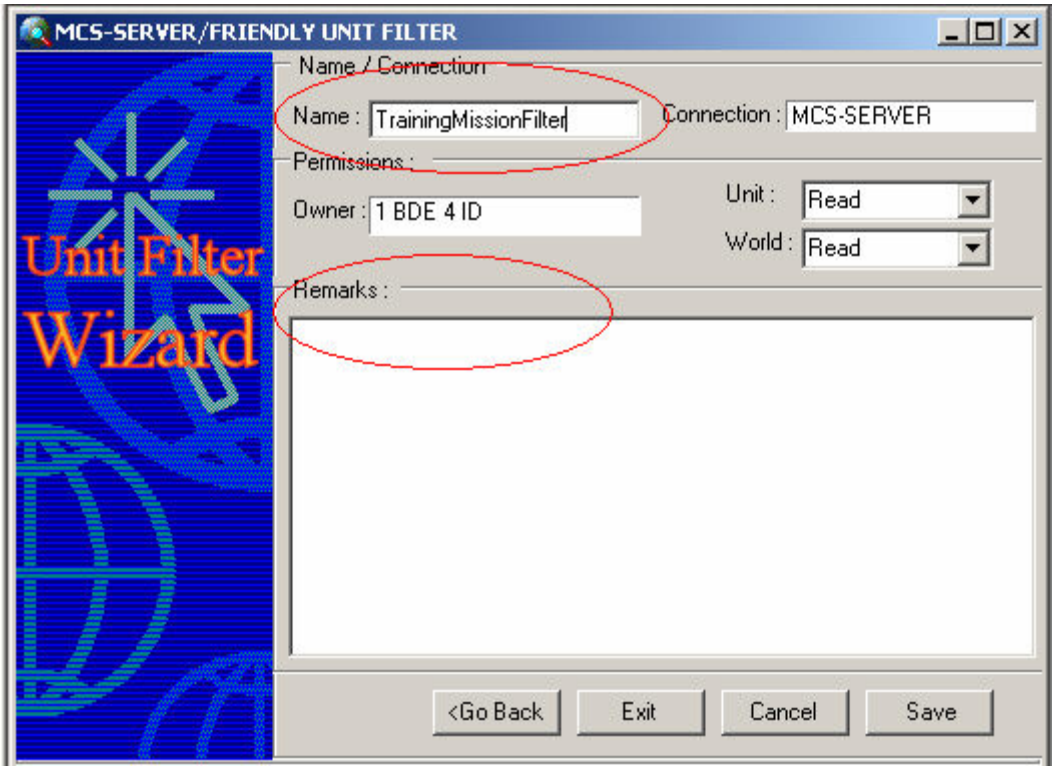


Figure 4-29 Filter Name Window

13. **Enter** a name and remarks for the filter in the associated box(es).
14. **Click** *Save*. The *Filter Name* window closes and the new filter appears under the *THIS SESSION'S NEW FILTERS* branch of Request Explorer.

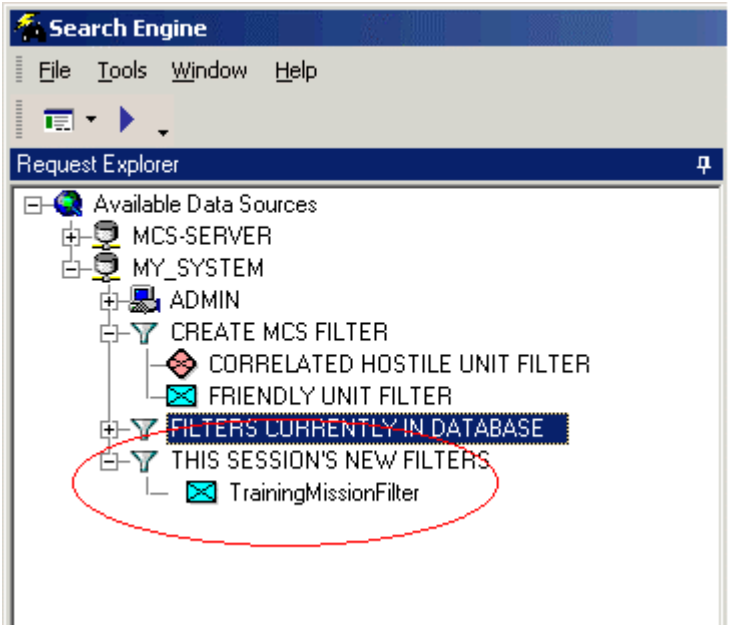


Figure 4-30 New Filter Saved

NOTE

The Save As feature in the File menu may also be used to save a filter. This feature only allows the user to save the file to the client's database. It cannot be saved outside of a database, such as in a directory on the local hard drive.

15. To refresh the filter, **right-click** on the filter icon, and from the menu, **select** *Refresh*. The filter is moved to the *FILTERS CURRENTLY IN DATABASE* branch.

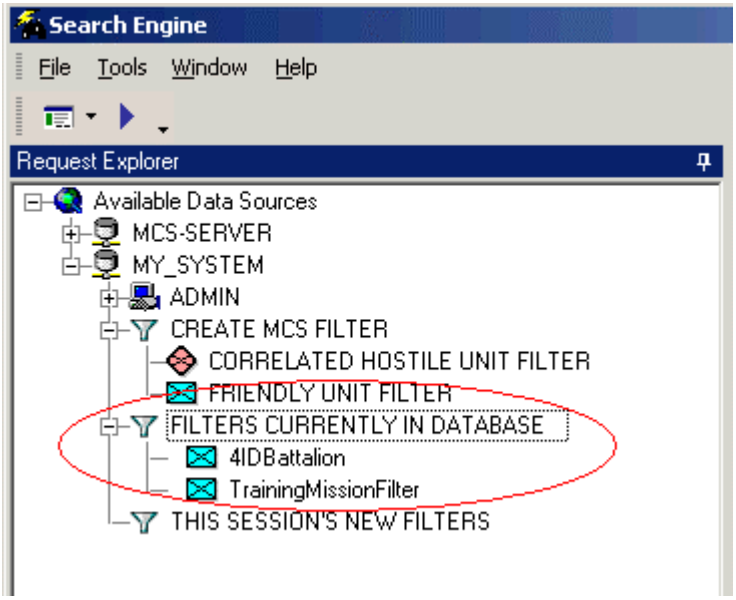


Figure 4-31 Filter Refreshed

4-4.4 Modify a Filter with Wizard

NOTE

Currently, if a filter on an AOI is edited, the editor will display the lower left and upper right coordinates instead of the upper left and lower right coordinates.

1. From the toolbar, **click** the *View Type Selection* icon drop-down arrow, and then, **select** *Wizard View*.

Figure 4-32 Wizard View Icon

2. From Request Explorer, in the *FILTERS CURRENTLY IN DATABASE* branch, **select** the desired filter.
3. **Right-click** the filter icon and, from the menu, **select** *Edit*. The *Unit Filter Wizard* opens.
4. **Repeat** Steps in "Create a Filter with Wizard".

4-4.5 Describe an Advanced View Filter

The *Advanced View* capability has been provided to enable the user to view specific data from the database in a tabular format. The criteria used to limit the scope of the displayed results is defined by the user based upon mission needs, (i.e., organization types, obstacles, data/time stamps, etc.).

The features of the Search Engine window in Advanced View are as follows.

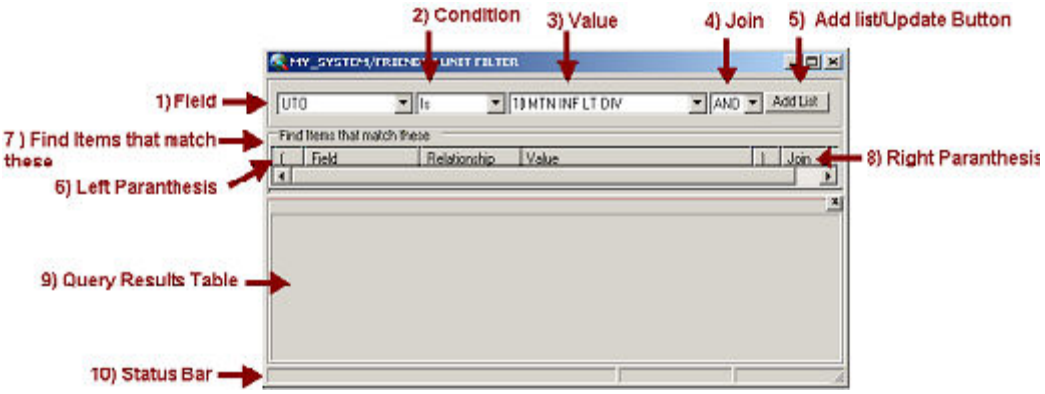


Figure 4-33 Advanced View Features

1. Field - The *Field* button activates a drop-down list, which enables the operator to select criteria components. The criteria components are a function of the *query/filter* selected in the *Look for* list. Selection of a *Field* from the list causes the field name to appear in the *Field* field. The appropriate *Conditions* for the *Field* are placed in the *Condition* drop-down. The appropriate *Values* for the *Field* are placed in the *Value* drop-down.
2. Condition - The *Condition* button activates a drop-down list. *Conditions* are: *In, Between, IS, Like, Greater Than, Less Than*). *Conditions* qualify the relationship between *Value* and *Field* components. The content of this drop-down is a function of *Field*.
3. Value - The *Value* button activates a drop-down list, consisting of the possible *Values* for the selected *Field*.
4. Join - The *And/Or* button allows the operator to join or exclude criteria.

5. Add/Update Button - The *Add* button is the fifth feature of the MCS *Advanced View* window. This button adds the filter criteria to the *Find items that match these* area. When the button changes to *Update* (during modifying a statement parameter), it effects the modified parameter.
6. Left Parenthesis -The *Left Parenthesis* bounds the beginning of a statement phrase.
7. Find Items that match these area - This feature allows the dynamic filter criteria to be displayed, grouped, and prioritized.

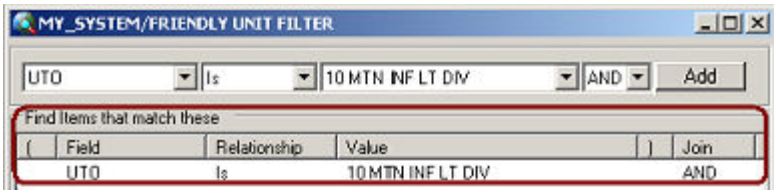


Figure 4-34 Find Items That Match These Frames

This area consists of six fields that are used to manipulate the dynamic filter criteria:

- *Left Parenthesis* - used for grouping and joining criteria.
- *Field* - identifies the criteria selected from the database.
- *Relationship* - identifies the relationship used to compare the field to the specified operator.
- *Value* - depicts the data compared to the field.
- *Right Parenthesis* - used for grouping and joining criteria.
- *Join* - concatenates the dynamic filter criteria and joins individual criteria into a filter.

This area also has horizontal and vertical slide bars that allow the user to pan the entire area.

8. Right Parenthesis - Bounds the end of a statement phrase.
9. Query Results Table - As a query/filter is executed, the results are displayed in tabular format in this window. The column headings are based on the database and fields selected for the query/filter. The contents of the display can be sorted by clicking on the column headings. This window has horizontal and vertical slide bars that allow the user to pan the entire window.

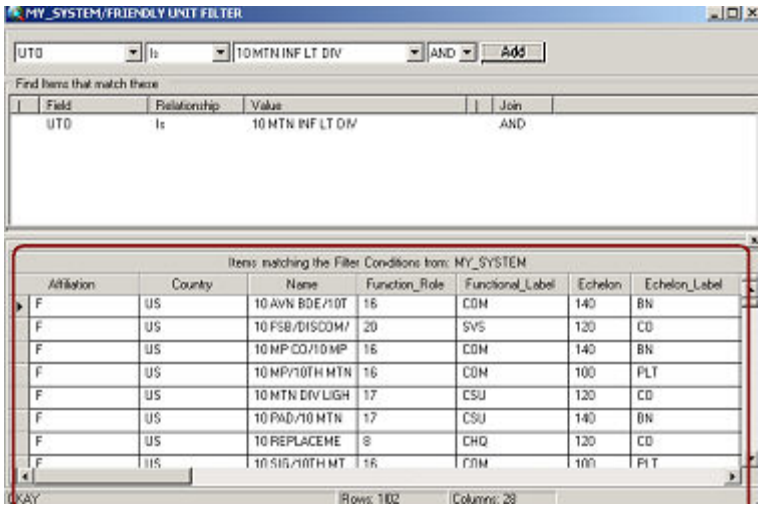


Figure 4-35 Results Display & Status Bar

10. Status Bar - The last feature of the *Advanced View Search Engine* window displays information about the number of records returned upon the execution of a query/filter. The *Status Bar* is used to display information and error messages that arise from the creation or processing of a query/filter. Warning Messages are informative in nature and do not require operator intervention. Warning Messages are displayed in the left panel of the *Status Bar.* In addition to being written to an Error Log, Error Messages are posted in the left panel of the *Status Bar*.

4-4.6 Create a Filter in Advanced View

A filter is used to correlate dynamic feature and unit data for display in an overlay. The filter contains the operator-specified criteria that encapsulates what data is retrieved from the database. The types of filters currently definable include *friendly and correlated enemy units*.

1. From the *Search Engine's* toolbar, **click** the *View Type Selection* icon down-arrow and *Advanced View*.
2. From *Request Explorer*, in the *CREATE MCS FILTER* branch, **double-click** on the desired filter icon. The advanced *Unit Filter* window opens.

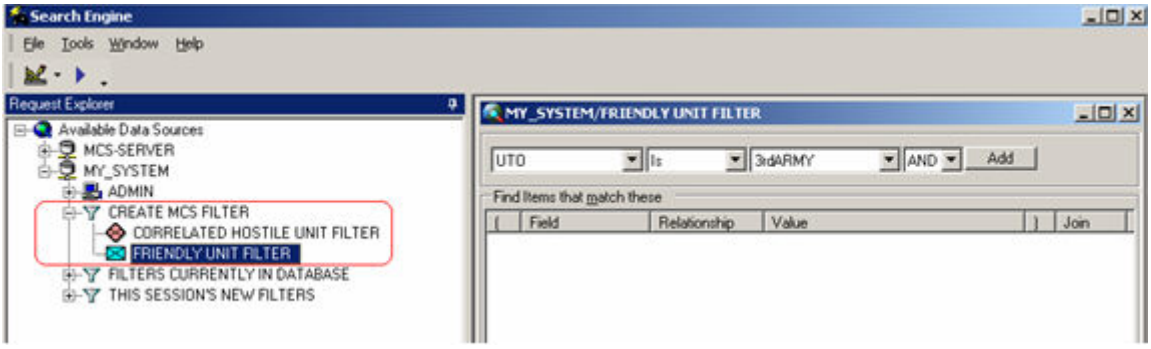


Figure 4-36 Request Explorer: Friendly Unit Filter Selected

3. From the *Field* box, **select** a field value.
4. From the *Condition* box, **select** a condition.
5. From the *Value* box, **select** a value.
6. From the *Join* box, **select** a parameter.
7. **Click** *Add*.
8. If additional query statements need to be added to the filter, **repeat** Steps 2 through 6.

NOTE

The AND conjunction combines statements together in a query. All conditions joined by the AND statement must be met to show in the filter.

The OR conjunction does not combine statements. All conditions joined by the OR statement will be shown in the filter whether or not they met any other statements listed in the query.

Queries can be deleted if no longer needed:

1. To **delete** a query statement, **right-click** on the statement, and from the menu, **select** *Delete*.
2. To **run** or **execute** a query, follow these steps:

NOTE

The query may be executed at any time to display its output. This assists the user in fine tuning the filter.

1. From the menu bar, **click** *Tools*, then **choose** *Execute*, or **click** the *Run Query* icon on the toolbar. Results are displayed in the bottom area of the window.

To **save** a query, follow these steps.

1. From the menu bar, **click** *File* then choose *Save.* The *Save* window opens.
2. **Enter** a name in the associated box.
3. **Click** *Save*. The *Save* window closes and the filter is saved in the *THIS SESSION'S NEW FILTERS* branch of Request Explorer.

Filters may be refreshed from time to time. Follow these instructions:

1. To **refresh** the filter, **right-click** on the filter icon, and from the menu, **select** *Refresh*. The filter is moved to the *FILTERS CURRENTLY IN DATABASE* branch.

4-4.7 Modify a Filter in Advanced View

NOTE

Currently, if a filter on an AOI is edited, the editor will display the lower left and upper right coordinates instead of the upper left and lower right coordinates.

1. **Ensure** the *Advanced View* is selected in the toolbar.
2. From *Request Explorer*, in the *FILTERS CURRENTLY IN DATABASE* branch, **double-click** on the desired filter icon. The advanced *Unit Filter* window opens.
3. **Select** the statement to modify. The statement is highlighted.

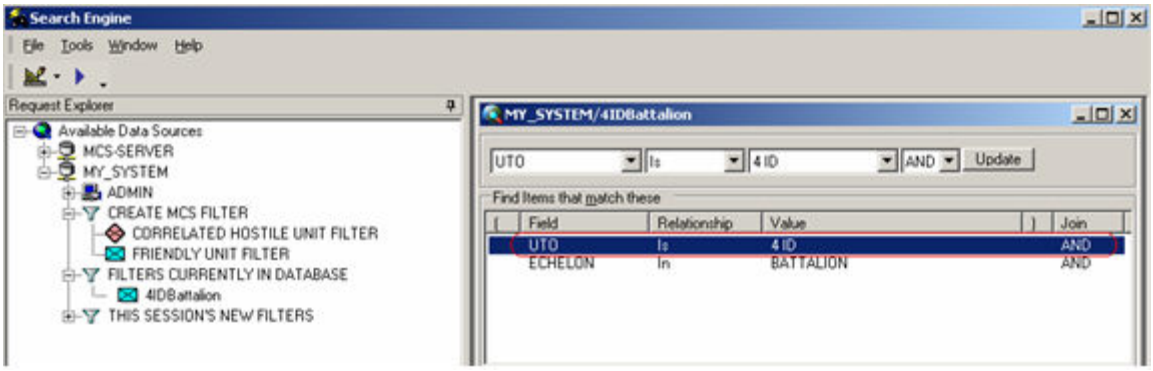


Figure 4-37 Statement Selected for Modification

4. **Modify** the parameters as necessary from the associated boxes.
5. **Click** *Update*. The filter is modified.

6. **Execute** the query after modifications to review the results.
7. From the menu bar, **click** *File* then **choose** either *Save,* or *Save As.*
8. If *Save As* is selected, the *Save As* window opens.
9. **Enter** a name in the associated box.
10. **Click** *Save.* The *Save As* window closes and the filter is saved in the *THIS SESSION'S NEW FILTERS* branch of Request Explorer.

4-5 Data Transaction (or DAS) Viewer

4-5.1 Introduction to Data Transaction (or DAS) Viewer

NOTE

Never open more than one (1) instance of the DAS Viewer.

The DAS Viewer, or Data Transaction Viewer, allows you to identify the following information: view queries pending execution, state of executed queries, default data source, list of any errors, and lists each query executed. This window is intended for debugging or system administrative support. You can search for data by the Datasource or Application views.

The DAS Viewer monitors and logs query information between the MCS applications and both the Access Database and the SQL Database. This information can be used to help identify failures logged by the DAS Viewer. During troubleshooting, it is helpful to collect the logged information and include any failures in the problem report. This will assist in locating the cause of a failure. The following diagram presents a simplified overview of the DAS.

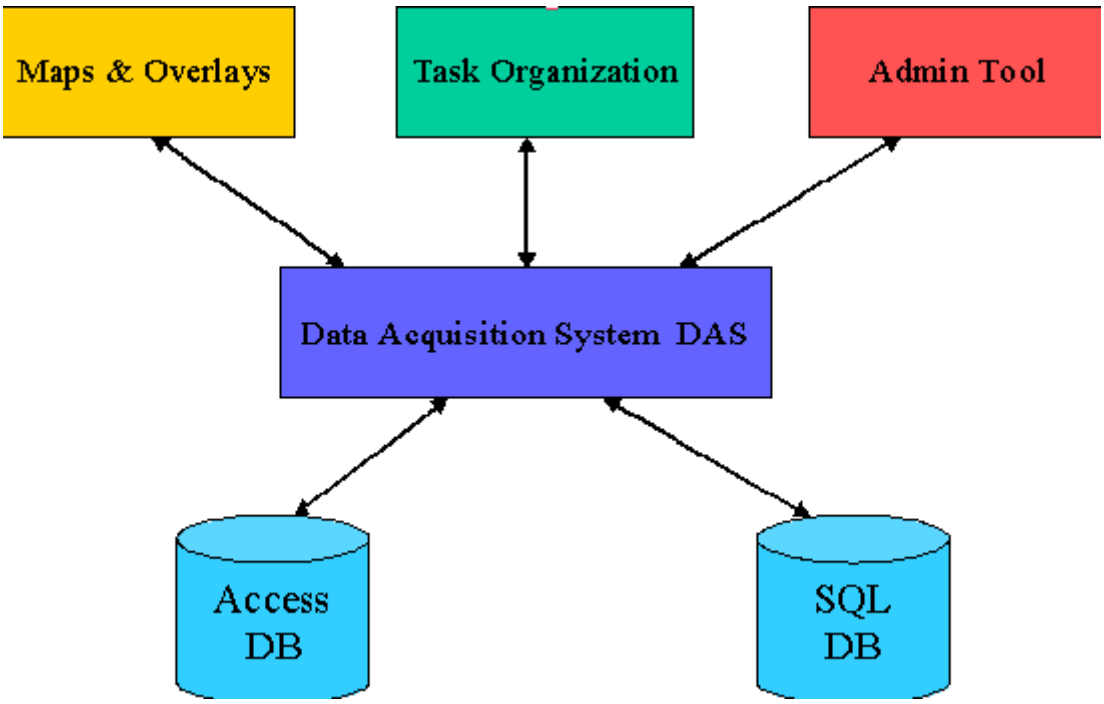


Figure 4-38 Data Acquisition System (DAS)

4-5.2 Starting the Data Transaction Viewer

1. From the desktop Start Menu, **select** *Programs, MCS, Administration, Data Transaction Viewer*:

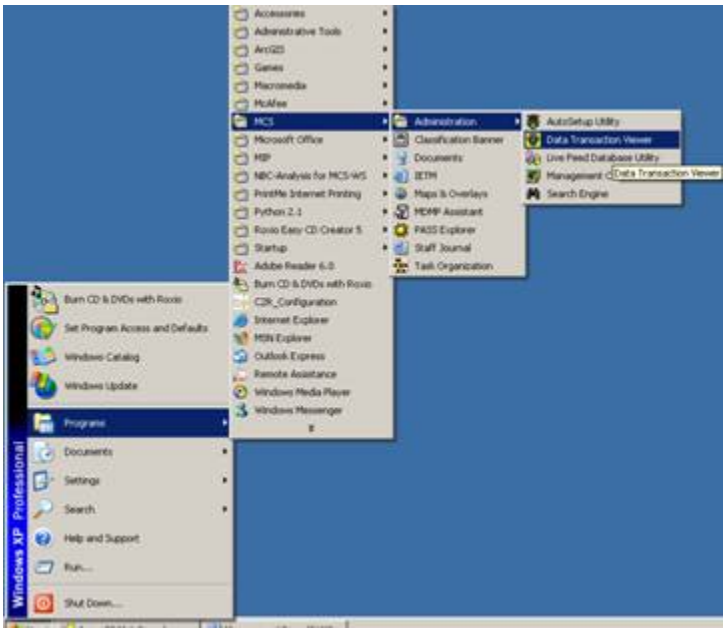


Figure 4-39 Starting the Data Transaction View

4-5.3 Starting the DAS Viewer from the Search Engine

1. From the *Search Engine Menu Bar*, **click** *Tools*. A drop-down list appears.

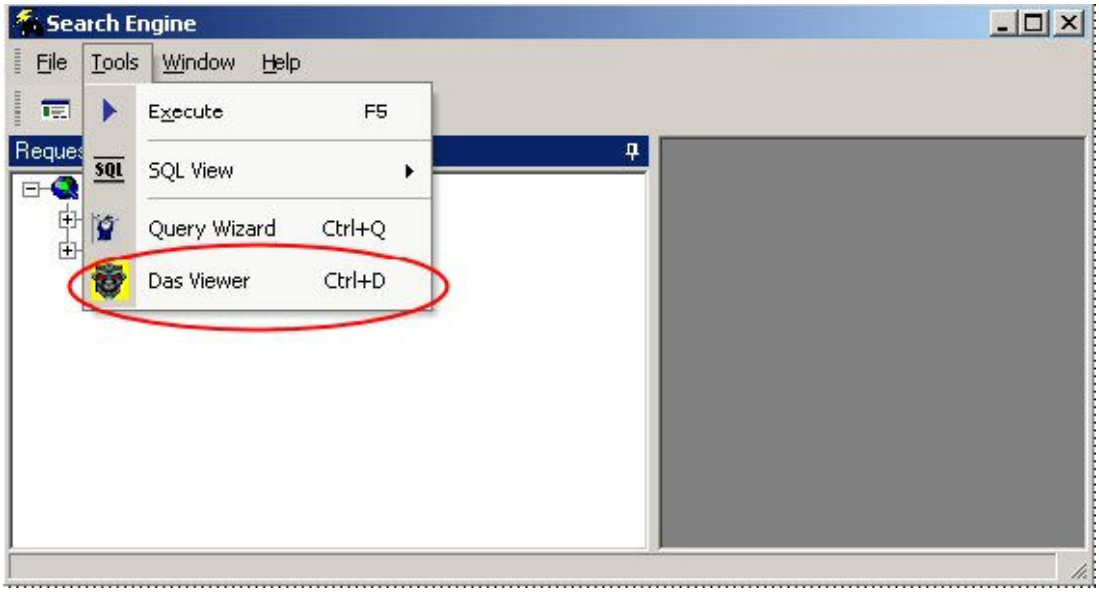


Figure 4-40 Search Engine Tools down-arrow menu

2. From the drop-down list, **select** the *DAS Viewer.* The DAS Viewer opens.

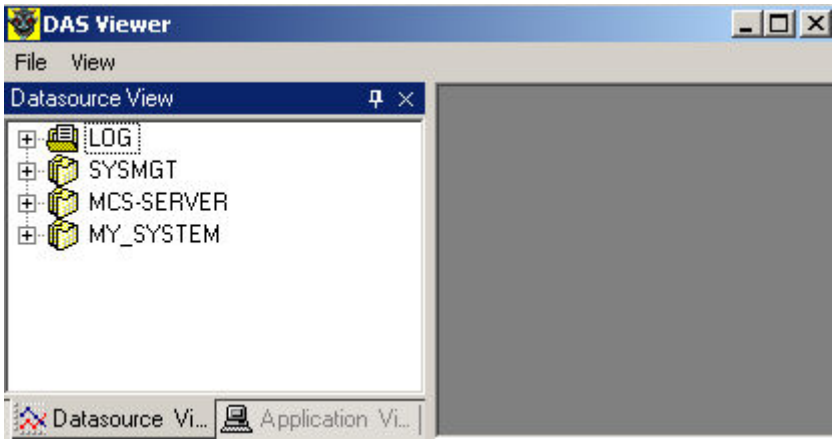


Figure 4-41 DAS Viewer

3. **Click** *File* in the menu bar to display the list of files you can open and close. The complete list is shown.

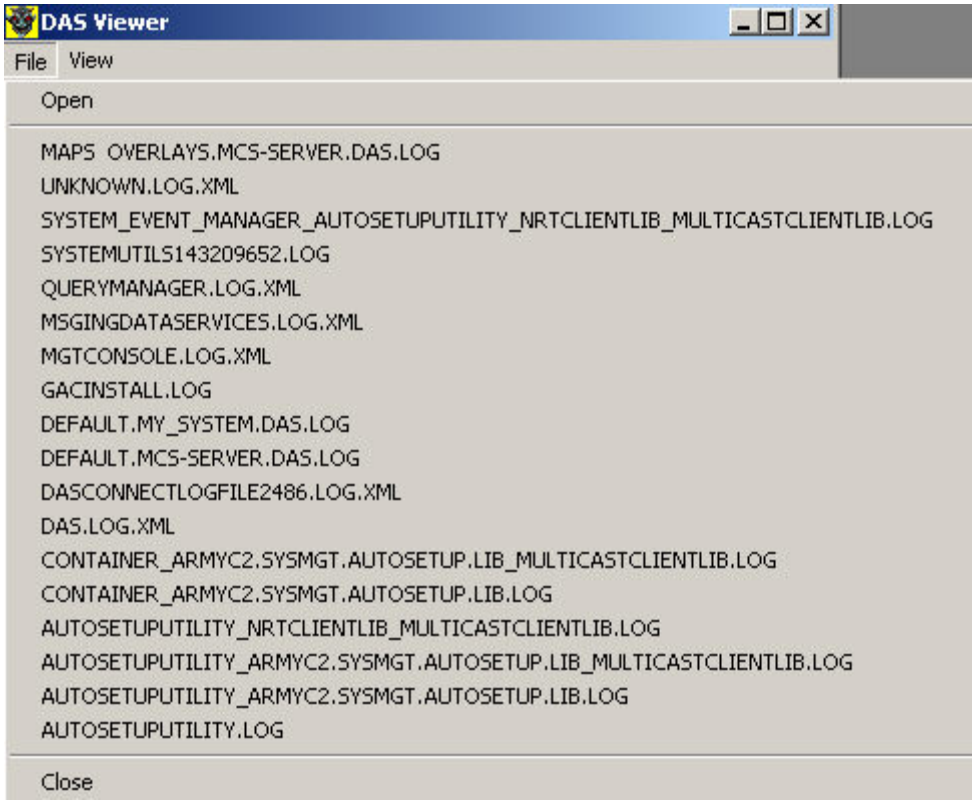


Figure 4-42 File menu item

4. **Click** *View* in the menu bar to switch between Application, Datasource, both, or none.

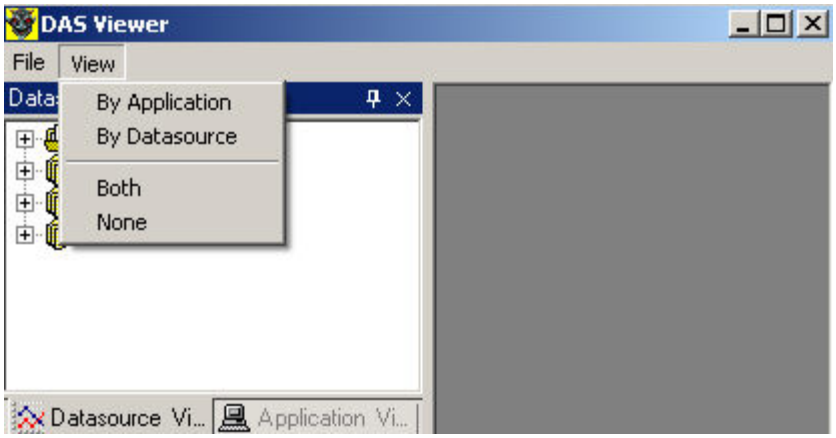


Figure 4-43 View menu item

5. **Click** the *Application View* button on the bottom left side pane of the DAS Viewer.
6. **Expand** the *DEFAULT* item in the treeview, then **double-click** *MY_SYSTEM* under the *DEFAULT* option. The right side pane displays the DAS Query Information for *MY_SYSTEM*.

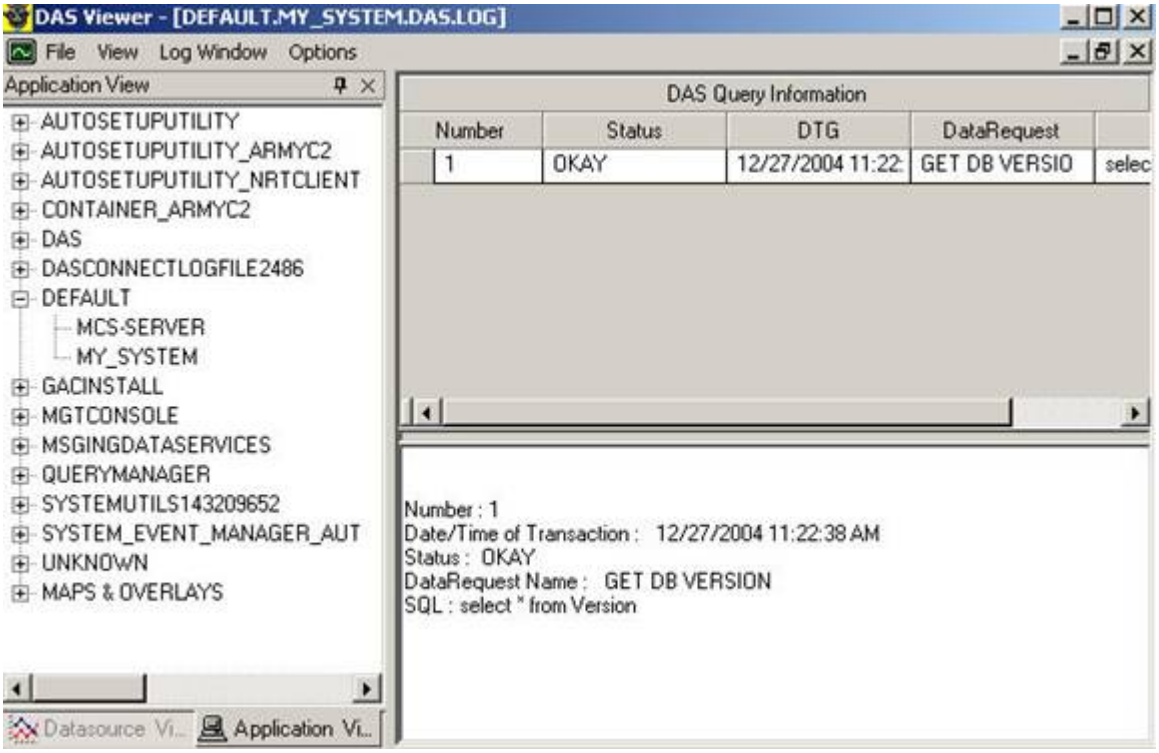


Figure 4-44 MY_SYSTEM DAS Query Information

7. **Click** the *Application View*, **expand** the *Maps & Overlays* item in the treeview. From the Application View, **click** MCS-SERVER (Hostname) under the MAPS & OVERLAYS item in the left hand pane of the DAS Viewer. The right hand pane displays the DAS Query Information.

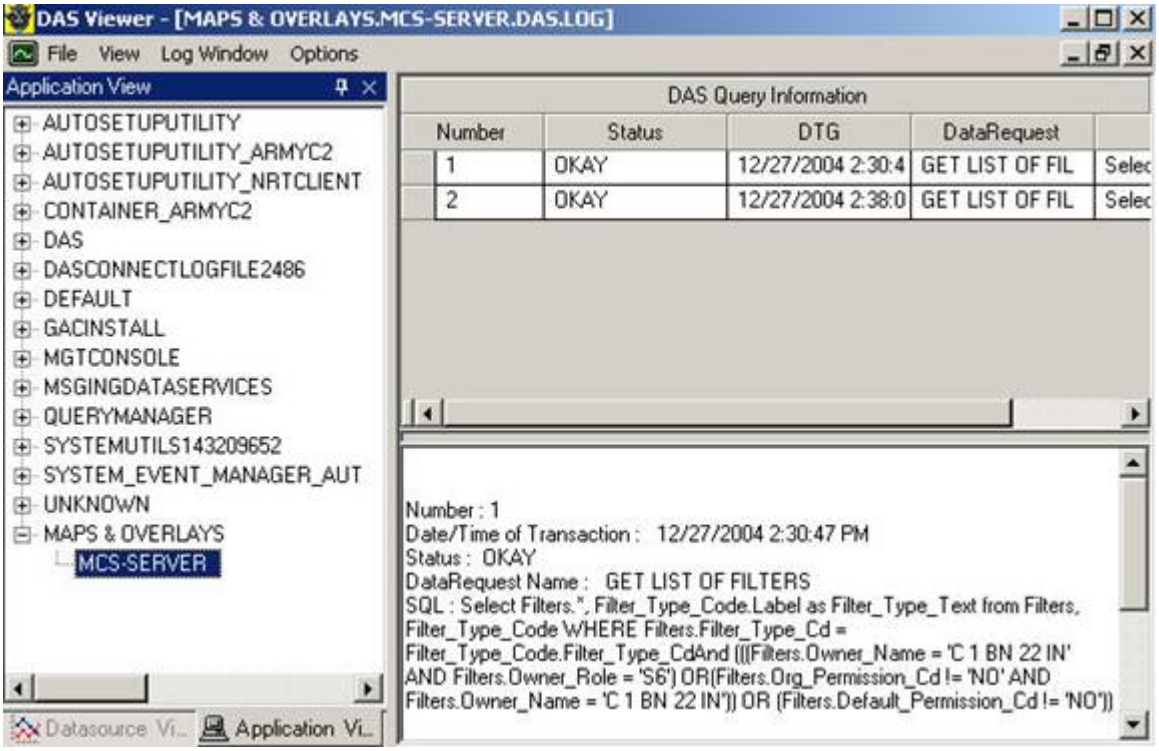


Figure 4-45 Maps & Overlays DAS Query Information

8. To **view** one of the available log files, **double-click** the *LOG* option below the log of interest (i.e. DAS, GACINSTALL, MAPSAPPLICATION,MGTCONSOLE, QUERYMANAGER, SYSTEMUTILS145085720) appears.
9. **Click** *Log Window* in the menu bar. The *Log Window* options are displayed.

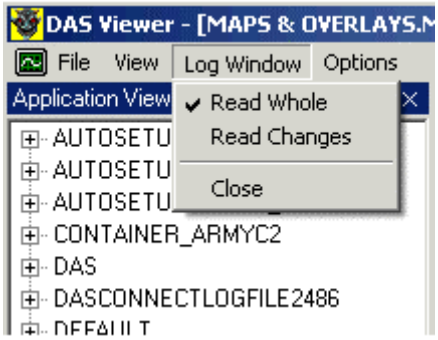


Figure 4-46 Log Window menu item

10. **Click** *Options* in the menu bar. The *Options* drop-down list is displayed.

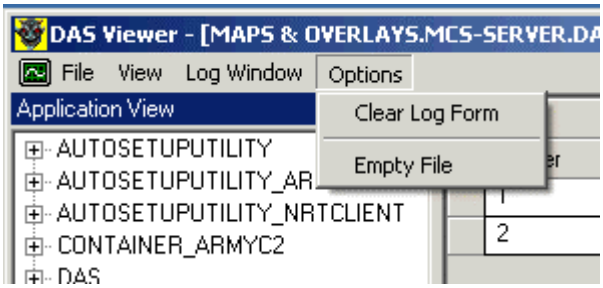


Figure 4-47 Options menu item

Chapter 5 Perform Preventative Maintenance Checks/Services (PMCS)

5-1 Perform Before Operations Preventative Maintenance Checks/Services

1. **Unpack** system components.
2. **Conduct** an inventory of system components.
3. **Visually inspect** all cables and connectors for the following:
   - Burns
   - Broken
   - Frayed
   - Loose
   - Missing components
4. **Inspect** all hardware for the following:
   - Cracks
   - Deformation
   - Loose attachment hardware
5. **Assemble** system components

CAUTION

Do not set equipment on damp or wet floor.

   - **Place** laptop at desired operating location
   - **Ensure** that the operating location is as close to power source as needed
   - **Install** Removable Hard Disk Drive (RHDD), if required
   - **Install** battery, if required

NOTE

On some MCS Workstation models a fully discharged battery will not charge.

CAUTION

If the cover is not attached properly, the battery may fall out while the computer is being carried.

   - **Connect** AC power adapter with cord, if required
   - **Connect** LAN (RJ-45) connector
   - **Connect** external mouse, if available
6. **Check** all connections to ensure that all are securely attached
7. **Identify** deficiencies, if present
   - Take specified operator **corrective** actions as directed by the TM
   - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750

- **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority

5-2 Apply Power to the System

NOTE

Operator will perform step 1 or 2 to apply power to the system, not both.

1. **Ensure** that system is properly ventilated by:
   - **Checking** and **ensuring** all system ventilation ports are free of any obstruction
   - **Checking** that the operating location provides for adequate ventilation
2. **Initialize** system using AC Power:
   - **Ensure** that AC Power cord is attached to the Automated Information System, if present
   - **Ensure** that the AC power cord is plugged into an uninterrupted power supply or surge protected power strip
   - **Press** the *power switch* until the power indicator illuminates, then release

NOTE

On the Panasonic CF-72 MCS Workstation and earlier models the power switch is located on the far right side of the computer as you face it. Slide the Power Switch toward the rear of computer until power indicator illuminates, then release.

CAUTION

After confirming that the power indicator has turned on, do not touch the power switch until setup has started. Failure to observe this caution may result in damage to the hard drive.

   - **Observe** that the opening boot screen appears, memory is checked, and the *Begin Logon* dialog box displays
3. **Identify** system irregularities, if any, during boot-up
   - **Take** specified operator **corrective** actions as directed by the TM
   - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
   - **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority
4. **Initialize** system using Battery Power:
   - **Ensure** that a battery is installed in the MCS Workstation
   - **Press** the *power switch* until the power indicator illuminates, then release

NOTE

On the Panasonic CF-72 and earlier models the power switch is located on the far right side of the computer as you face it. Slide the Power Switch toward the rear of computer until power indicator illuminates, then release.

CAUTION

After confirming that the power indicator has turned on, do not touch the power switch until setup has started. Failure to observe this caution may result in damage to the hard drive.

- **Observe** that the opening boot screen appears, memory is checked, and the *Begin Logon* dialog box displays

5. **Identify** system irregularities, if any, during boot-up
   - Take specified operator **corrective** actions as directed by the TM
   - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
   - **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority
   - **Select** *OK* on DOD security message to bring up the *Logon to Window* dialog box
6. **Log on** to the system
   - **Enter** *User name:*
   - **Enter** *Password:*
   - **Select** the *Domain*: from the pull down menu by **clicking** on the *down-arrow* next to the *Domain:* box
   - **Click** *OK.*
7. **Observe** that the Windows Operating System desktop displays

NOTE

Log on per unit SOP, either as administrator or specific user name.

5-3 Perform During Operations Preventative Maintenance Checks and Services

NOTE

For optimum performance, reboot the MCS workstations and gateways every 24 hours and the servers every 72 hours.

1. Periodically **check** the system's computer processing unit cooling fan to ensure that it is operating properly.
2. Periodically **check** the *Windows OS System Tray* to assess the status of the battery.
   - **Determine** if the battery is charging or is charged if the system is on AC Power

NOTE

If the battery is being charged by the system a plug icon will appear in the system tray. Placing your mouse over the icon will cause a dialog box to display showing the percentage charge of the battery.

   - Determine if the battery has enough power to sustain operations of the system if the system is on battery power
3. **Observe** any error messages or unusual actions by the system or application.
4. **Perform** routine system maintenance.
5. Periodically **scan** the system for viruses.
   - **Open** the system's antivirus application
   - **Check** to ensure that the antivirus program is using the latest virus definition file

NOTE

The S6 section can provide you with this information.

- **Ensure** that all scheduled scans in the *Scan History* were completed without error
- **Scan** all removable media, from any source not known to be safe, the first time it is inserted into
  the system
- **Report** any virus infections to the S6 section immediately
- **Close** the antivirus program

6. **Clean** the system surfaces.

NOTE

A soft dry cloth should be used to clean the system. For areas that require more cleaning use detergent diluted with water applied to a piece of gauze or soft cloth that has been thoroughly dry.

CAUTION

Do not use benzene or thinner, or disinfectant-type alcohol on these components:

- **Clean** Display and Touch pad with soft towel
- **Clean** other surface areas
- **Clean** keyboard and CD drives with compressed air
- **Clean** compact disc drive with commercial CD cleaner (monthly or as necessary)

7. **Identify** deficiencies, if present.
   - Take specified operator **corrective** actions as directed by the TM
   - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
   - **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority

The following table identifies additional tasks specific to MCS and the frequency each task is to be performed

Table 1: MCS PMCS

Task	Frequency	Current Settings
1. Verify Network Cable is seated in Network Adapter Card/Slot.	Daily	
2. Turn On Power	Daily	
3. MCS Synchronizes Time with the Active Directory, make sure both Active Directory and PASS are Synchronized		
4. Start C2 Management Console a. Verify Data Source b. Verify Org ID	See Note (at bottom)	

c. Verify NRTS d. Verify Pass e. Verify Messaging C2R f. Verify Security Level g. Verify/Configure Time Server (Active Directory IP)		
5. Start Message Log a. Clean out all messages that are not needed.		
6. Conduct Normal Operations	Daily	
7. Backup all data	Site dependent	
8. Defrag Hard Drive	Weekly	
9. Re-Boot System every 24 hours	Daily	
10. Shut down and re-start the C2PC Gateway	Every 4 - 6 Hours	
11. Shut down and re-start the TMS Broker	Every 4 - 6 Hours	
12. Update Statistics within the Database Management System (DBMS)	Periodically	

NOTE: The C2 Management Console should only be run during the following circumstances.

- **After Initial Installation of Software.**
- **If you have been told to re-role your system i.e., from CDR to S3.**
- **If you have been told to change Pass Nodes.**
- **If you have been told to change C2R Roles**

5-4 Perform Pre-Shut Down After Operations Preventative Maintenance Checks/Services

1. **Save** all data.
2. **Close** all applications.

NOTE

Operator should be at the Windows desktop at this point.

NOTE

This search displays all zip files on your system. You probably will not want to delete all of them. Be especially sure before selecting all files to delete.

3. **Cleanup** old files on the system.
   - **Right-click** on *Start* and **select** *Explore.* Wait for *Windows Explorer* to open

4. **Remove** old zip files by:
    - **Click** on the *Search* button on the *Standard Buttons* toolbar
    - **Enter** "*.zip" in the *Search for files or folders named:* text box
    - **Select** *Local Hard drives* in the *Look in: pull down* menu
    - **Click** on the *Search Now* button and wait for the search to complete
    - **Hold down** the *Ctrl* key and **use** the mouse to **left click** *select* each of the zip files that you wish to delete or if you wish to delete all of the zip files click on *Edit* on the menu bar and **select** *Select All*

NOTE

This search displays all zip files on your system. You probably will not want to delete all of them. Be especially sure before selecting all files to delete.

5. **Remove** files that begin with a tilde (~) as follows:

NOTE

Ensure that all application programs, such as word-processing, spreadsheet, and graphics programs, are closed first since the temporary file that you are viewing in these applications sometimes uses a tilde (~).

- **Enter** "~*.*" in the *Search for files or folders named:* text box
- **Select** *Local Hard drives* in the *Look in: pull down* menu
- **Click** on the *Search Now* button and wait for the search to complete
- **Click** on *Edit* on the *menu bar* and **select** *Select All*
- **Click** on *File* on the *menu bar* and **select** *Delete*

6. **Remove** chk files as follows:
    - **Enter** "*.chk" in the "*Search for files or folders named:"* text box
    - **Select** *Local Hard drives* in the *Look in: pull down* menu
    - **Click** on the *Search Now* button and wait for the search to complete
    - **Click** on *Edit* on the *menu bar* and **select** *Select All*
    - **Click** on *File* on the *menu bar* and **select** *Delete*
7. **Delete** temporary files using the Disk Cleanup utility
    - **Click** on the *Folders* button on the *Standard Buttons* toolbar in *Windows Explorer*
    - **Right-click** on *Local Disk (C)* and **select** *Properties*. Wait for the *Volume (?) Properties* tool to open
    - **Select** the *Disk Cleanup* button on the *General* tab. Wait for the *Disk Cleanup* utility to open
    - **Click** on the *check box* next to each of the type of temporary files that you wish to purge
    - **Click** on the *OK* button
    - **Click** on the *Yes* button on the *Disk Cleanup for Local Disk (C)* dialog box. Wait for the *Disk Cleanup utility* to finish purging all selected file types
8. **Back-up** critical user files from the system.

CAUTION

Ensure that any removable media (disk, CD, or tape) used to perform the Back-up is appropriately marked and handled based on the classification level of the material backed up on it.

- **Right-click** on *Local Disk (C)* and select *Properties.* Wait for the *Volume (?) Properties* tool to open
- **Select** the B*ackup Now* button on the *Tools* tab. Wait for the Backup utility to open
- **Select** the *Backup* tab
- **Select** the volumes and/or folders to be backed up

NOTE

Sub directories can be selected by expanding (clicking on the "+" sign next to the volume) the volume in the "Tree" window or clicking on the volume and selecting the desired folders in the "Folder" window.

- **Click** on the *Browse* button next to the *Backup Media or File Name:* box in the lower left corner of the *Backup* utility window
- **Navigate** to the desired volume and folder in the *Open* window. **Select** the backup file to be used or name a new backup file in the *File Name:* box
- **Click** the *Open* button on the *Open* window
- **Select** the *Start Backup* button on the lower right corner of the *Backup* utility window
- **Enter** a description of the backup in the *Backup Description* text box or accept the default description in the *Backup Job Information* window
- **Select** the *Append this backup to the media* or R*eplace the data on the media with this backup* option button in the I*f the media already contains backups:* box
- **Enter** a description of the backup in the I*f the media is overwritten, use this label to identify the media:* text box or accept the default description
- **Select** the *Advanced* button
- **Select** *Verify data after backup* check box in the *Advanced Backup Options* window
- **Select** the *OK* button
- **Select** the *Start Backup* button on the *Backup Job Information* window
- **Observe** for error messages during the backup process

NOTE

If an error occurs, contact your MAA for assistance.

- **Select** *Close* on the *Backup Progress* dialog box

NOTE

You can view, print, or save a copy of the backup status report by selecting the Report button on the Backup Progress dialog box. It is recommended that you print out the report if an error occurs during the backup process.

- **Click** on *Job* on the *menu bar* and select *Exit* in the *Backup* utility window.

9. **Defragment** the system's storage volume or volumes as follows.

NOTE

This step is only necessary if after analysis the system recommends that you defragment your volume.

- **Right-click** on *Local Disk (C)* and select *Properties*. **Wait** for the *Volume (?) Properties* tool to open
- **Select** the *Defragment Now* button on the *Tools* tab. **Wait** for the *Disk Defragment* utility to open.
- **Select** the volume to be analyzed
- **Click** on the *Analyze* button. **Wait** for the *Analysis Complete* dialog box to display
- If the *Analysis Complete* dialog box recommends that the volume be de-fragmented or you wish to defragment the volume, **click** on the *Defragment* button. **Watch** to ensure that the de-fragmentation process starts

CAUTION

Ensure that the volume has at least 15% free space before starting the de-fragmentation process.

NOTE

You can view, print, or save a copy of the analysis report by selecting the View Report button on the Analysis Complete dialog box.

NOTE

It is recommended that all applications be shut down before beginning the de-fragmentation process.
Having applications open will significantly slow down the process.

NOTE

The de-fragmentation process can, depending on the size of the volume, take several hours to complete. Keep this in mind before starting the process.

- **Select** *Close* once the *De-fragmentation Complete* dialog box appears

NOTE

You can view, print, or save a copy of the analysis report by selecting the "View Report" button on the Defragmentation Complete dialog box.

- **Close** the *Disk De-fragmentation* utility by **clicking** on the *close icon* (X) in the upper right corner of the *title bar* or **right-clicking** on the *title bar* and selecting *Close*
- **Repeat** the tasks in step 9 above for each volume. **Check** the integrity of all storage volume(s)
- **Right-click** on the volume that needs to be checked (A, C, etc.) and **select** *Properties*. Wait for the *Volume (?) Properties* tool to open

NOTE

Always select the volume with the Windows OS directory last as a restart of the computer is probably necessary.

- **Select** the *Check Now* button on the *Tools* tab. **Wait** of the *Check Disk* utility to open
- **Select** both *Check disk options* and **click** on the *Start* button
- **Select** *Yes* if the *Checking Disk* dialog box message: The disk check could not be performed because exclusive access to the drive could not be obtained. Do you want to schedule this disk check to occur the next time you restart the computer?

- **Select** *OK* on the *Disk Properties* window
- **Select** *OK* when the *Checking Disk (?:/)* dialog box appears
- **Click** on the *OK* button to **close** the *Volume (?) Properties* tool
- **Repeat** the above steps for each volume

10. **Restart** the computer as follows:
    - **Click** on *Start* and **select** *Shut Down*
    - **Select** *Restart* from the *pull down* menu
    - **Select** *OK*
    - **Wait** for the *Microsoft Windows* to restart
    - **Observe** the startup procedure to ensure that no file or disk errors are identified
11. **Identify** any deficiencies, if present.
    - Take specified operator **corrective** actions as directed by the TM
    - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
    - **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority

5-5 Perform Shut Down of the MCS Workstation and Gateway

1. **Remove** all removable media discs from the system.
2. **Select** the *Windows Start* button.
3. **Select** *Shut Down* from the *start* menu.
4. **Select** *Shut down* from the *pull down* menu on the *Shut Down Windows* dialog box.
5. **Select** the *OK* button.

NOTE

You should observe the Shut Down Windows dialog menu close, all opened menus and icons close, and the computer system's screen blank out.

6. **Look** for any error messages or unusual actions by the system during the shut down process.
7. **Identify** deficiencies, if present.
    - Take specified operator **corrective** actions as directed by the TM
    - **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
    - **Submit** a completed DA Form 2404 or 5988E to appropriate maintenance authority

5-6 Perform Post-Shut Down After Operations PMCS

1. **Perform** routine system maintenance.
2. **Clean** the system surfaces.

NOTE

A soft dry cloth should be used to clean the system. For areas that require more cleaning use detergent diluted with water applied to a piece of gauze or soft cloth that has been thoroughly wrung.

CAUTION

Do not use benzene, thinner or disinfectant-type alcohol.

- **Clean** the Display
- **Clean** the Touch pad
- **Clean** other surface areas
- **Clean** the keyboard and CD drives with compressed air
- **Clean** the compact disc drive with commercial CD cleaner (monthly or as necessary)

3. Disassemble system components.

CAUTION

Do not set equipment on a damp or wet floor during the disassembly process.

- **Remove** the Removable Hard Disk Drive (RHDD), if required

CAUTION

The Mission Application Administrator (MAA) should be contacted to install the RHDD.

- **Install** the battery, if required

NOTE

On some MCS models a fully discharged battery will not charge when installed in the system. A fully discharged battery should be charged using the battery charger before reinstalling in the computer.

CAUTION

If the cover is not attached properly, the battery may fall out while the computer is being carried.

- **Disconnect** the AC power adapter with cord, if required
- **Disconnect** the LAN (RJ-45) connector, if required
- **Disconnect** the external mouse, if available

4. Visually inspect cables and connectors for the following:
   - Burns
   - Broken
   - Frayed
   - Loose
   - Missing components
5. **Inspect** all hardware for the following:
   - Cracks
   - Deformation
   - Loose attachment hardware
6. **Conduct** an inventory of system components
7. **Identify** deficiencies, if present.
   - Take specified operator **corrective** actions as directed by the TM

- **Complete** the applicable blocks on a DA Form 2404 or 5988E IAW DA Pam 738-750
- **Submit** completed DA Form 2404 or 5988E to appropriate maintenance authority

5-7 Shut Down and Re-Start Both C2PC and TMS Broker

The TMS Broker looses connection with the C2PC Gateway. To remedy this condition the MAA is required to stop and start both the TMS Broker and the C2PC Gateway Services. The following steps describe how to perform this required operation. With this release of the MCS product, this action is required every 4 to 6 hours to prevent the loss of connection or if the COP is being cleaned.

1. **Stop** the *TMS Broker*.
2. **Stop** the *C2PC Gateway Manager*.
3. **Start** the *C2PC Gateway Manager*.
4. **Start** the *TMS Broker*.

Chapter 6 Supplementary MCS Server Software Setup

6-1 MCS Database Restore

6-1.1 MCS Database Restore Procedure

After completing the software installation of the Server, the MCS database needs to be restored. The following steps describe the procedure necessary to configure the initial MCS Database.

1. **Start** the *Enterprise Manager* by selecting *Start, Programs, Microsoft SQL Server, Enterprise Manager.*
2. **Expand** *Microsoft SQL Servers*.
3. **Expand** *SQL Server Group*.
4. **Expand** your server group (e.g., D_REAR_SVR (Windows NT)).
5. **Right-click** on *Databases*.
6. **Select** *All Tasks*.
7. **Select** *Restore Database.* The *Restore Database* window appears.

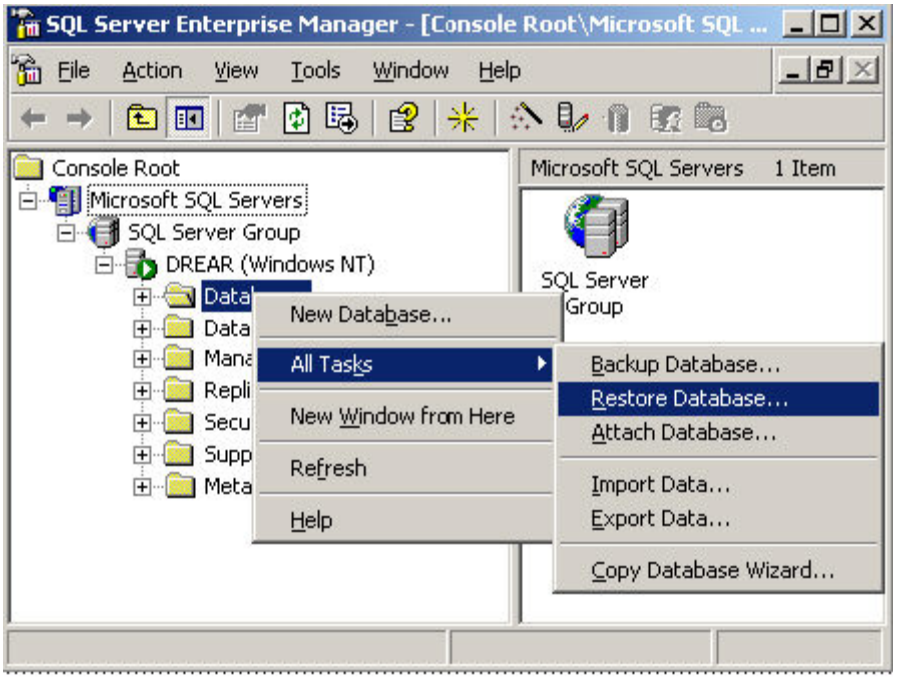


Figure 6-1 Start Enterprise Manager

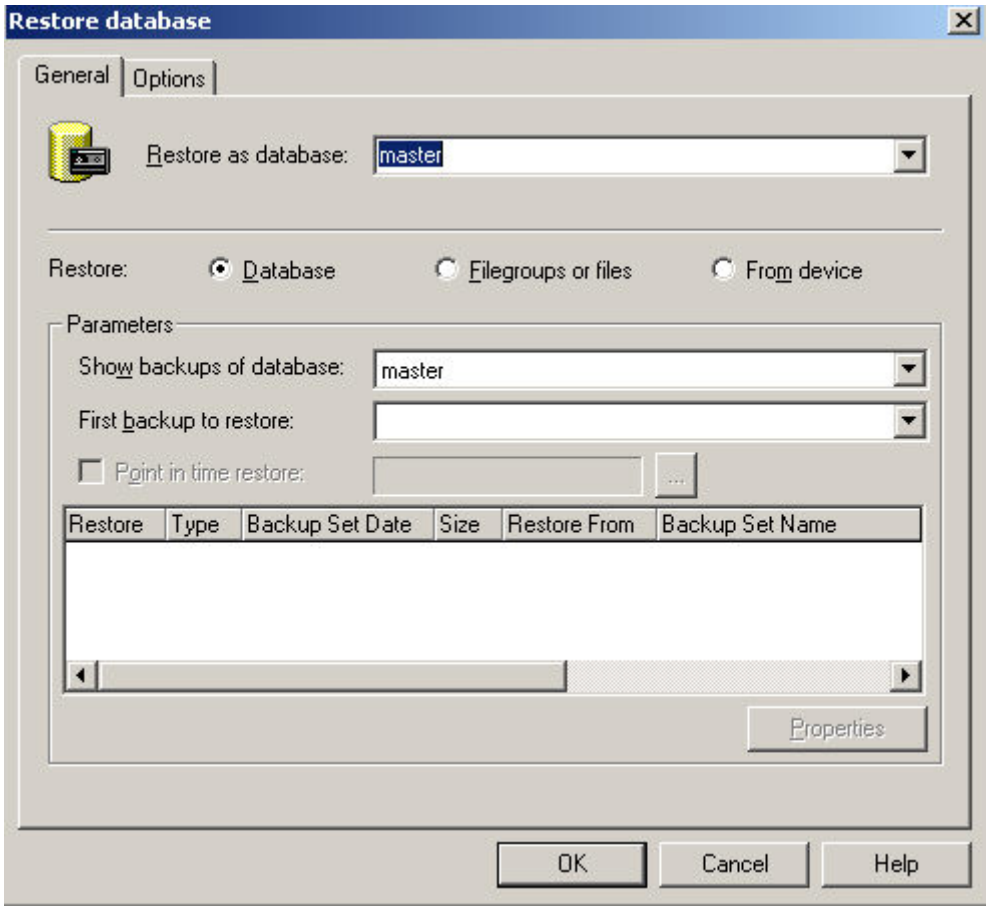


Figure 6-2 Restore Database General Tab

8. **Enter** “mcs_db” in the *Restore as database* text field.
9. **Select** the *Restore From device* option button. The *Restore Database* window**.**

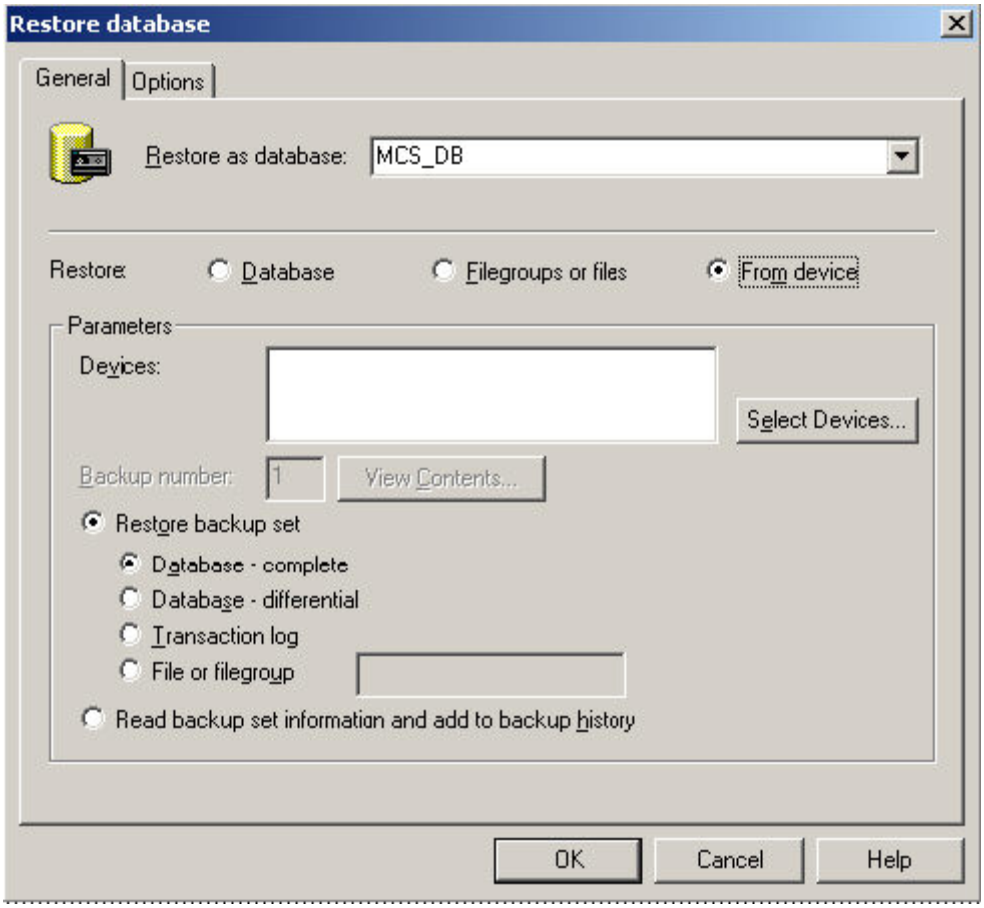


Figure 6-3 Restore Database from device window

10. **Accept** other default settings.
11. **Select** the *Select Devices* button. The *Choose Restore Devices* window opens.

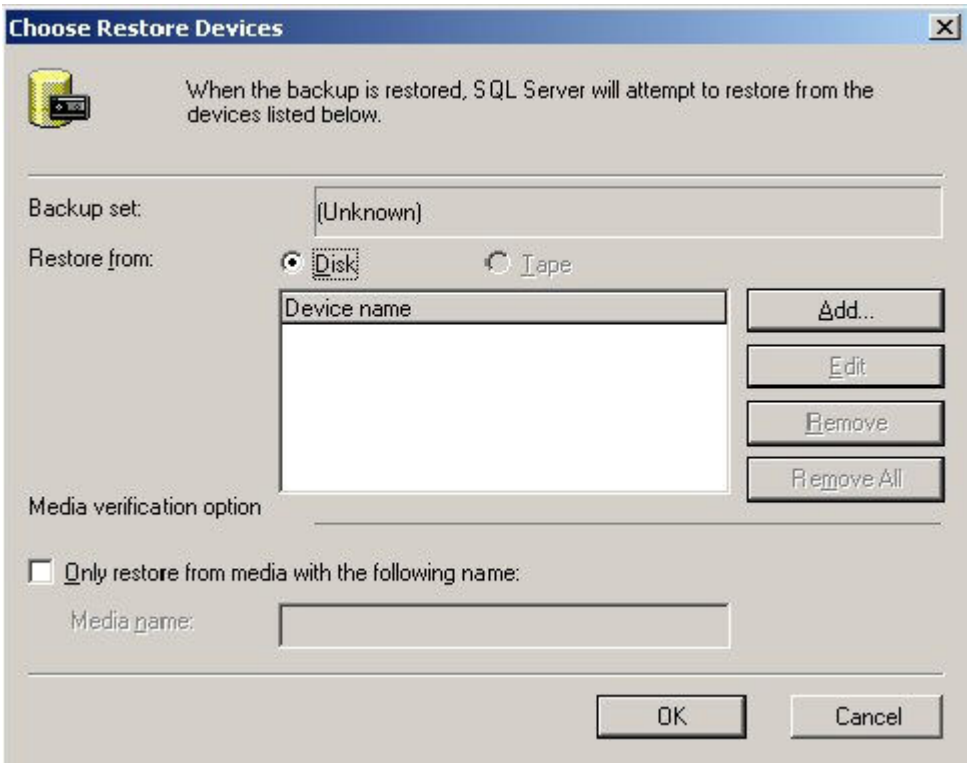


Figure 6-4 Choose Restore Devices Window

12. From the *Choose Restore Devices* window, **select** the *Disk* option button.
13. **Click** the *Add* button. The *Choose Restore Destination* window opens.

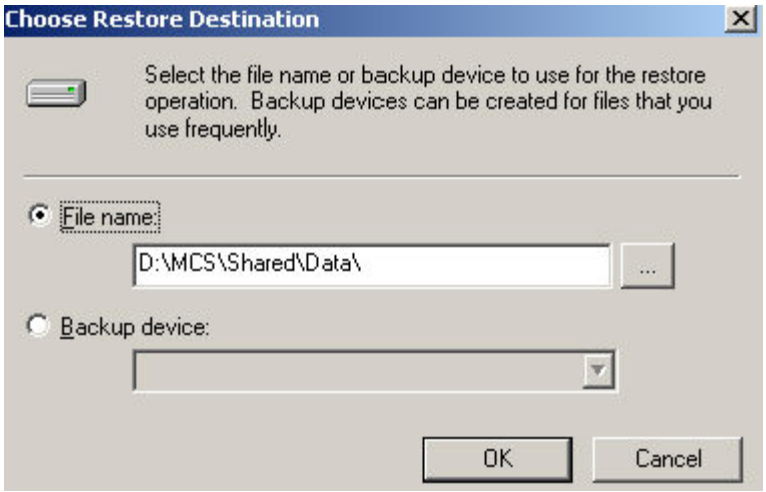


Figure 6-5 Choose Restore Destination Window

14. From the *Choose Restore Destination* window, **select** the *File name* option button.

NOTE

In this window do Not select the OK Button at this time.

15. **Click** the "…" button. The *Backup Device Location (Local)* window opens.

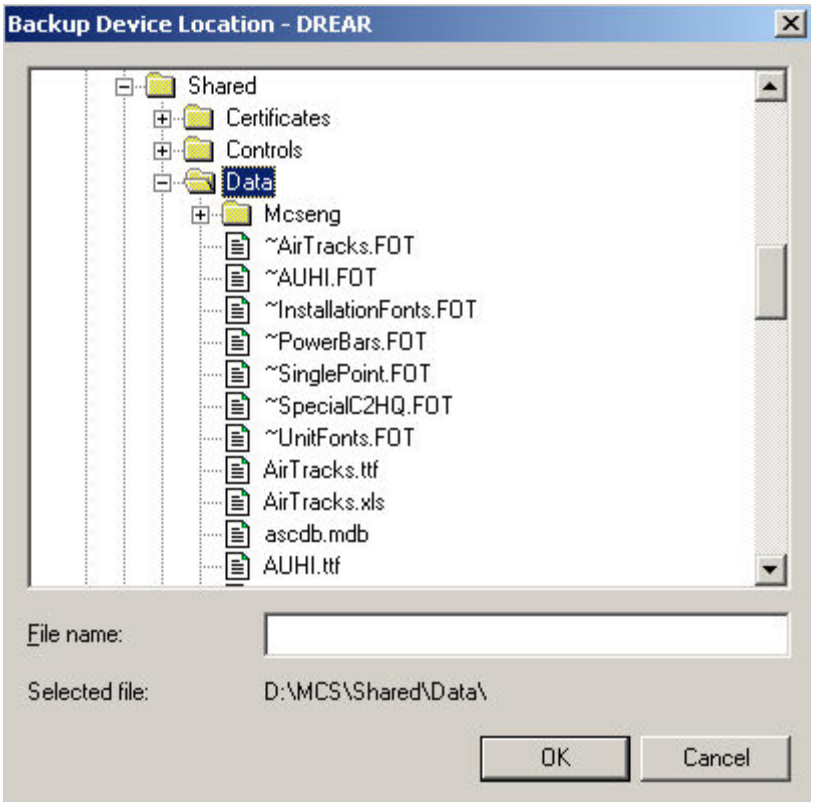


Figure 6-6 Backup Device Location Window

16. From Backup Device Location window, **navigate** to the *<drive letter>:\MCS \ Shared \ Data* folder.
17. **Select** the *Sql_mcs_db* file.
18. **Click** *OK.* The *Backup Device Location* window closes, and the path and file name appear in the *Choose Restore Destination* window.
19. From the *Choose Restore Destination* window, **verify** that the file name is correct.
20. **Click** *OK.*
21. From the *Choose Restore Devices* window, **verify** that the file name is correct.

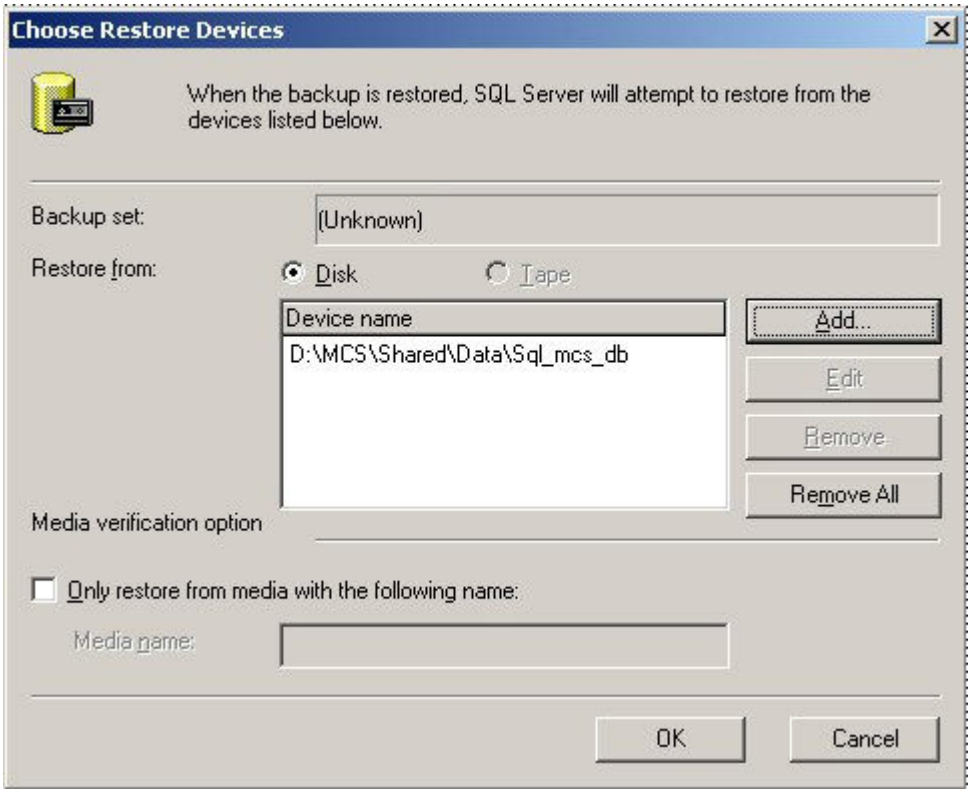


Figure 6-7 Choose Restore Devices Window

22. **Select** *OK*. The *Restore Database* window appears.

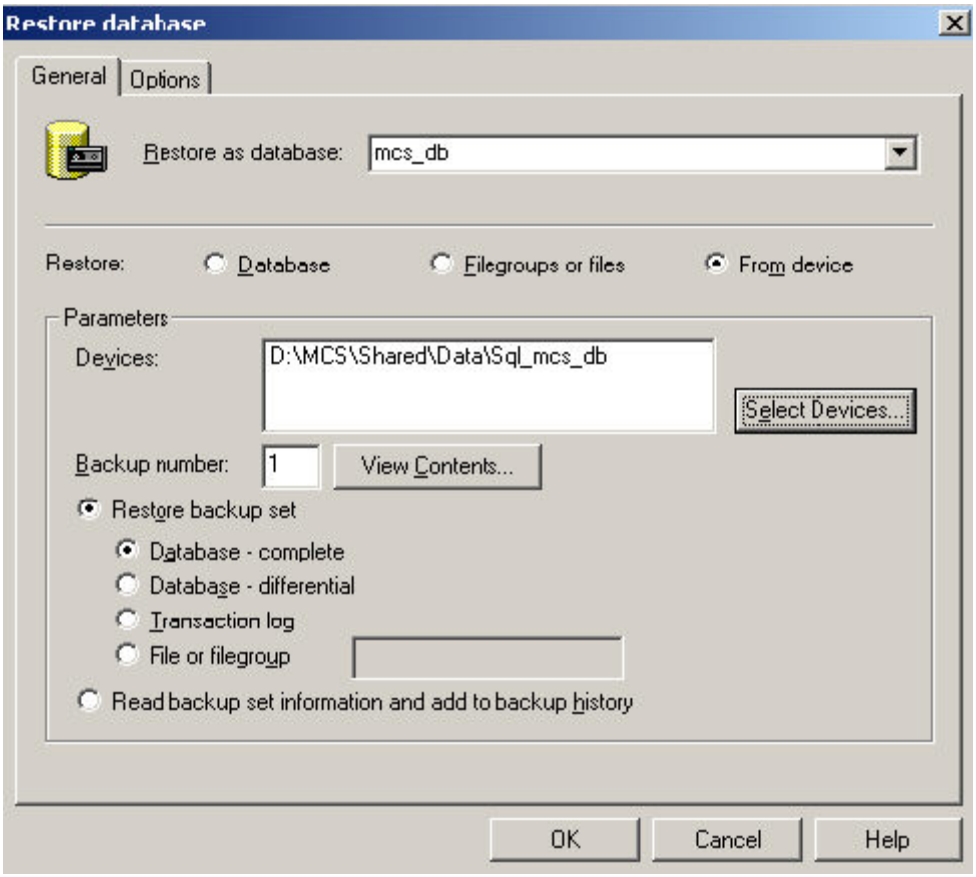


Figure 6-8 Restore Database Window - Devices Selected

23. From the *Restore Database* window, **verify** information is correct.
24. **Click** *OK. The Restore Progress* window appears.

NOTE

At first the Restore Progress window progress bar appears as though nothing is being accomplished. After a pause, the progress bar will show progress as data is being passed into the database.

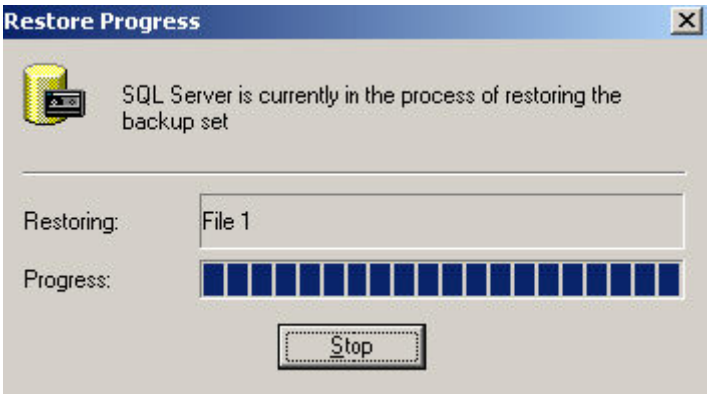


Figure 6-9 Restore Progress Window

25. When the restore process is finished, the *SQL Server Enterprise Manager* confirmation window appears.

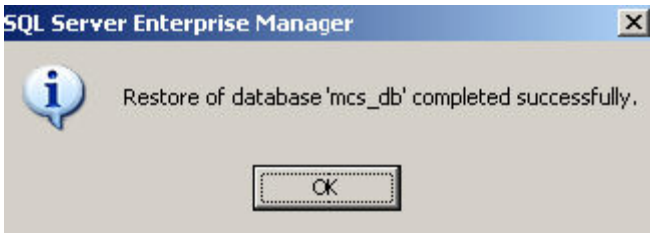


Figure 6-10 SQL Server Enterprise Manager Confirmation Window

26. **Click** *OK*.
27. The MCS database is now restored.

6-1.2 Creating a New User

Now that the MCS database is restored, a user must be created to use the database.

NOTE

For SQL database replication, a mcsuser account (login & password) MUST be present.

1. From the *SQL Server Enterprise Manager* window, **verify** *mcsuser* does not exist in the *Logins* Name area. If *mcsuser* exists, **delete** it.
2. **Select** *Security* and **right-click** on *Logins*. A pop-up menu appears.

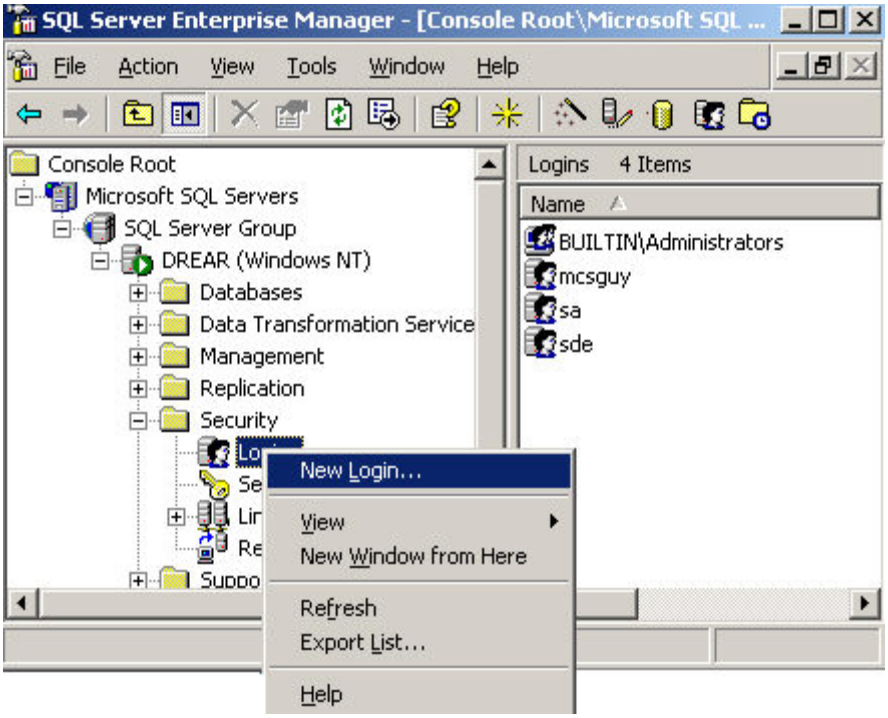


Figure 6-11 SQL Server Enterprise Manager Window

3. **Click** on *New Login*. The *SQL Server Login Properties* window opens.

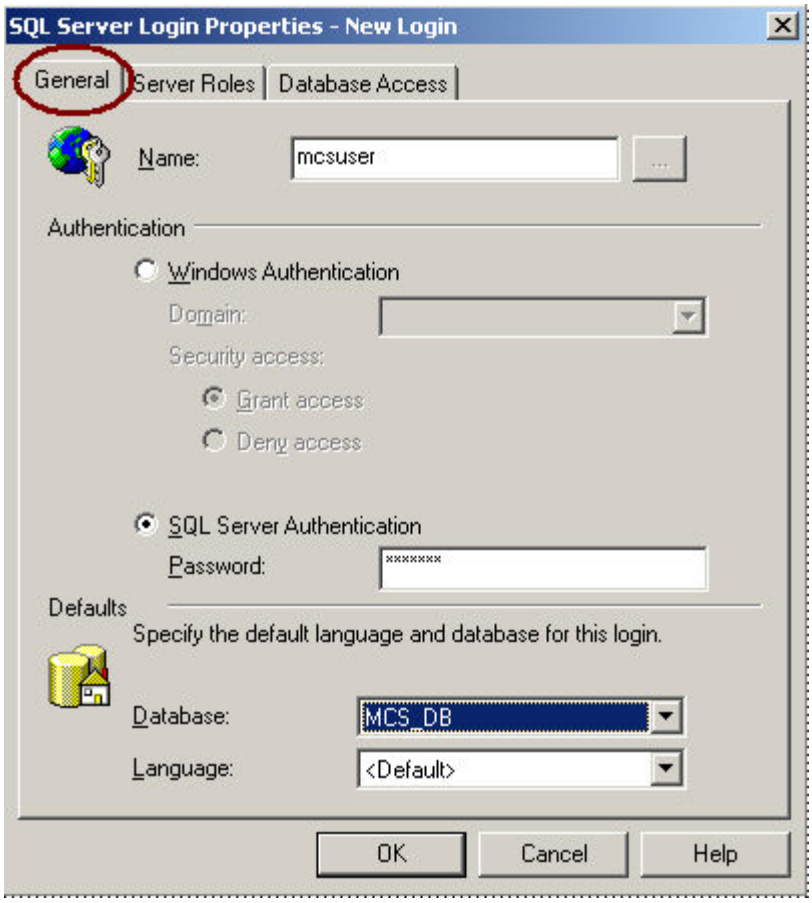


Figure 6-12 SQL Server Login Properties Window - General Tab

4. From the *General* tab, **enter** the SQL Login User name (“mcsuser”) in the *Name* field.
5. From the *General* tab, **select** the *SQL Server Authentication* option button and **enter** the associated password.
6. In the *Database* box, **click** the *down arrow.* A *drop-down* list of databases appears.
7. From the list, **select** *MCS_DB*.
8. **Click** the *down-arrow* in the *Language* box. A list of languages appears.
9. From the list, **select** <*Default*>.
10. **Select** the *Server Roles* tab in the *SQL Server Login Properties* window.

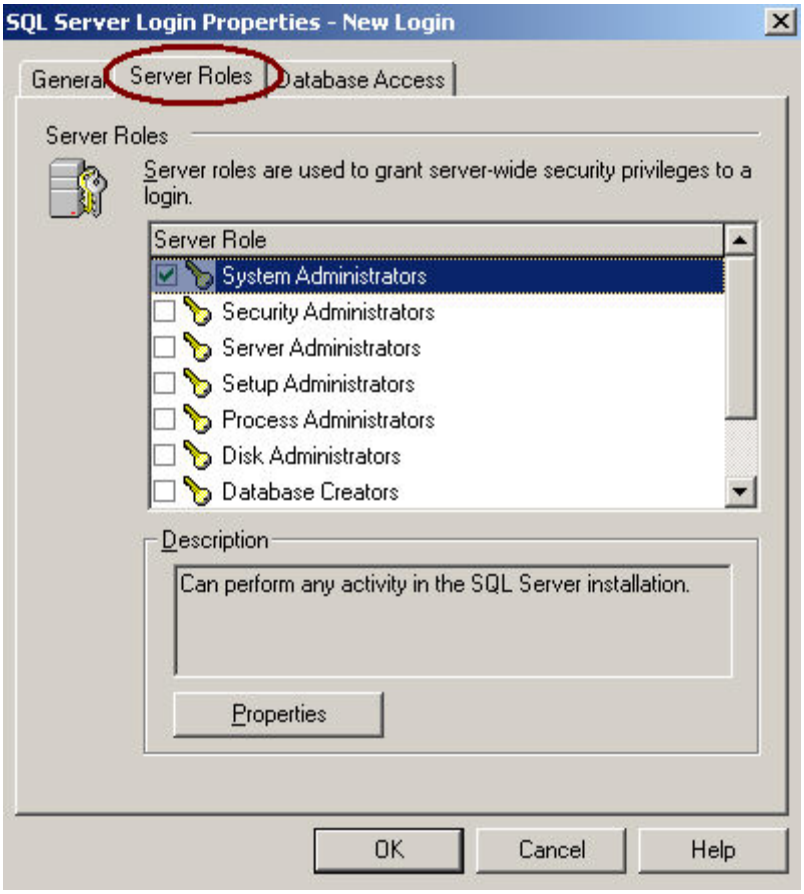


Figure 6-13 SQL Server Login Properties Window - Server Roles Tab

11. From the *Server Roles* tab **check** *System Administrators* (see the figure above)
12. **Select** the *Database Access* tab.

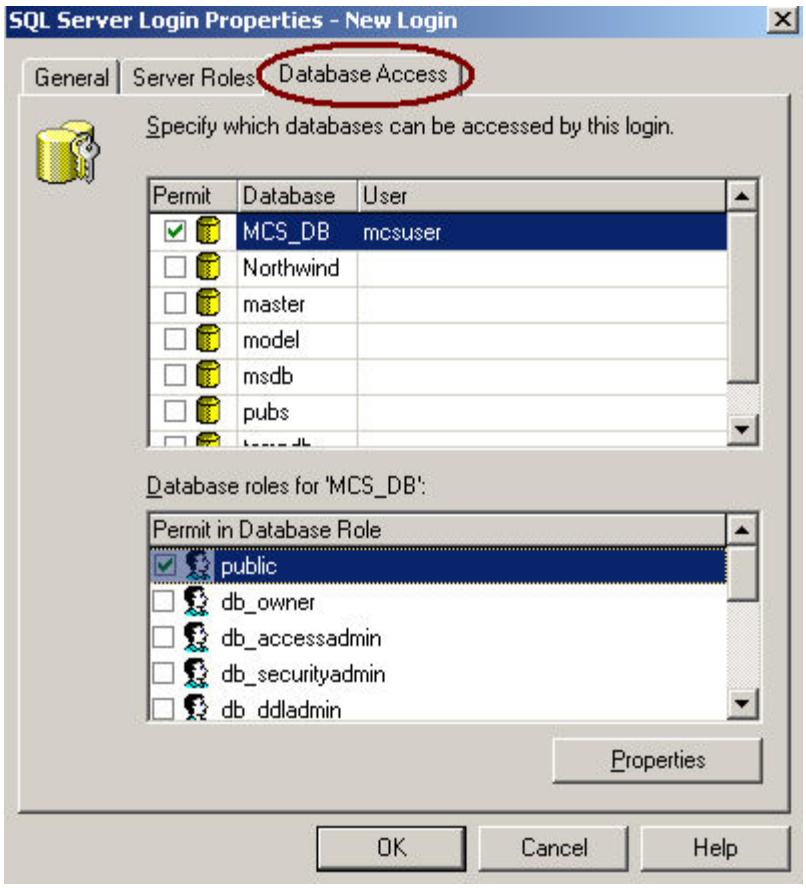


Figure 6-14 SQL Server Login Properties Window - Database Access Tab

13. From the *Database Access* tab, **select** *MCS_DB* in the upper frame.
14. From the lower frame, *Database Roles for MCS_DB*, **select** *public.*
15. **Select** *OK.* The *Confirm Password* window appears.

Figure 6-15 Confirm Password Window

16. **Enter** the account password in the *Confirm new password* box.
17. **Click** *OK.* The account login and password are now set for database use.
18. **Close** the *SQL Server Enterprise Manager*.

6-2 Message Data Replicator (MDR)

6-2.1 Introduction to Message Data Replicator (MDR)

The MCS Message Data Replicator (MDR) application can be used to process incoming USMTF and JUNIT messages into the database. Typically it is used on the units SQL Server box. The SQL Server MCS_DB functions as a central database server for MCS machines.

6-2.2 Set Up the MCS Lookup Table

The MDR uses the MCS_Lookup.mdb access database to translate between values received from the message and the data source MCS_DB. To ensure that consistent values are used between the MDR and the MCS_DB this database needs to link in one of the MCS_DB tables. Link in the table Org_Symbol_Code from the SQL Server MCS_DB into this database. Call this linked table ORG_SYMBOL_CODE.

To link tables from the SQL Server MCS_DB to the MCS_Lookup.mdb follow these steps:

NOTE

Copy the <drive-letter>:/MCS/Shared/Data/MCS_Lookup.mdb file from the MCS Workstation System onto the Server System into the same folder if the MCS_Lookup.mdb file does not exist on the Server System.

1. In Windows Explore, **navigate** to the *<drive-letter>:/MCS /Shared/Data* folder.
2. **Double-click** on the *MCS_Lookup.mdb* file. The *Microsoft Office Access* window opens. **Click** *Yes*. Depending on the level of security, you may experience security warnings of the file being opened. You can safely ignore both of the security warnings as shown here by clicking *Open*. The *MCS_Lookup:Database* window opens.

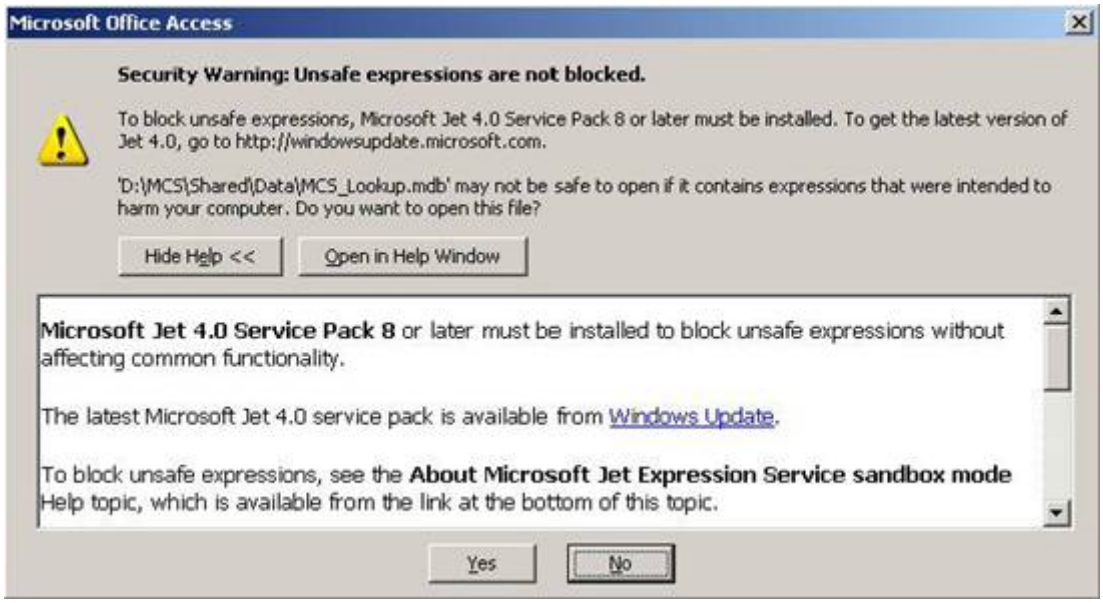


Figure 6-16 Microsoft Office Access Window

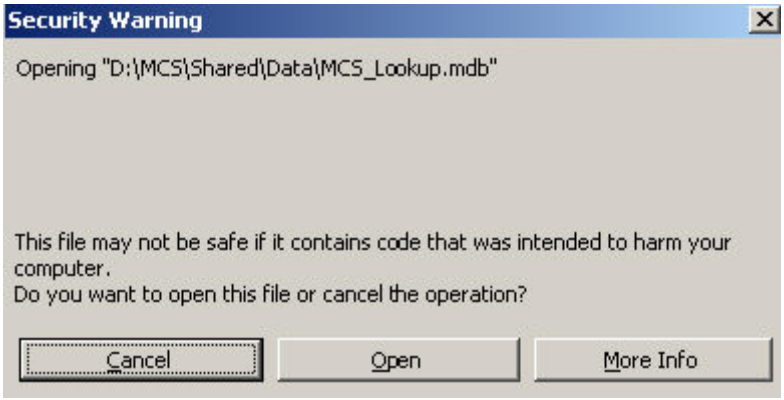


Figure 6-17 Security Warning Window

3. **Select** *Tables,* then **right-click** on a white space and **select** *Link Tables.* A *Link* window opens.

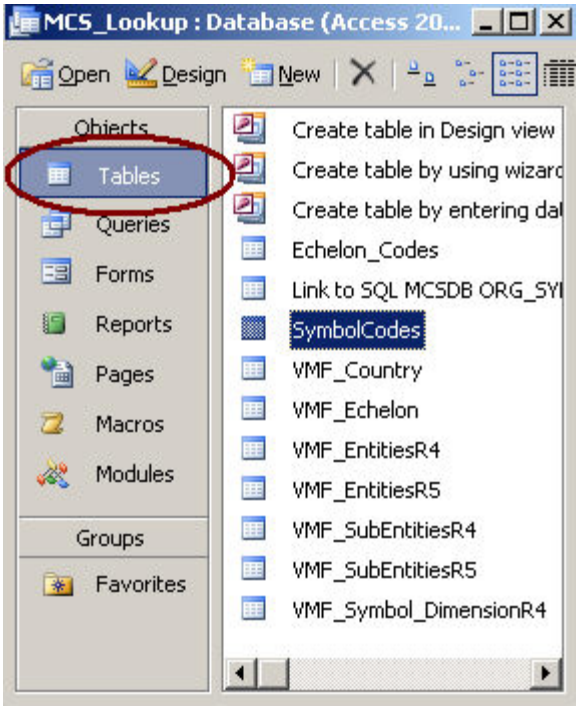


Figure 6-18 MCS_Lookup: Database Window

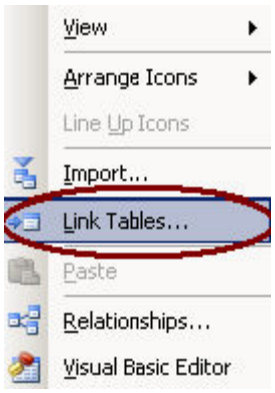


Figure 6-19 Pop-Up Window - Link Tables

4. In the *Link window* that opens, **set** *Files of type:* to ODBC Databases. A *Select Data Source* window opens.

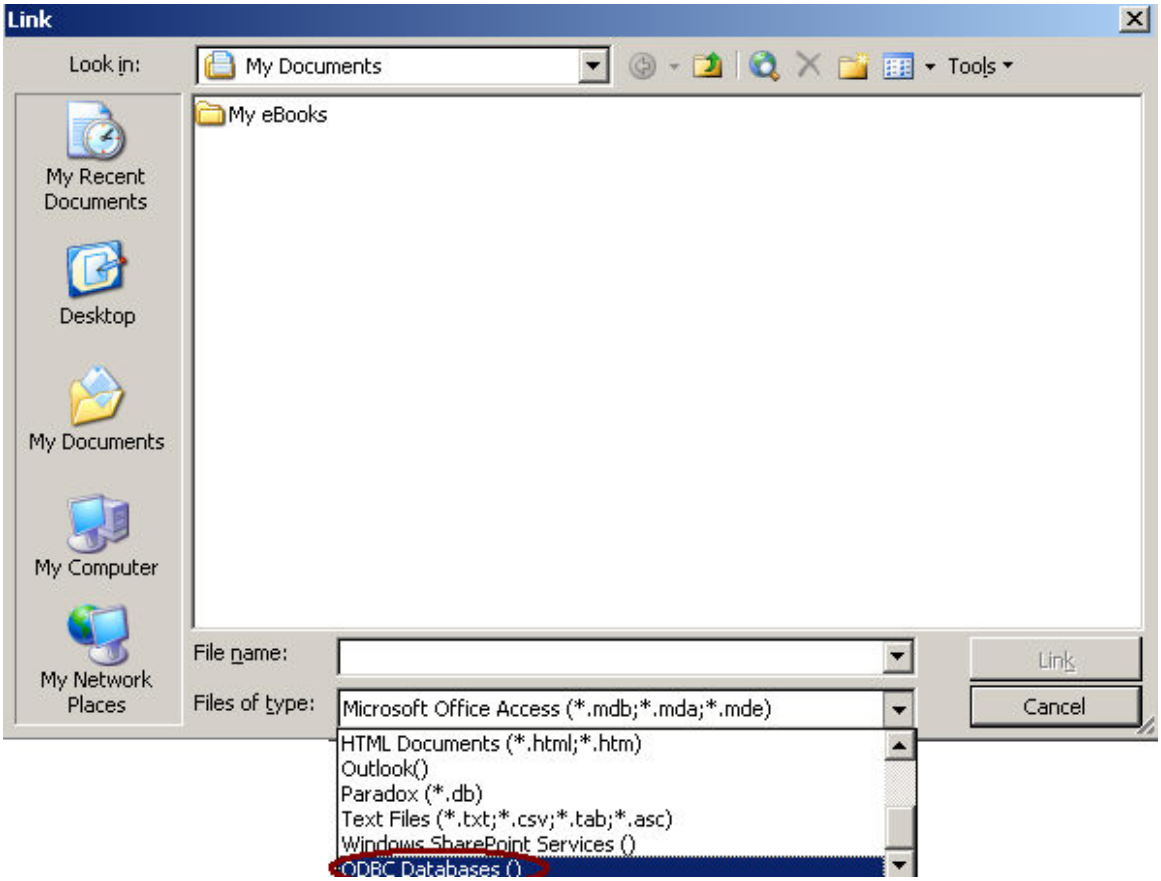


Figure 6-20 Link Window

5. **Select** the *Machine Data Source* tab in the Select *Data Source Window*. **Locate** the SQL Server you want to link to, **select** this server and **click** *OK*. The *SQL Server Login* window is displayed.

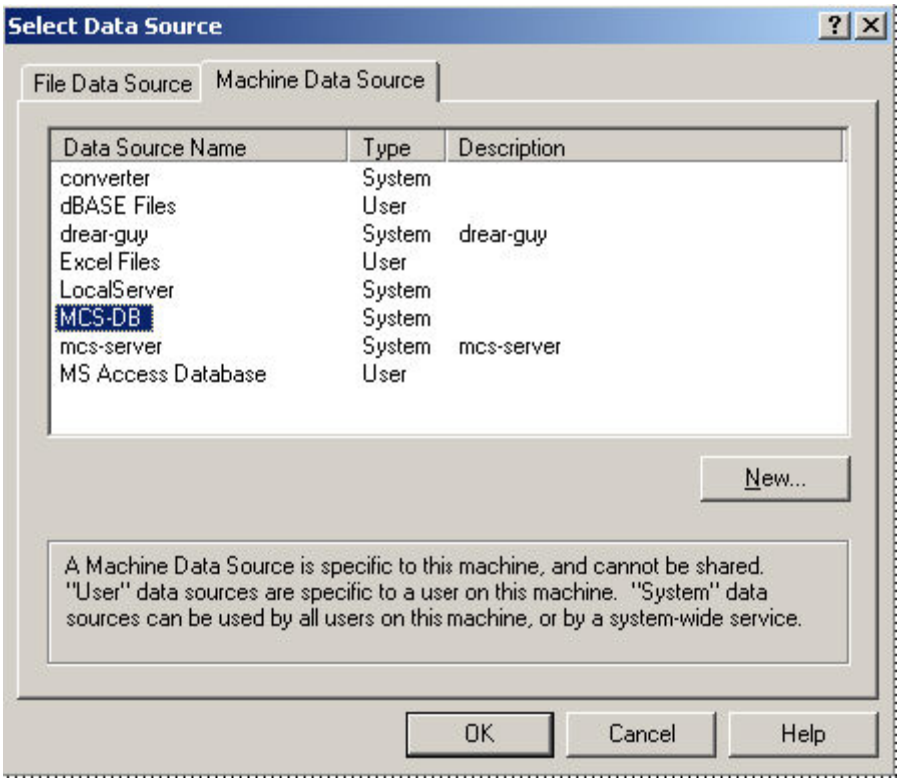


Figure 6-21 MDR Select Data Source Window

6. **Select** the *Use Trusted Connection* or **enter** the appropriate *Login ID and Password* as shown in the *SQL Server Login* window below. **Click** *OK* to connect to the SQL Server selected. The *Link Tables* window will then be displayed.

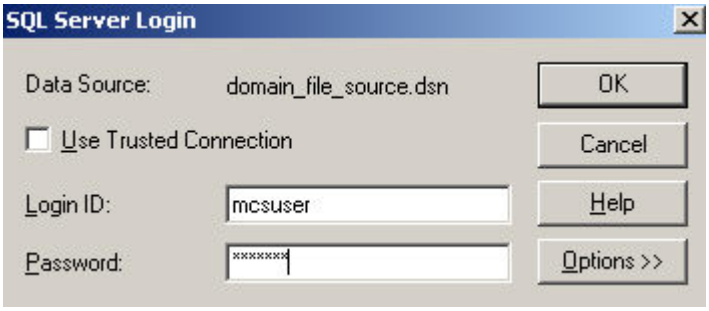


Figure 6-22 MDR to SQL Server Authentication Window

7. In the *Link Tables* window **locate** and **select** the *dbo.Org_Symbol_Code*.

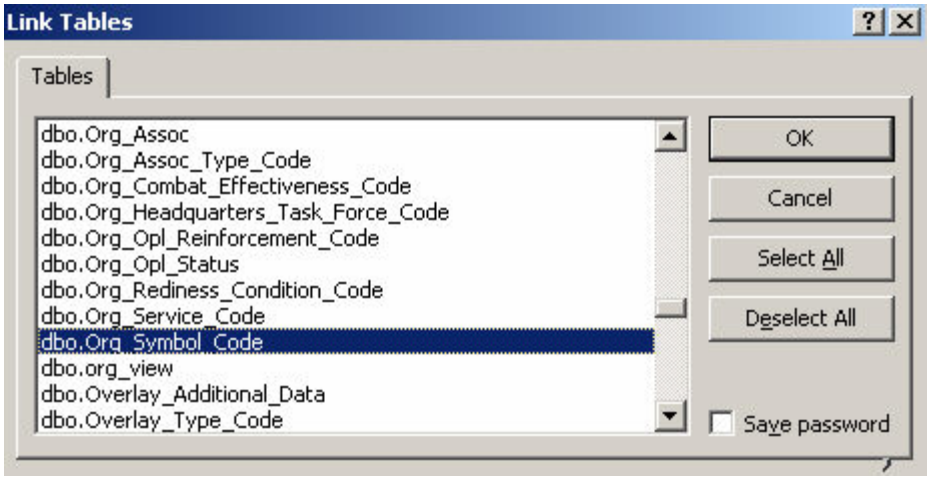


Figure 6-23 Link Tables Window

8. **Select** the *Save password* check box and **click** *OK*. The table is now linked and named *dbo_Org_Symbol_Code*.

9. **Rename** the linked table to *Org_Symbol_Code* by **right-clicking** on the *dbo_Org_Symbol_Code*; **select** *Rename* and make the necessary change.

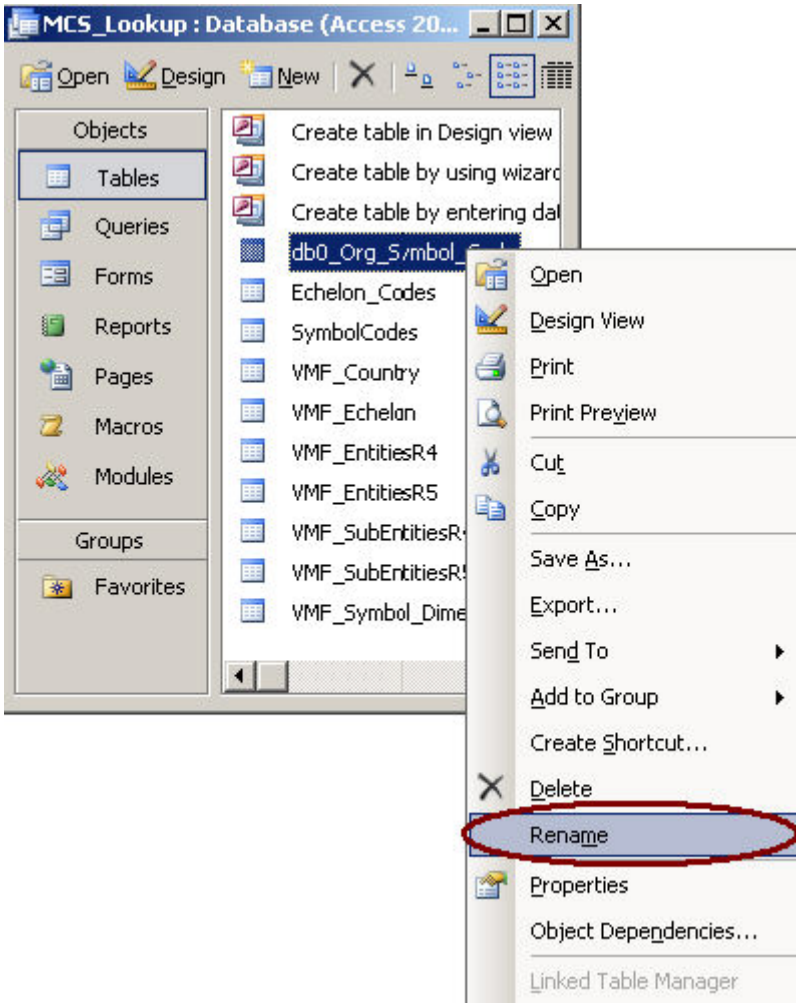


Figure 6-24 Rename the Linked Table

6-2.3 Creating a New Data Source

A Data Source is an access point to a remote database. Many applications use configured *Data Sources* to connect with remote databases. The following steps outline the procedure required to create a new data source.

1. **Start** the *Microsoft Access Data Base Utility* as in previous section (Set Up the MCS Lookup Table).
2. **Open** the *Select Data Source* window.

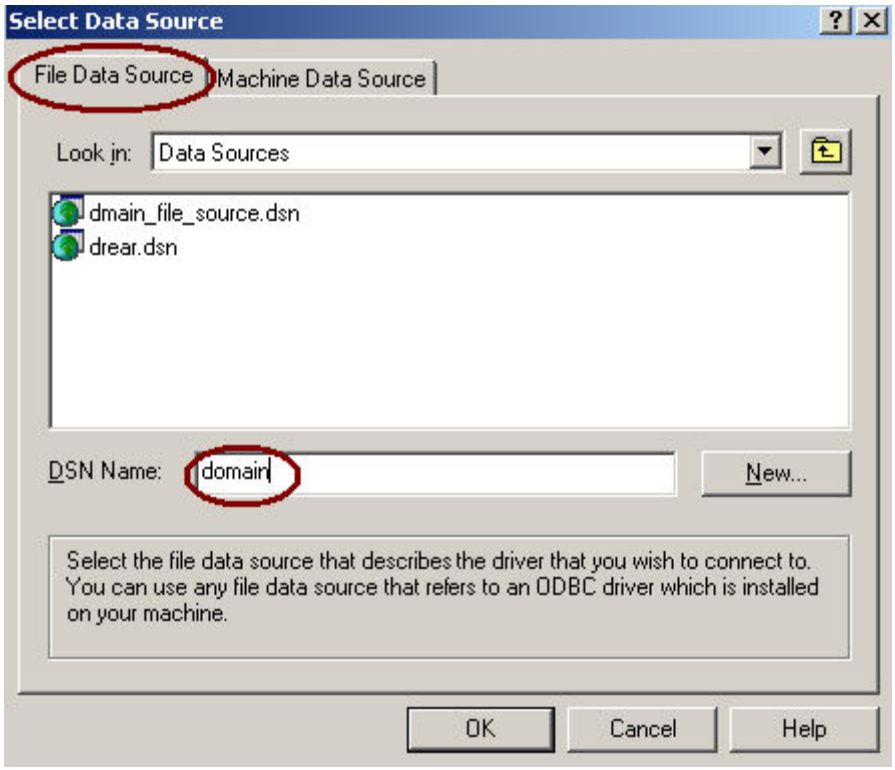


Figure 6-25 Select Data Source Window

3. **Select** the *File Data Source* tab as shown above.
4. **Enter** a new data source name into the *DSN Name* field. In this sample exercise we have entered the DSN Name of “domain.”
5. **Click** the *New* button. The *Create New Data Source* window opens.

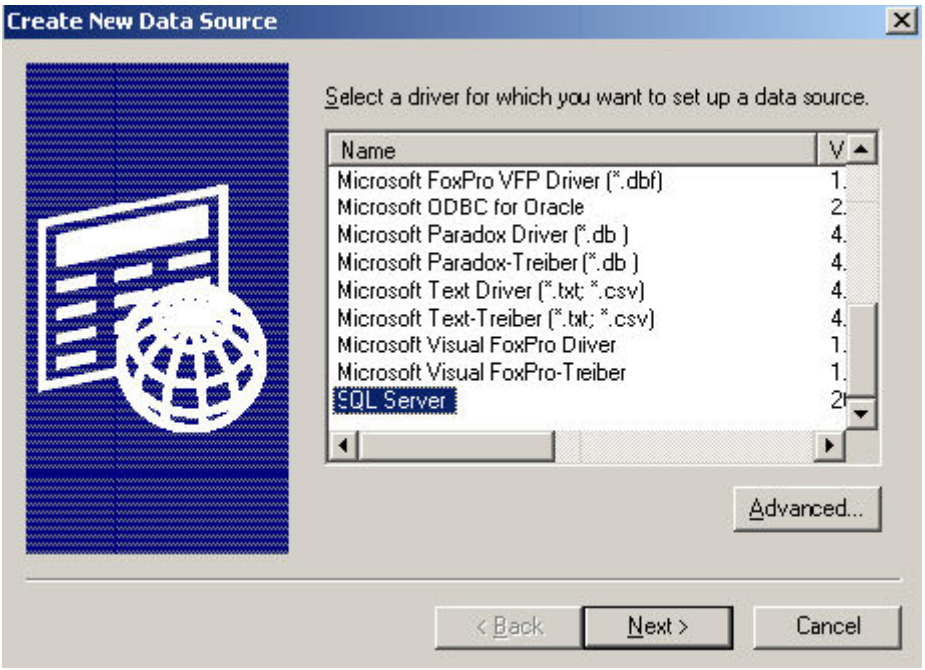


Figure 6-26 Create New Data Source Window

6. From the *Create New Data Source* window, **select** *SQL Server*.
7. **Click** *Next.*
8. **Enter** the filename you want to save the data source under.

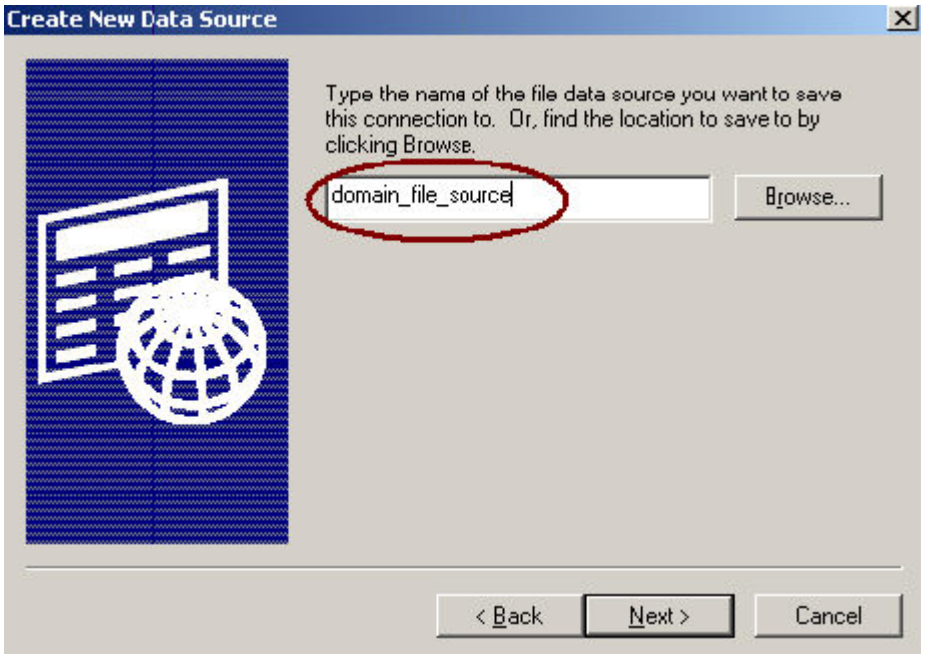


Figure 6-27 Create New Data Source

9. **Click** *Next to* see a summary window.

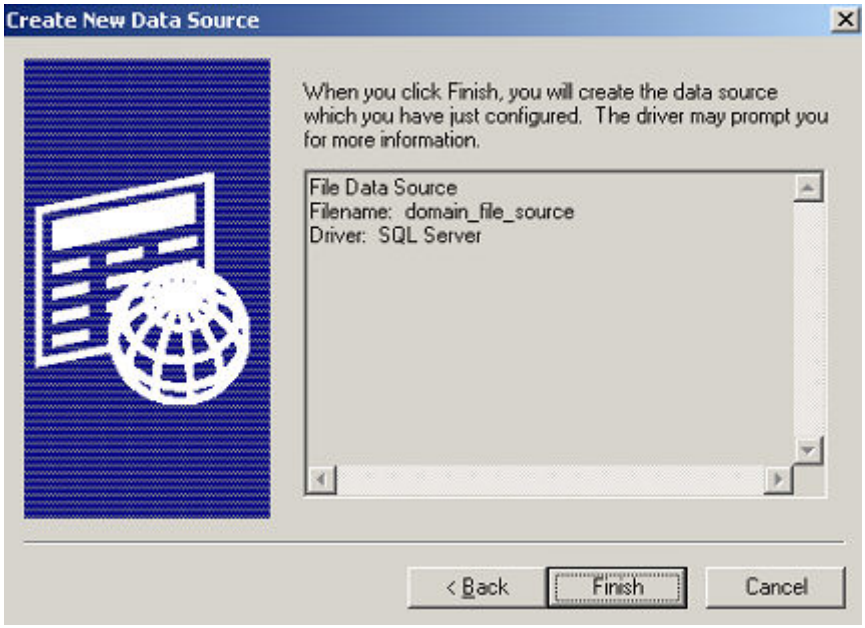


Figure 6-28 Create a New Data Source to SQL Server Window

10. If the information is correct **click** *Finish The Create a New Data Source to SQL Server* window opens. Otherwise **click** *Back*.

11. Using the *Server field pull-down*, **select** the SQL Server you wish to connect with. This may take a second while the computer looks for available SQL Servers. In the example below we have selected the DREAR server.

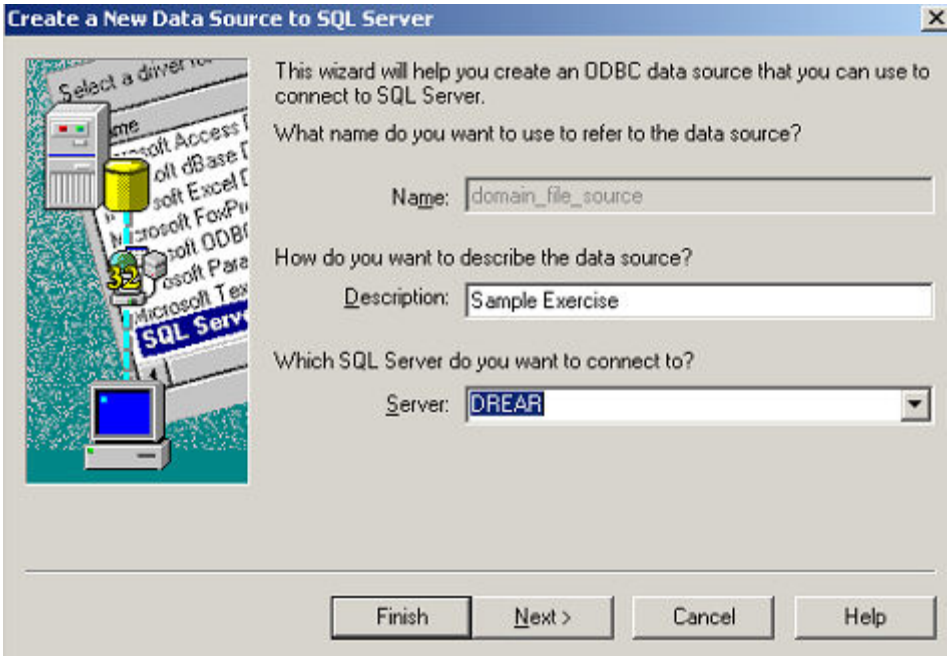


Figure 6-29 New Data Source to SQL Server

12. To **access** the SQL Server, you will be prompted for authentication, **enter** the login ID and password of the SQL Server you are connecting to.

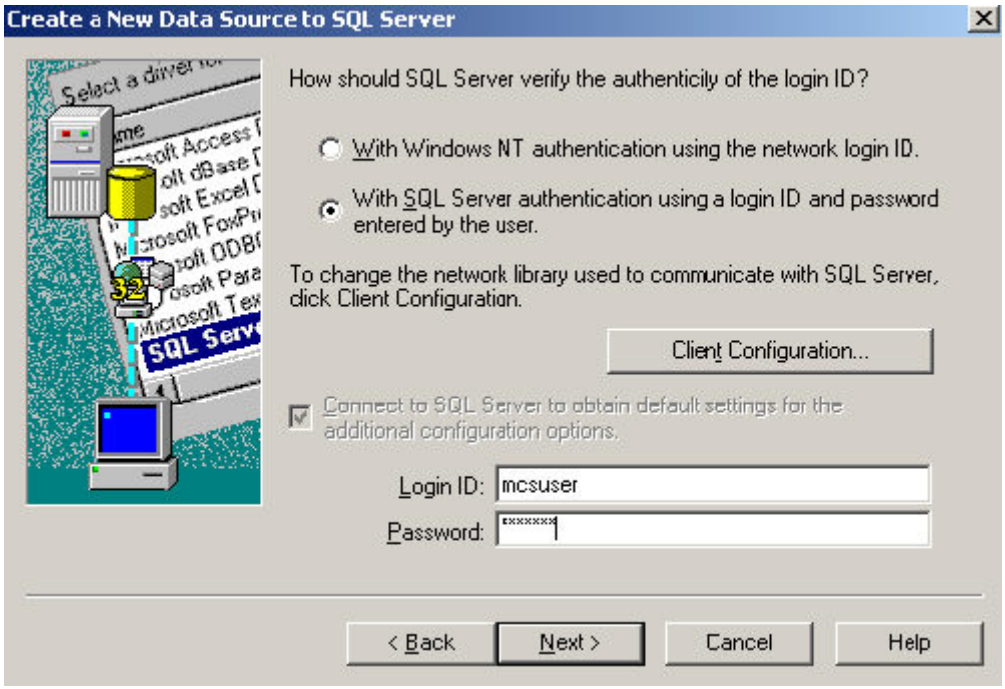


Figure 6-30 SQL Server Authentication Login ID and Password

13. The *Create a New Data Source to SQL Server* window is displayed.

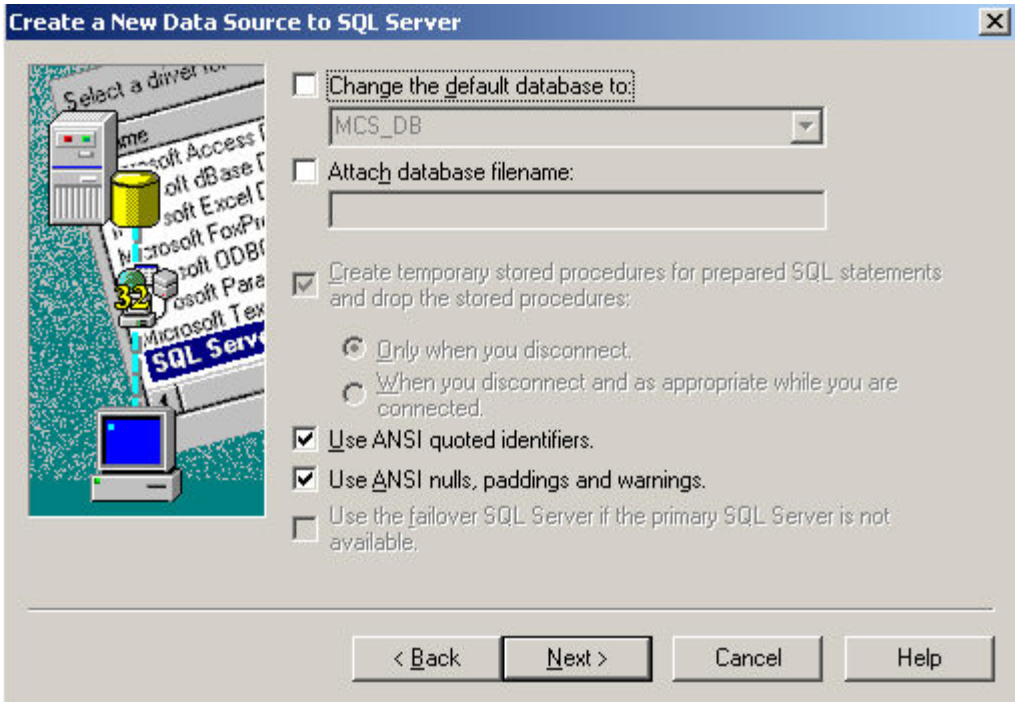


Figure 6-31 New Data Source to SQL Server ANSI parameters

14. **Click** *Next* to continue creating a new data source to the SQL Server, the following window is displayed.

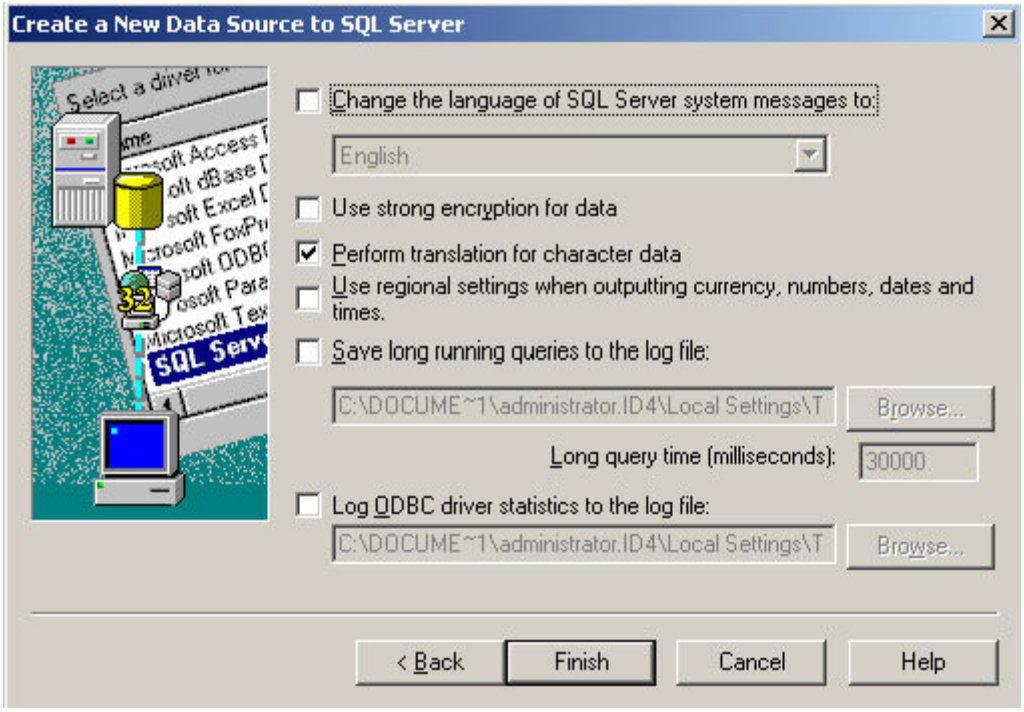


Figure 6-32 New Data Source to SQL Server translation parameters

15. **Click** *Finish*. A summary window appears. **Click** *OK*

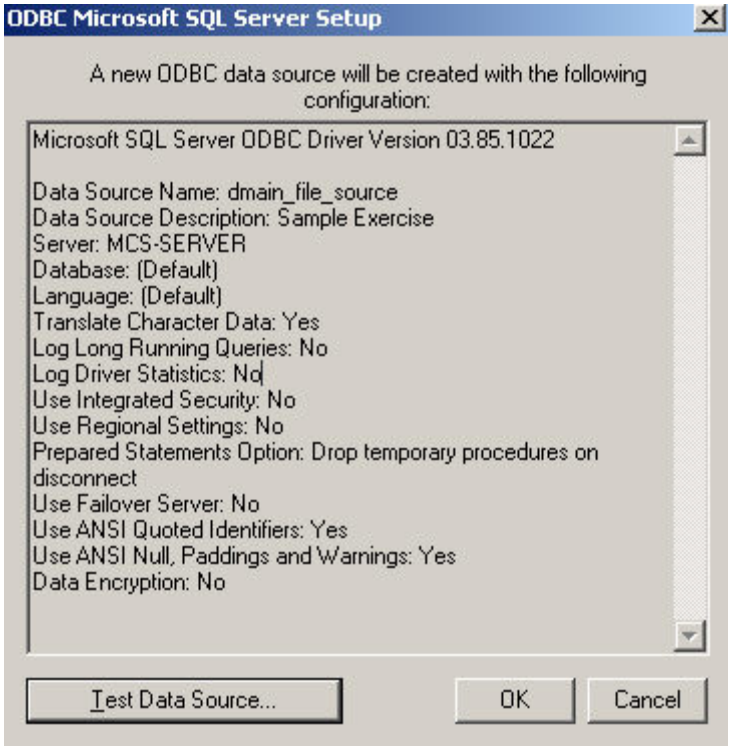


Figure 6-33 ODBC Microsoft SQL Server Setup Window - Summary

16. From the *ODBC Microsoft SQL Server Setup* window **click** the *Test Data Source* button. The test results are displayed.

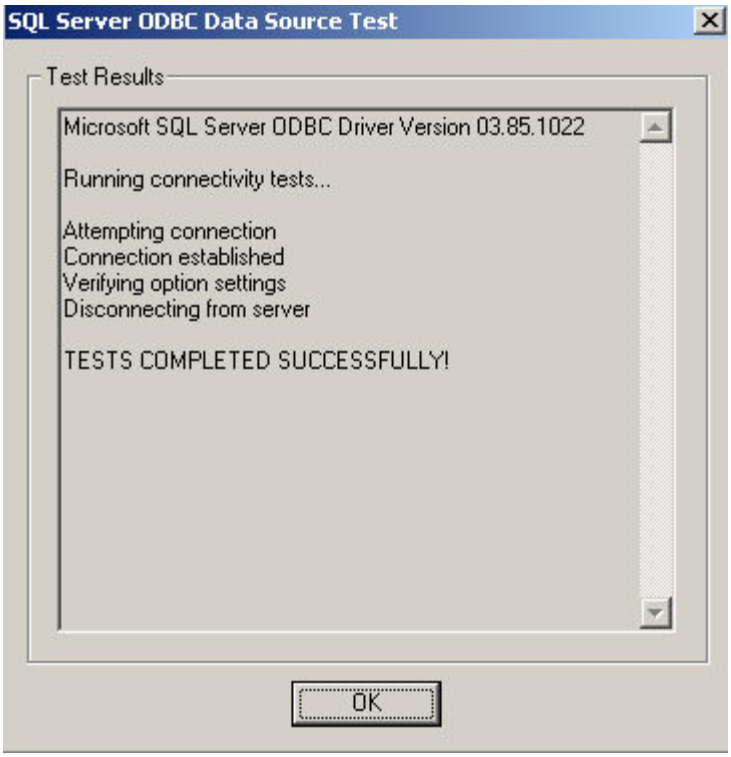


Figure 6-34 SQL Server ODBC Data Source Test results

17. **Click** the *OK* button to close the *Data Source Test* window.
18. **Click** the *OK* button to close the *SQL Server Setup* window.

6-2.4 Startup MDR

1. In Windows Explore, **navigate** to the MDR folder in the MCS Installation directory.
2. **Double-click** the *MDR.exe* to start the MDR. The *Message Data Replicator* window opens. MDR establishes a connection to an Outlook email account on the local machine.

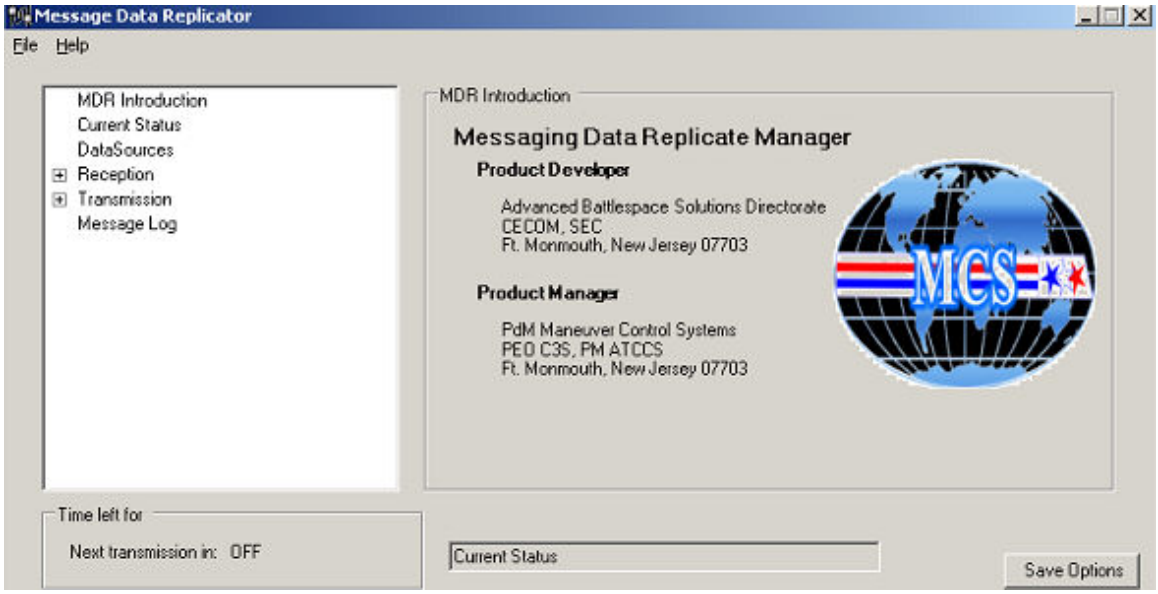


Figure 6-35 Message Data Replicator Window

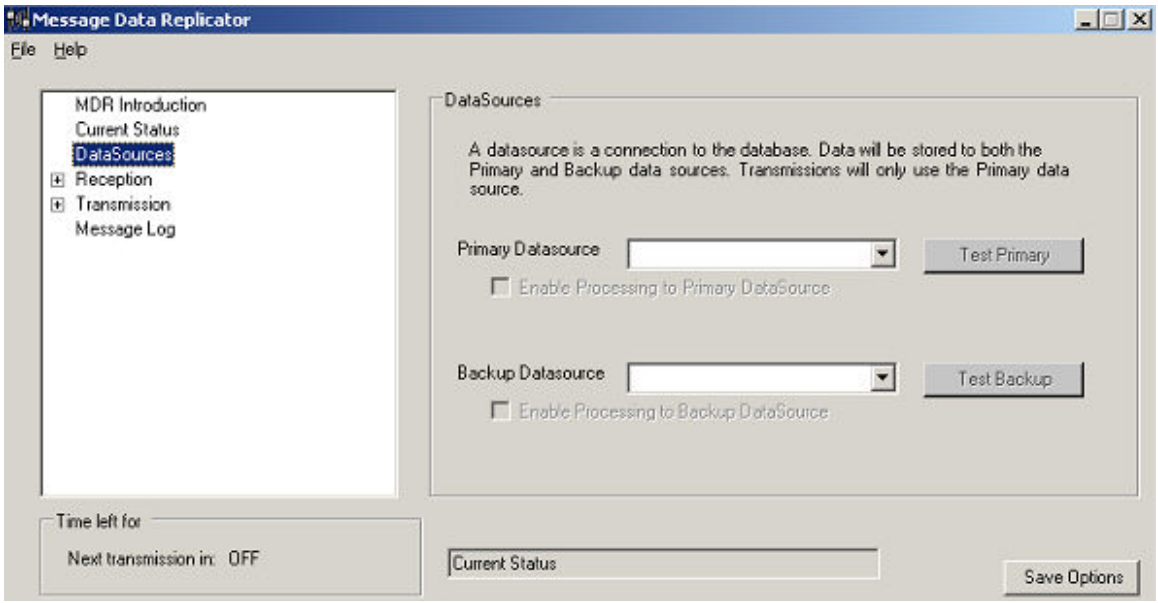


Figure 6-36 Message Data Replicator Window - DataSources Selected

3. **Select** *DataSources* in the left pane.
4. In the *Primary Datasource* drop-down menu **select** the data source you want to use as your primary connection.
5. In the *Backup Datasource* drop-down menu **select** your backup data source.
6. **Click** the *Test Primary* button to verify that you have connection to your databases. If the button turns green, you have good database connectivity. If the button is red, there is no database connectivity.
7. **Click** the *Test Backup* button to verify that you have connection to your backup database.

6-2.5 MDR Reception Options

1. From the *Message Data Replicator* window, **select** *Reception.*
2. In the *Reception* area of the window, **select** the *Process incoming emails* option.

NOTE

If you want to delete emails after they are processed, select the Delete emails after processing check box.

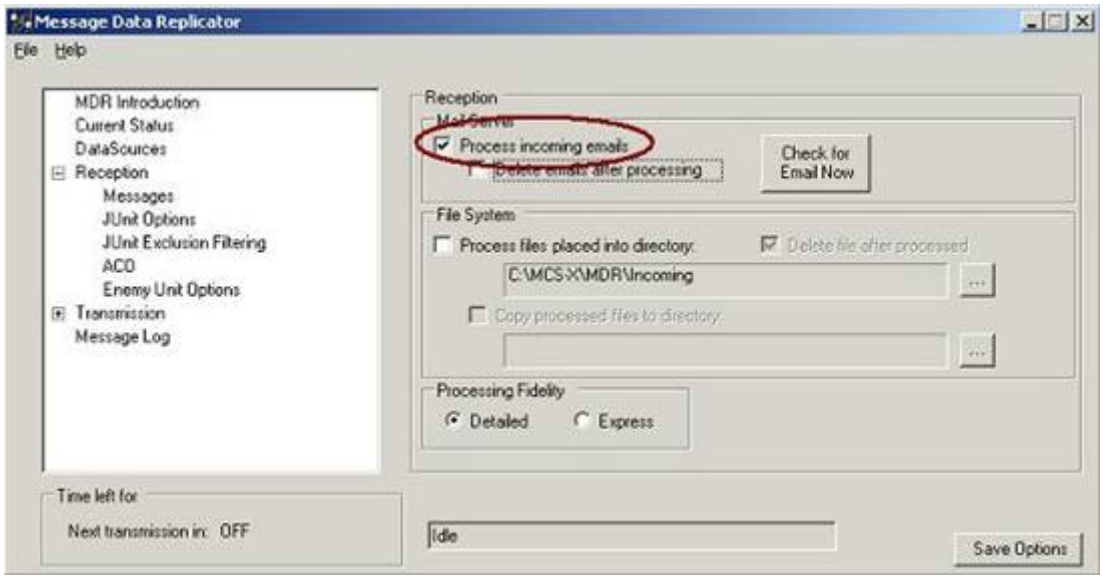


Figure 6-37 Reception Item - Process Incoming Emails Selected

3. Under *Reception*, **select** *Messages.*

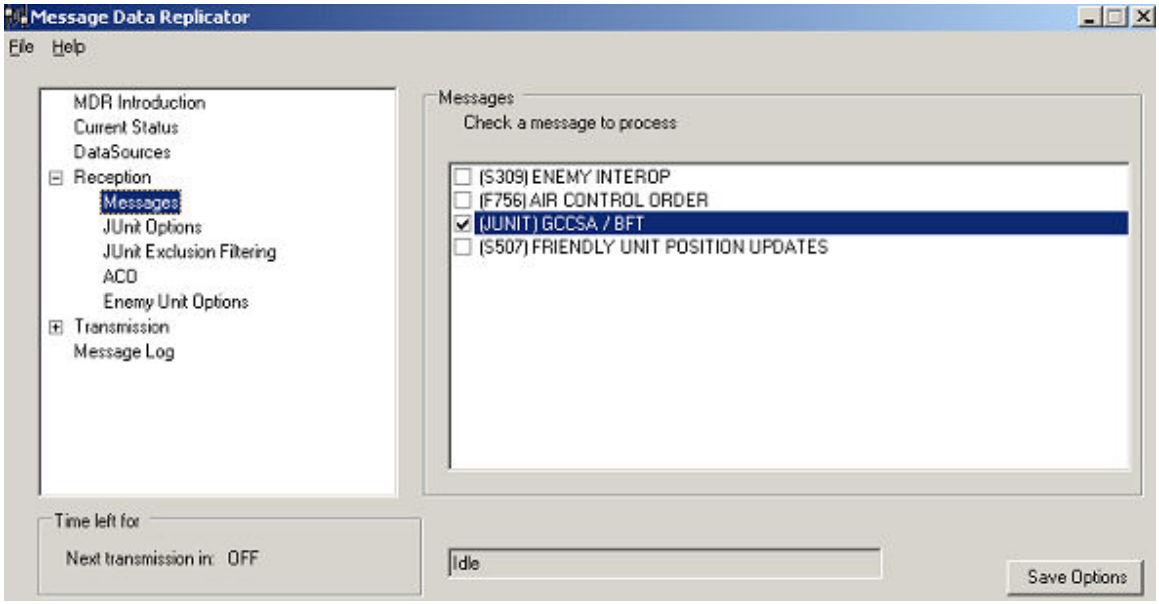


Figure 6-38 Message Data Replicator window - Messages to Process Selected

4. **Select** the check marks for the types of messages that you want to process.

5. Under *Reception,* **input** the required information for *Junit Options, Junit Exclusion Filtering,* and *ACO.*

6. Under *Reception*, **select** *Enemy Unit Options.*

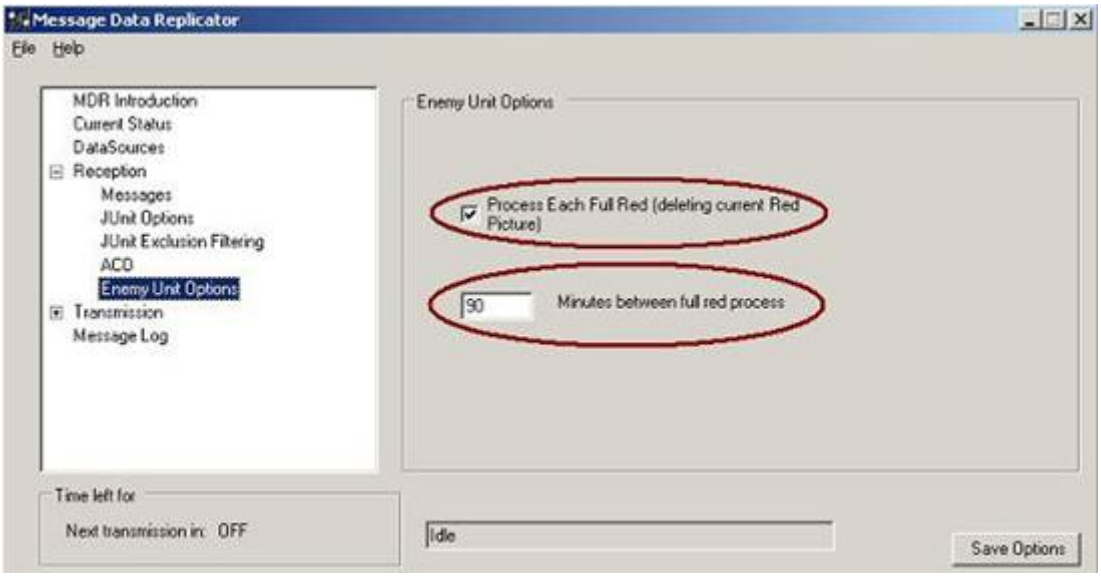


Figure 6-39 Message Data Replicator Window - Enemy Unit Options Selected

7. The *Process Each Full Red* check box will delete the old red picture prior to a new S309 message being processed. **Adjust** the variable for time between full red pictures.

6-2.6 MDR Transmission Options

6-2.6.1 Filter Addressing Option

1. Under *Transmission*, **select** *Filter Addressing*.

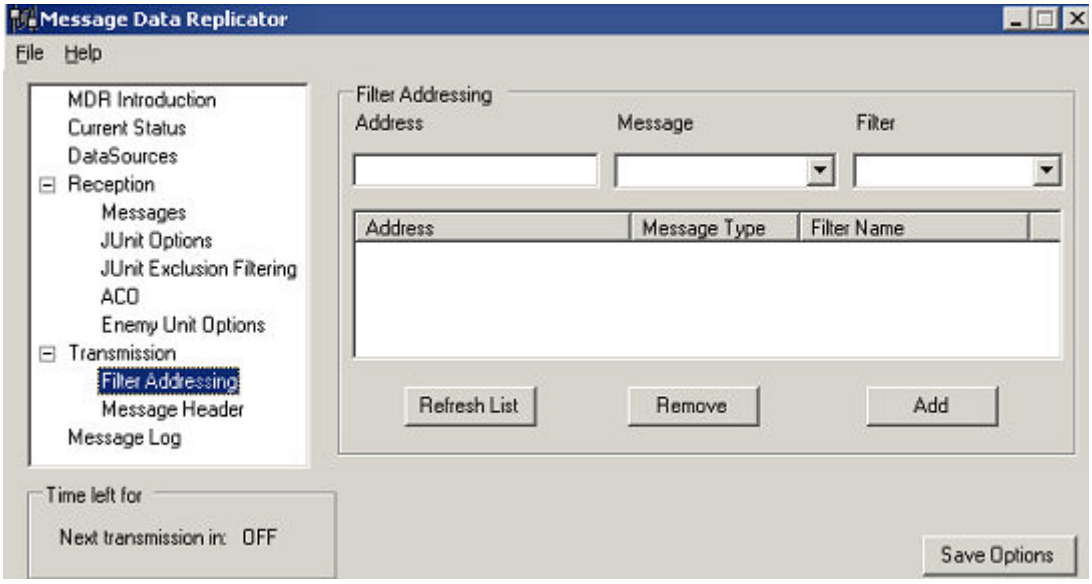


Figure 6-40 Message Data Replicator Window - Transmission Filter Addressing Selected

Add an Address

1. For each Addressee, **enter** the email address, **select** the message type, and **select** the filter if appropriate, then **click** *Add.*
2. **Repeat** for each addressee.
3. **Click** *Save Options* to save the settings.

Refresh Address List

1. **Click** *Refresh List* button. Address list refreshes with latest changes.

Remove an Address

1. **Select** the address and then **click** *Remove*.
2. **Repeat** for each addressee.
3. **Click** *Save Options* to save the settings.

6-2.7 Message Header Option

1. Under *Transmission*, **select** *Message Header.* **Add** your required information.

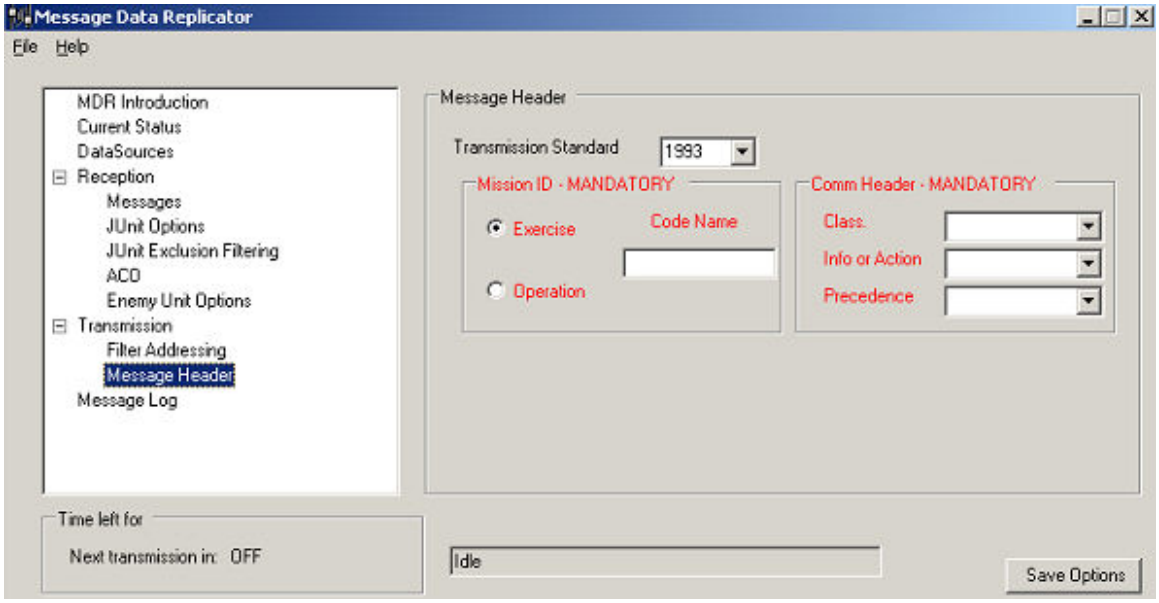


Figure 6-41 Message Data Replicator Window - Transmission Message Header Option Selected

2. **Select** either *Transmission Standard USMTF 1993, 2000,* or *2004*.
3. If real units are being used, **set** the *Mission ID* to *Operation*. If this is only an exercise **set** this to *Exercise.*
4. **Select** a classification from the *Class* drop down, **select** *Information* or *Action* from the *Info or Action* drop- down, and **select** either *Routine, Immediate, Priority,* or *Flash* from the *Precedence* drop-down.
5. **Click** the *Save Options* button to commit changes.
6. **Close** the *Message Data Replicator* window. MDR is now configured and started.

6-3 Database Management Utility

6-3.1 Introduction to Database Management Utility Tool

The Database Management Utility tool is used to help assist the System Administrator in performing database maintenance, setting up replication, synchronizing servers, and viewing the replication status.

6-3.2 Replicator Environmental Checklist

The following SQL Server Replicator environmental checklist of information should be verified before starting the Database Management Utility:

1. **Verify** *Hostname Resolution*.

   Verify that each server participating in replication can ping the other servers using the servers hostname. If a server cannot be pinged by host name, then the server is not registered with the Exchange Server. If you are unable to register, then you will need to hard code the hostname and IP in the …/etc/hosts file

2. **Verify** *Server Date/Time.*

   Verify all the servers participating in replication are in the same time zone and are set to the same time

3. **Verify** *SQL server Timeout Setting*.

   The following needs to be modified to allow SQL server time to connect to other servers. If the network connection is slow, SQL Server will timeout thinking the server is not reachable. The following steps will change the timeout setting and waits until a connection has been established:

   a. **Open** *SQL Server Enterprise Manager.*
   b. **Click** on *SQL Server Group* to highlight.
   c. **Click** on *Options.*
   d. In the SQL Server Enterprise Manager Properties window, **click** the *Advanced* Tab.
   e. Under Connection Settings, **change** the *Login time-out = 60*
   f. **Click** *OK* to close the window.

4. **Verify** *SQL Server Processes Running* as Administrator.

   For replication to function correctly, the following SQL server processes need to be modified to run using the Admin account. The following are the steps to make that modification:

   a. **Open** services: *Start, Programs, Administrative Tools, Services*.
   b. **Right-click** on *MSSQLSERVER* process and **chose** *Properties.*
   c. **Click** on the *Log On* tab.
   d. **Choose** *This account.*
   e. **Click** the *Browse* button.
   f. **Click** on the *Administrator User* and **click** *OK.*
   g. In the MSSQLSERVER Properties window, **Enter** the *Password/Confirm Password* for the Admin.
   h. **Click** *OK* to close the window.

i. **Repeat** the above steps for the *SQLSERVERAGENT* process as well.

j. **Right-click** the *SQLSERVERAGENT* process and choose *stop.*

k. **Right-click** the *MSSQLSERVET* process and **choose** *restart.*

l. **Right-click** the *SQLSERVERAGENT* process and **choose** *start.*

5. **Register** *SQL Server* as the hostname

Verify that the registration for the database server is not registered as local. Replication will not work if the server is not registered as the host name of the server where the database resides. If it is defined as local remove the registration and reregister as the server name:

Remove the local Server Registration:

a. **Right-click** on the *local* server and **choose** *Delete SQL Server Registration*.

b. **Click** *Yes* for *are you sure.*

Register a Server:

a. **Right-click** on *SQL Server Group*.

b. **Click** on *New SQL Server Registration.*

c. **Click** *Next*.

d. Under Available Servers, **type** the *host name* of the server you want to register and click *Add.*

e. **Click** *Next*.

f. **Choose** *SQL Server Login information.* and **click** *Next*.

g. **Enter** the login / password (*mcsuser/mcsuser*) and **click** *Next*.

h. **Click** *Next* in the *Select SQL Server Group window*.

i. **Click** *Finish*.

j. **Click** *Close* to close the screen.

6. **Verify** Database Registration Name.

Verify within the database that the server name matches the host name for the server. This will cause problems with replication if they are different. The following steps will verify:

Verify SQL server Database Server name:

a. **Open** SQL Server *Query Analyzer* (*Start, Programs, Microsoft SQL Server, Query Analyzer)*.

b. In the *Connect to SQL Server* window:

- **Choose** your server from the dropdown list of database servers.
- **Choose** SQL Server authentication and enter the username/ password.
- **Click** *OK*

i. In the window **type** the following and then **press** F5:\. Select @@servername.

ii. If the name returned is the same name as the hostname of the server, then you are good to go.

iii. If the name returned does NOT match the hostname, then you will need to change the SQL server database server name.

Delete the SQL server Database Server name:

a. In the window **type** the following, **press** F5 and write down the server name: *select @@servername*.

b. **Clear** the above statement from the window, **type** the following and **press** F5. sp_dropserver 'the-db-server-name-from-above'

c. **Stop** and **start** the database

d. **Clear** the above statement from the window, **type** the following and **press** F5: *select @@servername*

e. If the database server name is NULL, then continue to add the correct database server name.

If it is still not NULL, then do the above again.

Add the SQL server Database Server name:

a. **Clear** the above *statement* from the window, **type** the following, and **press** *F5 sp_addserver 'the-host-name-of-the-server', LOCAL*

b. **Stop** and **Start** the *Database/Agent*.

c. **Clear** the above *statement* from the window, **type** the following and **press** *F5 select @@servername*

d. If the database server name is the same name as your host name, you are good to go. If the database server name is still NULL, then **do** the above again.

7. **Register** all SQL Servers to Participate in Replication.

On the servers that will be participating in replication, you need to register all the servers that will participate in replication. The following are the steps register servers within the database:

a. **Right-click** on *SQL Server Group*.

b. **Click** on *New SQL Server Registration.*

c. **Click** *Next*.

d. Under Available Servers, **type** the *host name* of the server you want to register and **click** *Add*. Keep adding until all the servers that will participate in replication are added.

e. **Click** *Next*.

f. **Choose** *SQL Server Login information* and **click** *Next*.

g. **Enter** the login / password and **click** *Next*.

h. **Click** *Next* in the *Select SQL Server Group* window.

i. **Click** *Finish*.

j. **Click** *Close* to close the screen.

6-3.3 Starting the Database Management Utility

1. **Select** *Start*, *Programs*, *MCS*, *Administration*, *Database Management*. The *Database Management Utility* is displayed.

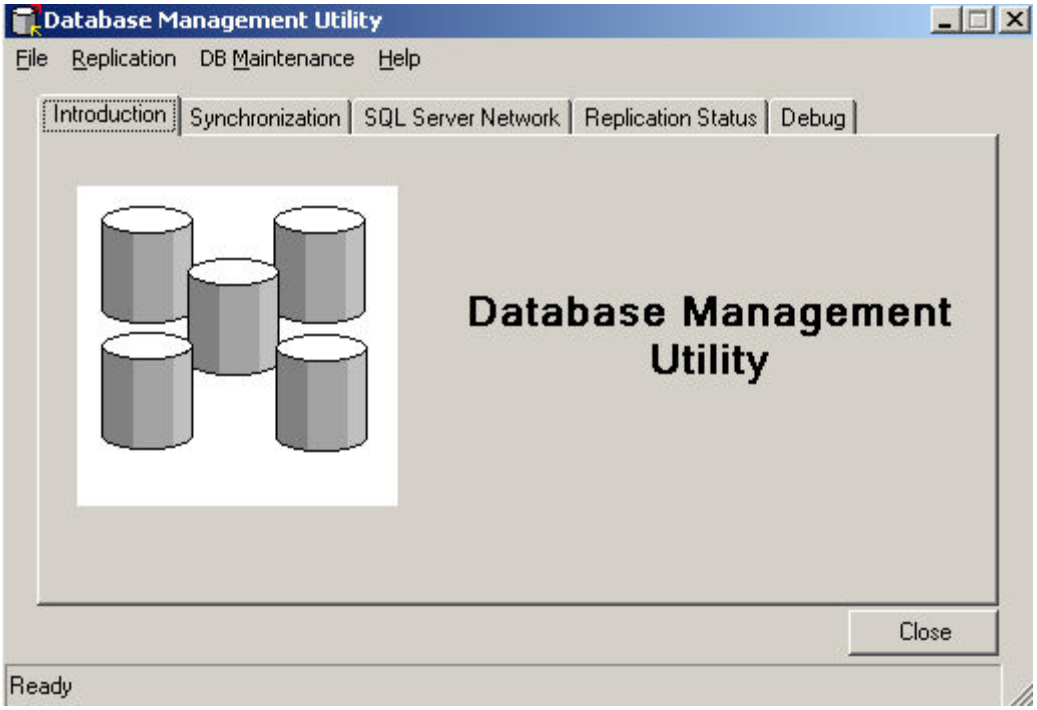


Figure 6-42 Database Management Utility

6-3.4 File Menu Item

The File menu item gives the user information about the database servers and access to the Replication log files. There are two main log files associated with the Database Replication; DB Maintenance Error Log and the DTS Log. The DB Maintenance Error Log displays the error messages that are generated by the Database Management Utility. The DTS Log shows information about the data that is transferred each time Replication is run.

1. **Click** the *File* option in the *Database Management Utility* window, the drop down list of available options is displayed.
2. **Click** the *Open Log* option to view the available logs.

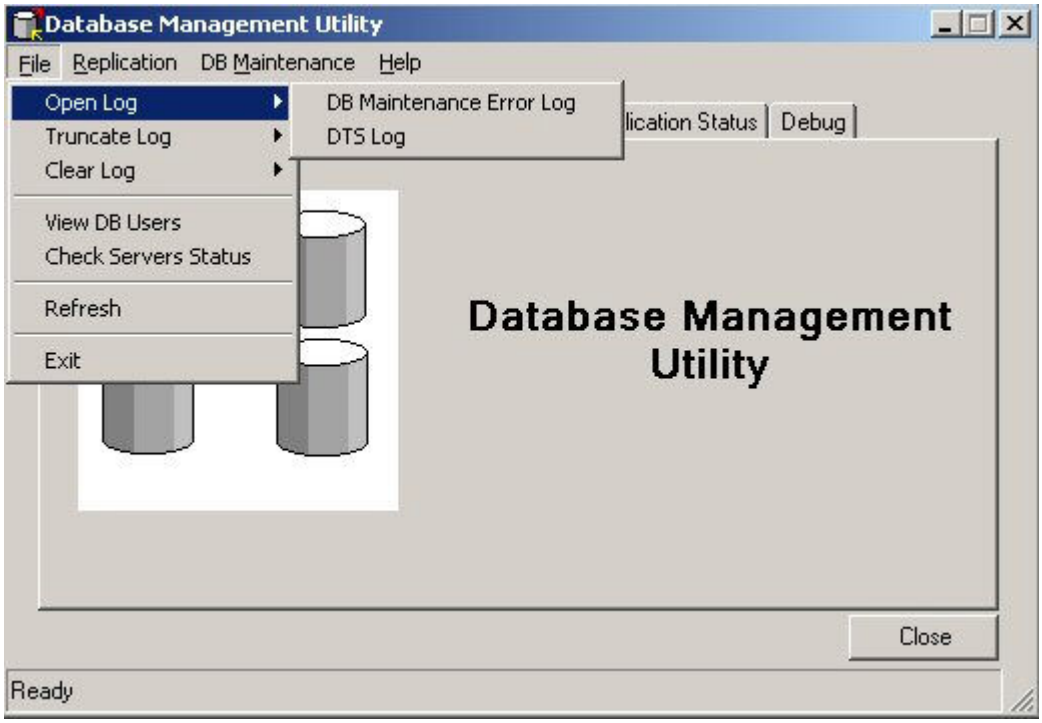


Figure 6-43 Database Management Utility Logs

6-3.4.1 Open Log Files

The user has the option to view either the DB Maintenance Error Log File or the DTS Log File by **selecting** *Open Log*.

6-3.4.2 Truncate Log Files

Over time, the DB Maintenance Error Log File or the DTS Log files will grow in size. Truncate Log will reduce the size of the logs to 1 megabyte leaving the latest information in the file.

6-3.4.3 Clear Log Files

By **selecting** *Clear Log*, the user will be able to delete all the information in either the DB Maintenance Error Log File or the DTS Log File.

6-3.4.4 View DB Users

Information about the database users can be seen by **selecting**, *View DB Users*. The *User Form* is displayed.

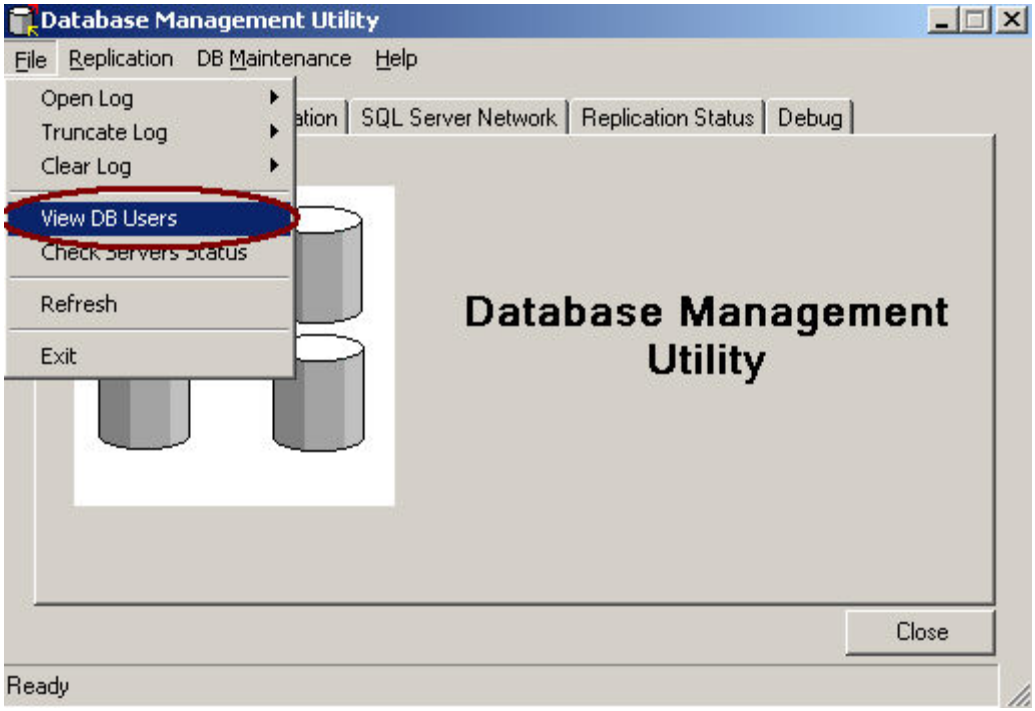


Figure 6-44 Database Management Utility Window - View DB USers Selected

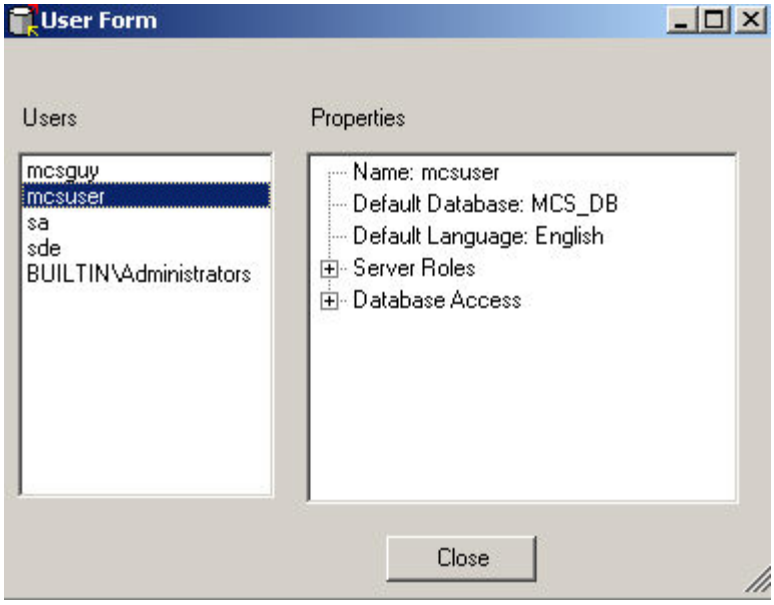


Figure 6-45 User Form

6-3.4.5 Check Server Status

There are a number of parameters that need to be configured for Database Replication. The user can view some of the server parameters prior to setting up Replication from Check Server Status. From the *File* button in the menu bar, select *Check Servers Status.* **Select** a *server* that will be the Publisher and check the boxes for the servers that will be Subscribers. When the user **clicks** on the *Get SQL Server Status* button, information on the server settings will be returned. The information will allow the user to determine if the servers are able to participate in Replication.

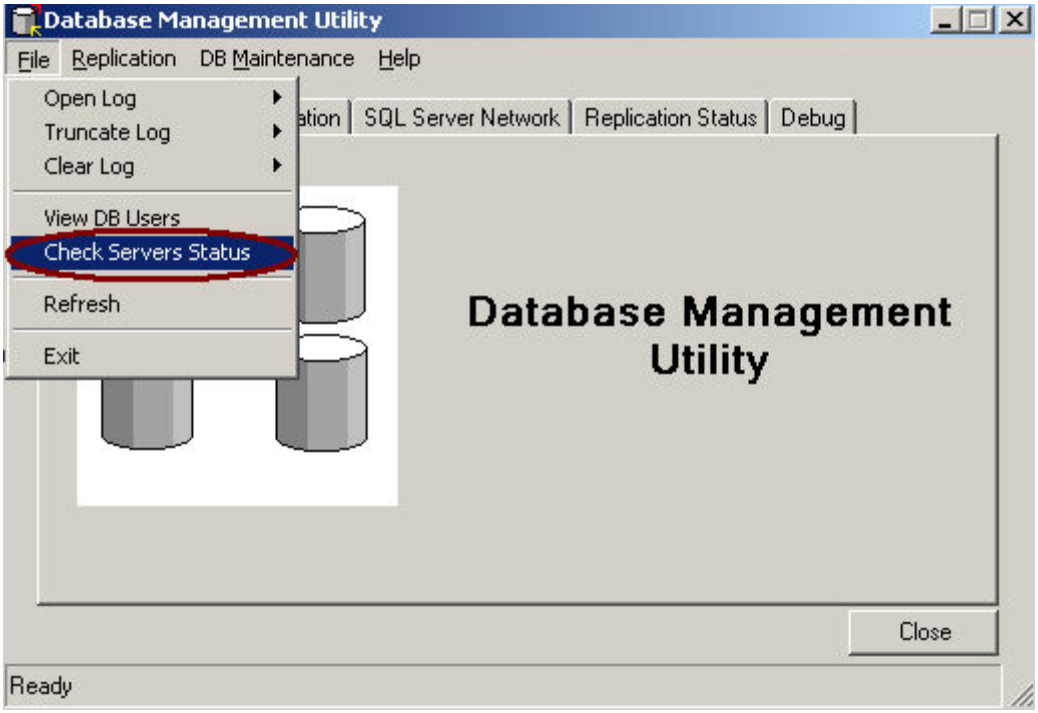


Figure 6-46 File Drop-Down Menu - Check Servers Status Selected

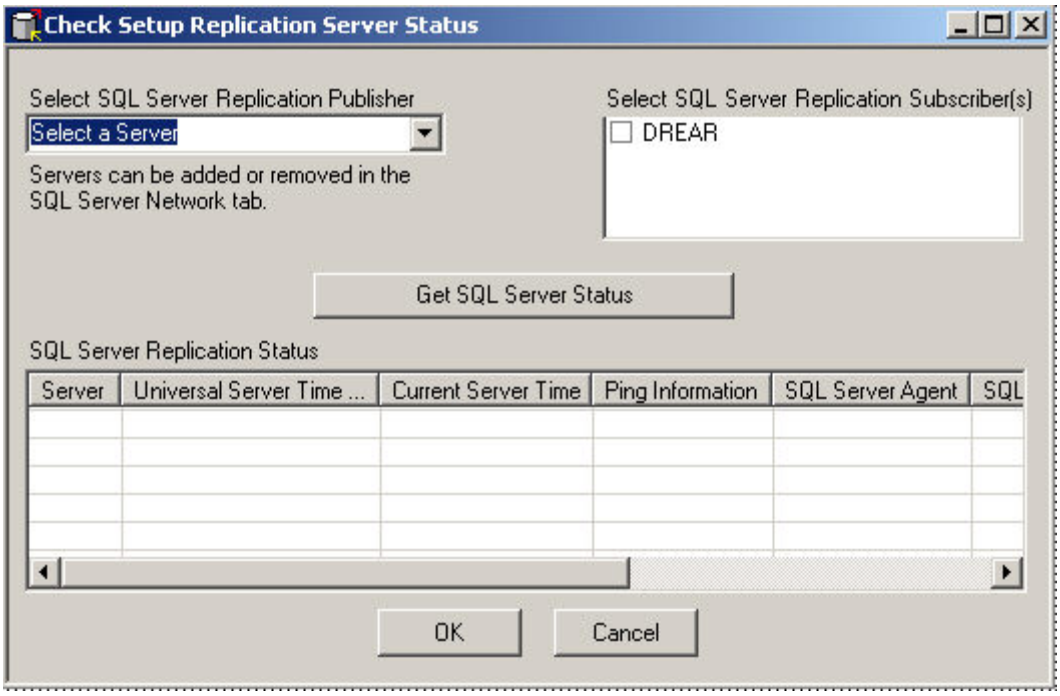


Figure 6-47 Check Setup Replication Server Status

The following information will be returned as a result of **pressing** the *Get SQL Server Status* button.

Server: The name of the server

Universal Server Time (UTC): The time in GMT. All the servers should have the same UTC time. If not exact, they should be very close.
Current Server Time: The server time in the time zone that is set in Date and Time Properties. The date-time should all be the same or close for all servers in Replication.
Ping Information: This returns information about a ping from the Publisher to each Subscriber. All packets that are sent should be received and the average time should not be more than a couple of seconds.
SQL Server Agent : Returns if the SQL Server Agent is running. This needs to be running for Replication to function. It can be started remotely with the SQL Server Service Manager.
SQL Server Name: Returns the SQL Server servername. The name must be the same as the Server name. It cannot be "Local" or greater than 14 characters.
Version of SQL Server: Returns the version of SQL Server on each server.
MCSSQLSERVER & SQLSERVERAGENT: This returns the owner of these two processes. The owner must have server administrator privileges.

MCSUSER Exists: This will check and see if the user MCSUSER exists in the MCS database and it will return the name of the MCS database.

6-3.5 Replication Menu

The Replication menu allows the user to configure, modify, remove and manage Replication.

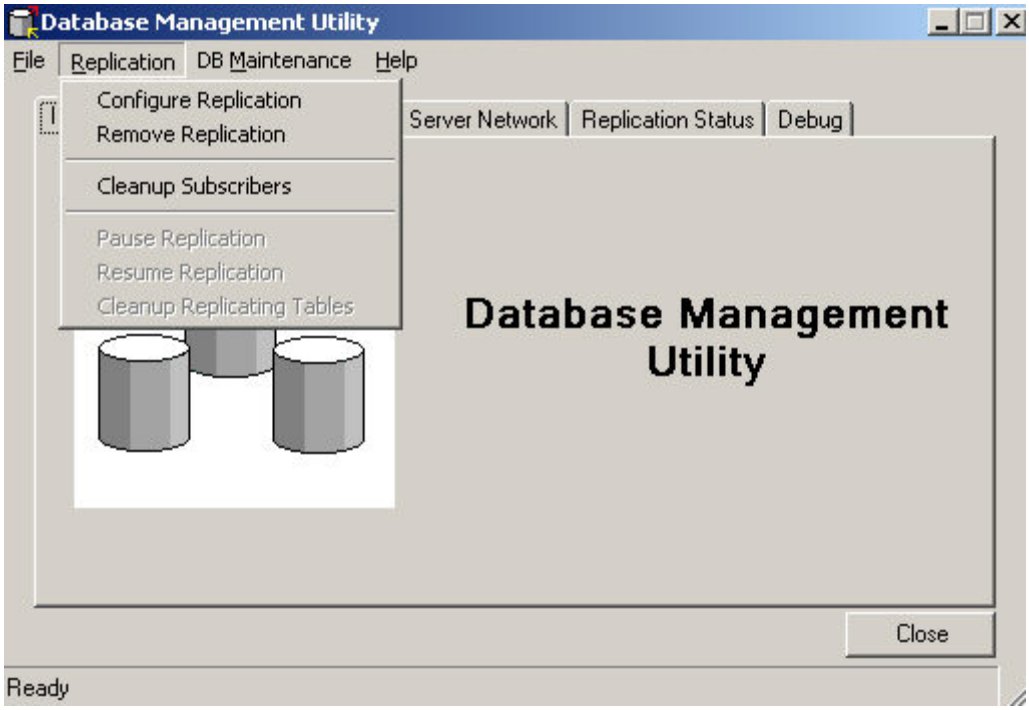


Figure 6-48 Replication Menu Item

6-3.5.1 Configure Replication

This allows the user to setup or change Database Replication. The user will **select** a *server* to be the Publisher and then **select** the other *servers* that will be participating in Replication as Subscribers. The time interval that Replication runs is then set. Any data changes made to the

publishing server will be sent to the subscribing servers when Replication runs. Changes made to the data in the database on a subscriber will be sent to the publisher when Replication runs and when Replication runs again the changes will be sent to the other subscribers. See the Select Publishers & Subscribers window.

Figure 6-49 Select Publishers & Subscribers

6-3.5.2 Remove Replication

To stop Replication **select** *Remove* Replication. This will stop Replication by removing all the Replication processes on all the servers that are configured for Replication. This should be done before the network between the serves is disconnected or servers go offline.

6-3.5.3 Cleanup Subscribers

If a server is having trouble connecting to the Subscribers through the Replication subscriptions, there may be a problem with the subscriptions. Cleanup Subscribers will remove the subscription and redefine the Subscribers subscriptions. Once this has been completed, Replication should function normally.

6-3.5.4 Pause Replication:

If the network bandwidth is needed for another reason, and the user would like to temporarily suspend the flow of replicated data over the network, **select** *Pause Replication*. This will queue up all the database changes on each of the servers. When Replication is resumed, the data will be replicated to the other servers defined in Replication.

6-3.5.5 Resume Replication

This will resume database Replication and all changes that were queued up in the database while Replication was paused will be replicated to the other servers defined in Replication.

6-3.5.6 Clean Up Replicating Tables

This will remove all unneeded data from the Replication tables to improve performance.

6-3.5.7 DB Maintenance Menu

The DB Maintenance menu item gives the user the ability to perform some basic database tasks.

1. **Click** the *DB Maintenance* item in the Menu Bar, the drop down menu appears.

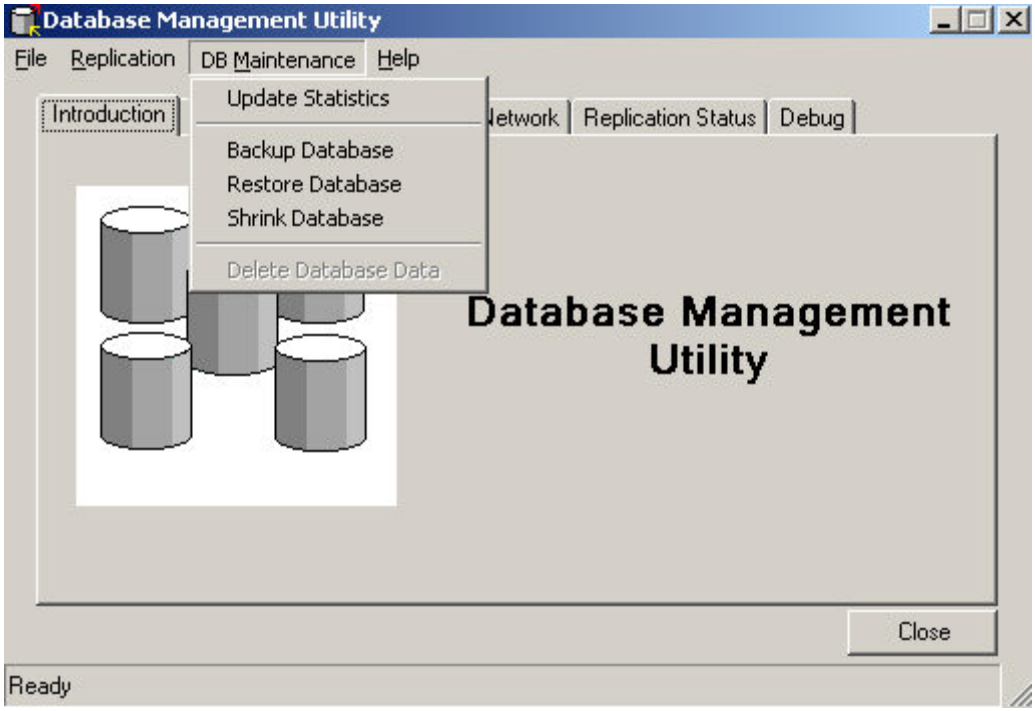


Figure 6-50 DB Maintenance Drop Down Menu list

6-3.5.8 Update Statistics

The Database Management System (DBMS) keeps statistics about the data in the database tables. It uses these statistics to determine the best way to run a query to maximize performance. Over time, as data is added and deleted, the statistics may become obsolete. This may slow the performance of the database. When Update Statistics is selected, this information is updated to reflect the current data in the database. It is recommended that Update Statistics is run periodically. This will keep this information current and should improve performance.

6-3.5.9 Backup Database

If the user wants to save a copy of the database on the server he can select Backup Database. It will save the database to a file that can be restored on this server or another server.

NOTE

The user should not back up a database that is involved in Replication. A database involved in Replication is altered for Replication and may not function properly when restored.

6-3.5.10 Restore Database

If the user has a backup copy of a database, **selecting** *Restore Database* will restore it.

NOTE

A database involved in Replication cannot be restored. Remove that server from Replication prior to restoring the database.

6-3.5.11 Shrink Database

All transactions made against the database are logged in the database. This information is used to restore the database from a catastrophic failure. This logging takes up hard drive space and is not automatically returned to the operating system when the data is no longer needed. The user can return this space to the operating system by selecting Shrink Database.

NOTE

The user should backup the database prior to running Shrink Database since the transaction logs will be purged and data may be lost if there is a database failure.

6-3.6 Synchronizing Database Data Tab

The user can synchronize some of the MCS data between servers from the *Synchronize* tab.

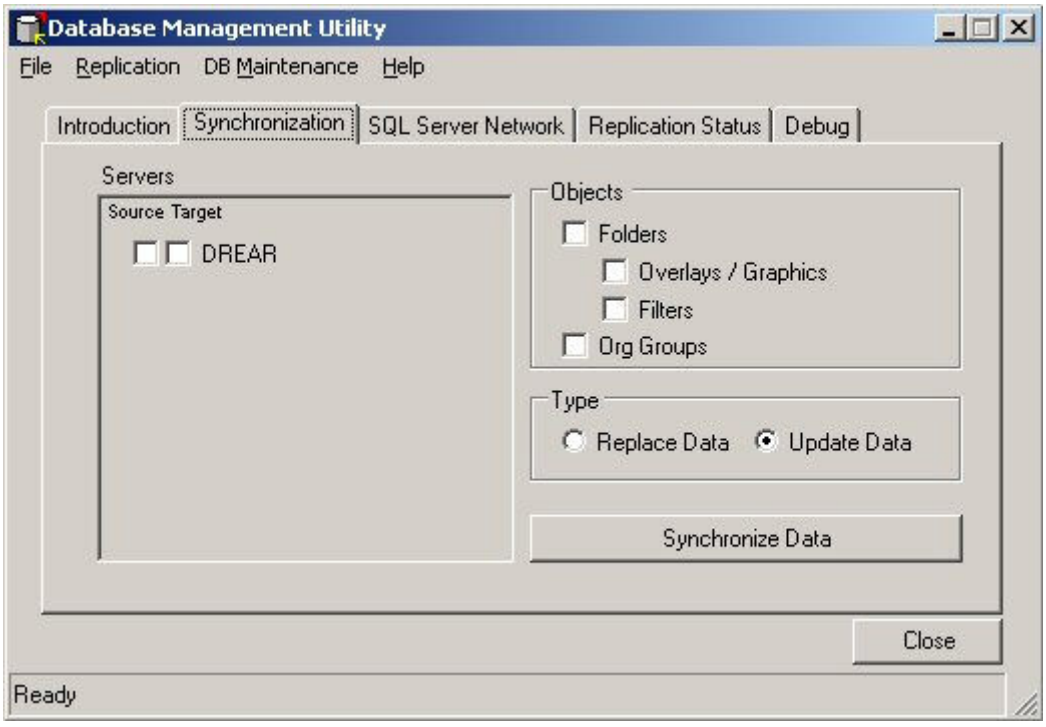


Figure 6-51 Synchronization Tab

6-3.6.1 Synchronizing data between 2 or more servers

1. **Select** the *servers*: In the Server pane, **select** which server is going to supply the data (Source) and which servers are going to receive the data (Target).
2. **Select** the *data*: In the Objects box, **select** the objects to synchronize.
3. **Select** the *synchronization type*: The user will then **select** the type of data transfer, Replace Data or Update Data.

- Replace Data: This will remove all existing data in the Target database(s) for the objects selected and then the data from the Source database will be inserted into the Target database(s).
- Update Data: If the user doesn't want to remove the existing data on the Target database(s), **select** *Update Data*. This will insert any new data and update the existing data with the data from the Source database.

4. **Click** the *Synchronize Button*: When the user has completed choosing the options, **click** the *Synchronize Data* button. A popup progress window will show the progress of the synchronization and let the user know when synchronization has completed.

6-3.7 The SQL Server Network Tab

The network of servers that can participate in Database Replication or data synchronization, are identified here. The user can also setup the server to check connectivity to the other servers that are involved in Replication.

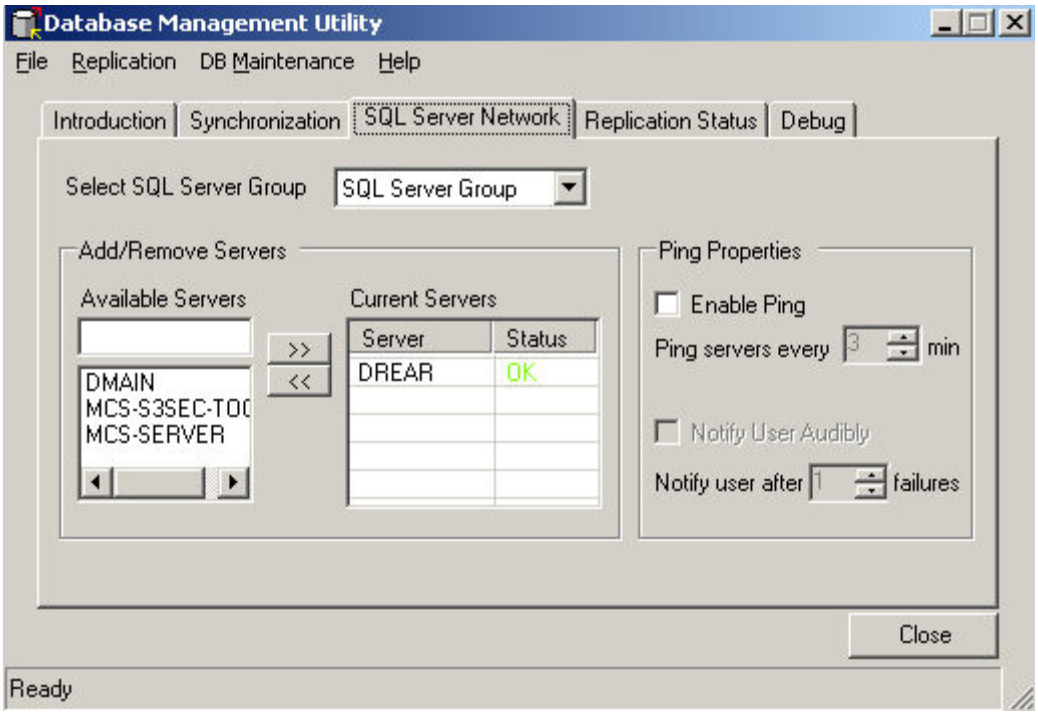


Figure 6-52 SQL Server Network Tab

6-3.7.1 Network of Current Servers

Only the servers listed in the Current Servers list can be included in Replication. The user can add a server by either typing the name in the Available Servers box or selecting one from the list then clicking the add button (">>"). To remove a server, select it in the Current Servers list and click the remove button ("<<").

6-3.7.2 Ping Properties

The user can be notified that the server has lost connectivity to other servers. If the Enable Ping box is checked, the application will check if the servers in Replication can be reached over the network (i.e. ping-able). This will ping all the subscribers periodically. The user can set how often to ping the servers by setting the interval in the Ping Properties. In environments where there could be inconsistent radio communication links, the user may not be able to consistently ping the

other servers. They can set the, "Notify user after", setting so the user will not be notified until there are a number of consecutive failures. If a server comes back on line, the count will reset back to zero. If a server cannot be pinged, a window will pop up identifying the server that cannot be reached. If the Notify User Audibly is checked, then a voice will tell the user to check the network.

6-3.7.3 Database Replication Status Tab

The Replication Status tab displays information about the current Replication scheme and performance.

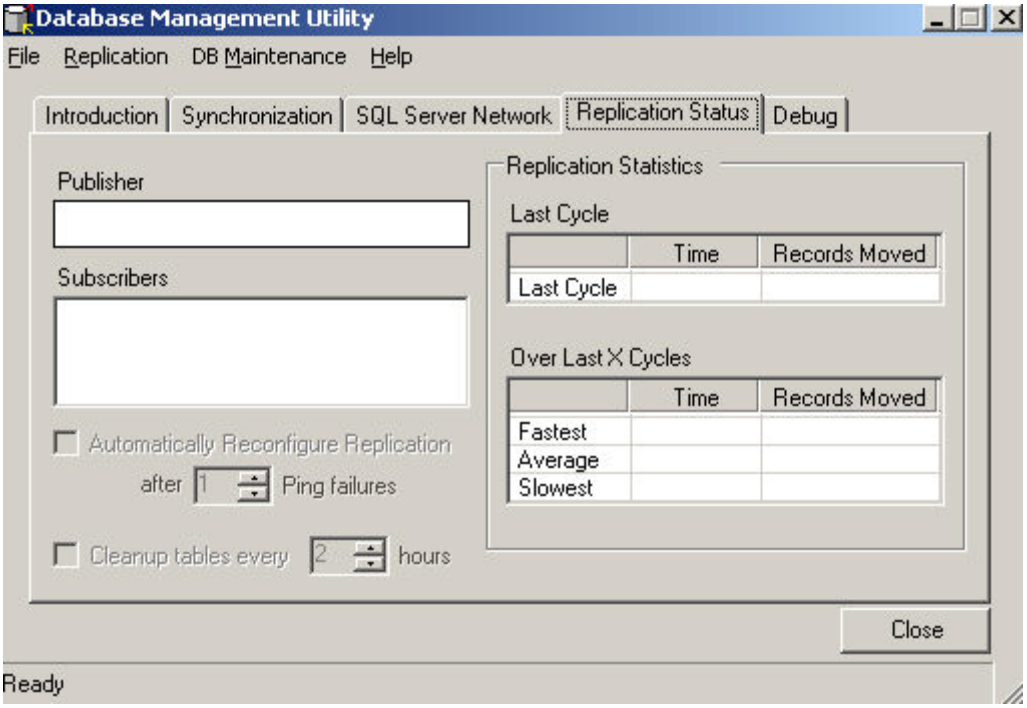


Figure 6-53 Database Replication Status Tab

6-3.7.4 Publishers & Subscribers

Displayed in the Publisher window is the server that is the Publisher in the Database Replication network. All the Subscriber servers are listed in the Subscriber window.

6-3.7.5 Replication Statistics

This information is provided to the user to show the Replication process time and how much data was replicated. This information will be helpful in determining the Replication interval time that is set in the Configure Replication item from Replication on the menu. The Replication interval time should be greater than the time it takes for Replication to run.

6-3.7.6 Automatically Reconfigure Replication

This functionality is currently not implemented.

6-3.7.7 Cleanup Unused Replication Table Data

This functionality is currently not implemented.

6-3.8 Debug Tab

The Debug tab displays any error and informational messages generated by database Replication.

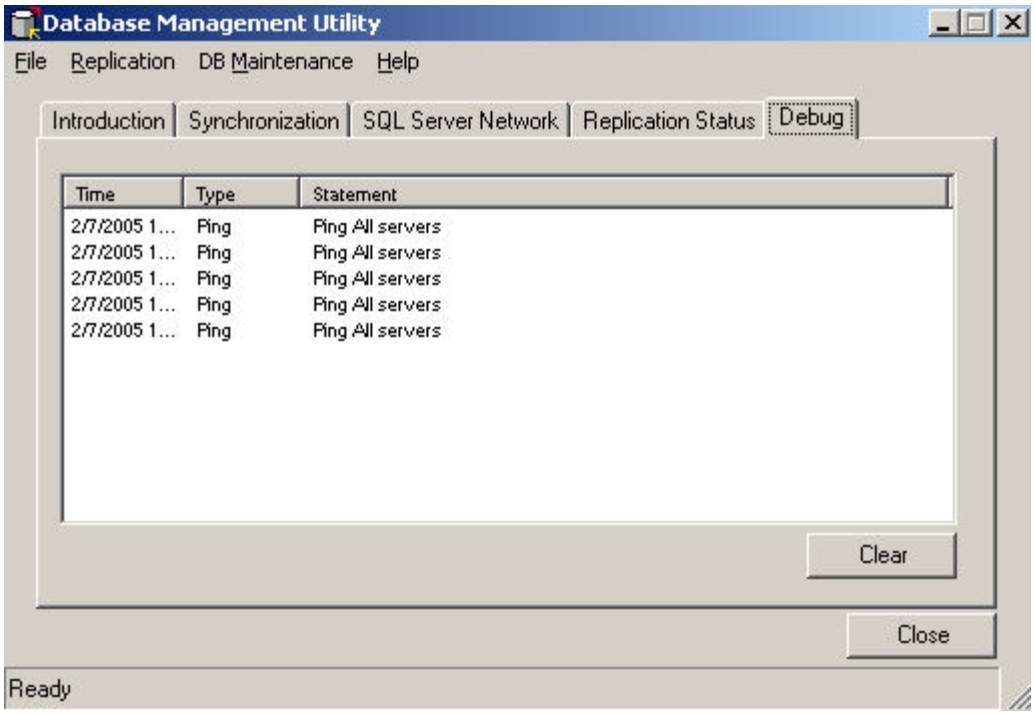


Figure 6-54 Debug Tab

6-3.8.1 Clear button

The Clear button will clear the display in the Debug Tab.

6-4 Configure Multilateral Interoperability Program (MIP)

MIP is located on Disk 2 of the MCS Installation CD's. You can launch the MIP installer directly from Disk 2. **Double click** the MPG.msi file located in the MIP folder of Disk 2. Follow the on screen instructions to complete the installation. To configure the MIP Server and Gateway, review the MIP_Installation.doc manual located on Disk 2 in the MIP folder.

To build a Multilateral Interoperability Protocol Server or Gateway, refer to the MIP Installation/configuration instructions, "Installing a Multilateral Interoperability Protocol (MIP) Server/Gateway". The MIP documentation is located in the MIP folder <drive letter>:\MCS\MIP once MIP has been installed.

6-5 Track Management System (TMS) Broker

6-5.1 Overview of Track Management System (TMS) Broker

NOTE

Before continuing verify that C2PC has been installed and configured. See the MCS Release Notes for C2PC installation instructions.

The TMS Broker provides an interface between the Near Real Time Server (NRTS) via the GCCS Data Provider and the Command and Control PC (C2PC) via the C2PC Gateway. The TMS Broker will send NRTS all tracks (Units, Platforms, Organic Links, and TBMS) it receives from the Gateway. Additionally, the TMS Broker will inject tracks (Units and Platforms) to the Gateway that it receives from NRTS. The data exchange between NRTS and the TMS Broker is based upon NRTS configuration settings (Administrator).

6-5.2 TMS Broker Menu Options

The TMS Broker does not require any user interaction to receive and inject tracks. The Broker is started automatically in the Windows tray.

Figure 6-55 TMS broker system tray icon

Hovering your mouse over the TMS Broker system tray icon will quickly display the status of the TMS Broker.

Figure 6-56 TMS Broker stopped

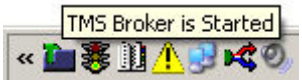


Figure 6-57 TMS Broker started

The user may **select** the following menu items via a **right-click** context menu.

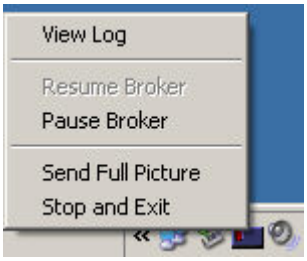


Figure 6-58 TMS Broker icon context menu

View Log
Displays logging information and the number of tracks updates and deletes received. The user may Reset the update (Upd) and Delete (Del) numbers via the Reset button. Additionally, the log may be Paused, Cleared and Closed via button selections. Closing the Log Window does not stop the TMS Broker from continuing to log information. It closes the log view from the user.

Pause Broker
Pauses the TMS Broker, preventing it from processing tracks from NRTS and/or C2PC Gateway.

Resume Broker
Resumes normal TMS Broker operation.

Send Full Picture
Forces the TMS Broker to send all C2PC tracks (via C2PC Gateway) to NRTS. This option should be used if the user believes NRTS and C2PC may have become out-of-sync due to LAN failure or similar. It is important to note that the full picture is automatically sent to NRTS whenever the GCCS Data Provider is started.

Stop and Exit
Stops the TMS Broker and Exits.

Manually starting the TMS Broker Application
The TMS Broker application is started automatically when the MCS Services Startup application is launched.

In the event a user exits the TMS Broker from the system tray icon; you will be required to **reboot** your system or manually **startup** the *TMS Broker.*

1. To **start** the *TMS Broker*, **locate** the application using the *Windows Explorer* window. The application is located in the following path:

   MCS-Installed-Directory\DataBrokers\TmsBroker\TMSBroker.exe

2. **Double-click** the *TMSBroker.exe* icon, the Login screen is displayed. **Starting** the *TMSBroker* will add the TMSBroker icon to the system tray. Additionally, the C2PC Gateway Login screen will be displayed.
3. **Select** the *Server* you need to connect with and **enter** the appropriate *password*. **Click** *OK* to connect to the appropriate C2PC server and to **close** the *Login* window, the *Visual Connection Display* window is displayed.

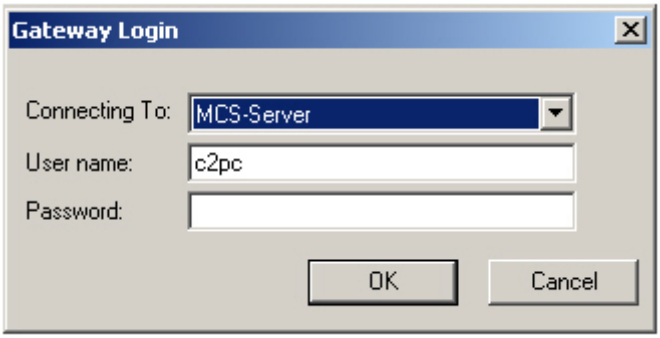


Figure 6-59 C2PC Gateway Login Window

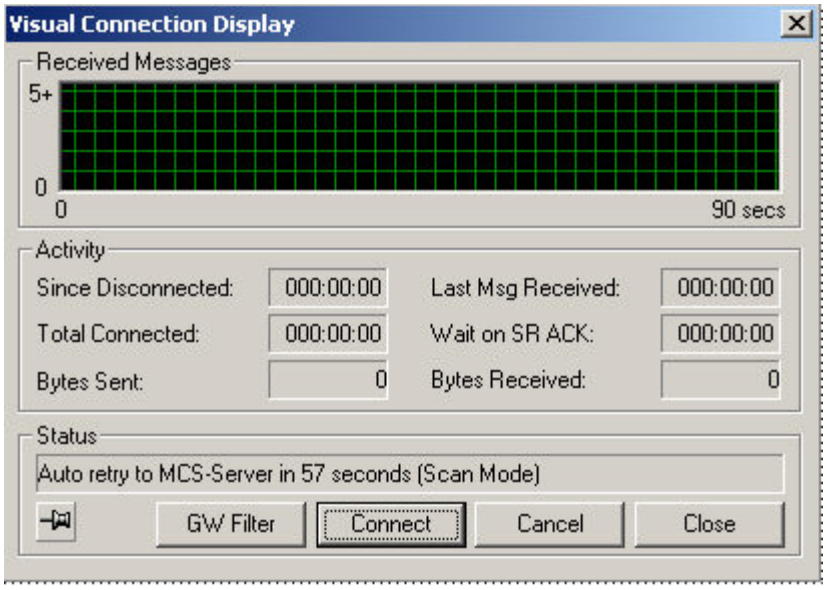


Figure 6-60 C2PC Visual Connection Display

Chapter 7 Troubleshooting Scenarios

7-1 Fault #1: Cannot View AFATDS Target Information in Live Feed

Information for Scenario Briefing:
The MCS Gateway is properly configured to use AFATDS AXE.

The MCS Gateway *NRTS Server Console* shows Targets received from AFATDS.

Fault Symptoms:
The MCS Workstation Maps & Overlays application shows AFATDS Units and Graphics, but no targets.

Fault Solution:
MAU:

1. **Check** with AFATDS operator to ensure targets are present.
2. **Check** with MAA to ensure NRTS is receiving AFATDS Target information.
3. **Open** Maps & Overlays, Tools, Options, Live Feed, AFATDS to ensure AFATDS Targets are selected for display.
4. **Right click** on AFATDS in the Maps & Overlay Mission Explorer, Live Feed and select Request All.
5. If AFATDS Targets are available, they will display in a short time (approximately 2 minutes).

MAA:

1. **Check** with AFATDS operator to ensure the AFATDS AXE is connected to the AFATDS. If not, stop and start the AFATDS AXE.
2. **Check** the *NRTS Server Console* to ensure the AFATDS Targets are present in the Data Providers drop-down list. If not, ask the AFATDS operator to generate a target to ensure AFATDS AXE and the NRTS AFATDS Data Provider displays Targets.
3. **Check** the MCS Workstation to ensure the AFATDS Targets display on Live Feed.

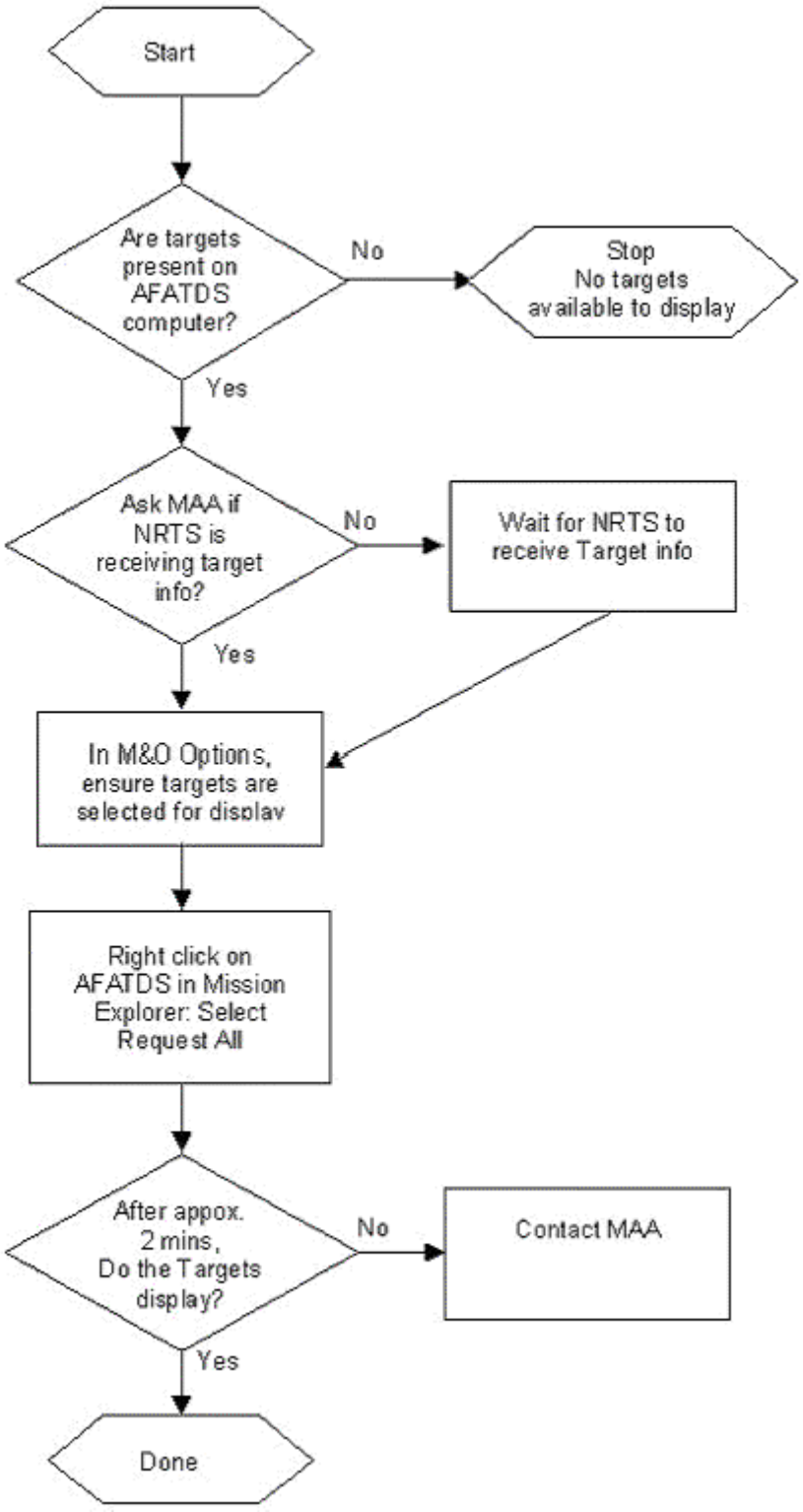


Figure 7-1 MAU Fault #1: Cannot View AFATDS Target Information in Live Feed

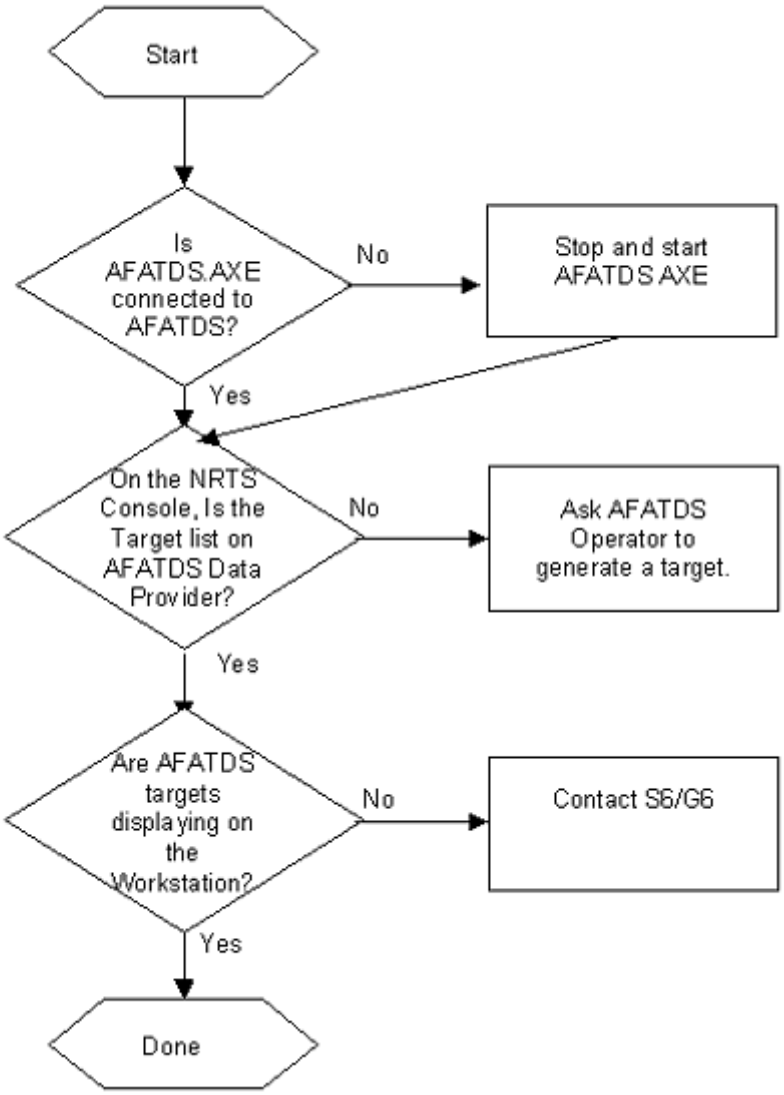


Figure 7-2 MAA Fault #1: Cannot View AFATDS Target Information in Live Feed

7-2 Fault #2: Cannot connect to the SQL Database

Information for Scenario Briefing:
The MCS Workstation *C2 Management Console* shows the system is configured to the Server IP Address and SQL Username.

Fault Symptoms:
When the MAU attempts to use the SQL Database in Task Organization or Maps & Overlays, Task Organization shows no TOs available on the SQL Server, Maps & Overlays returns the error message “There was an error creating the overlay on the SQL Server, Please check the database connection.”

Fault Solution:
MAU:

1. **Contact** the MCS MAA.

MAA:

1. **Open** the *C2 Management Console*, select the *SQL Server Data Connection* and **click** *Test Connection*. Note what part of the test connection fails.
2. If the test returned a problem with the Network, **notify** the S6 that a possible connectivity issue exists.
3. **Enter** the correct IP Address, Database User, Database User Password, and SQL Server hostname. Ensuring that the CAPS Lock is off.
4. **Select** the *SQL Server Data Connection* and click *Test Connection*. If the test fails, **contact** the SQL Server Administrator to ensure the Username and Password are correct on the SQL Server.
5. **Use** the *C2 Management Console* to test the SQL Server data connection. If successful, notify the MAU. If not, notify the S6/G6 for MCS Tech support.

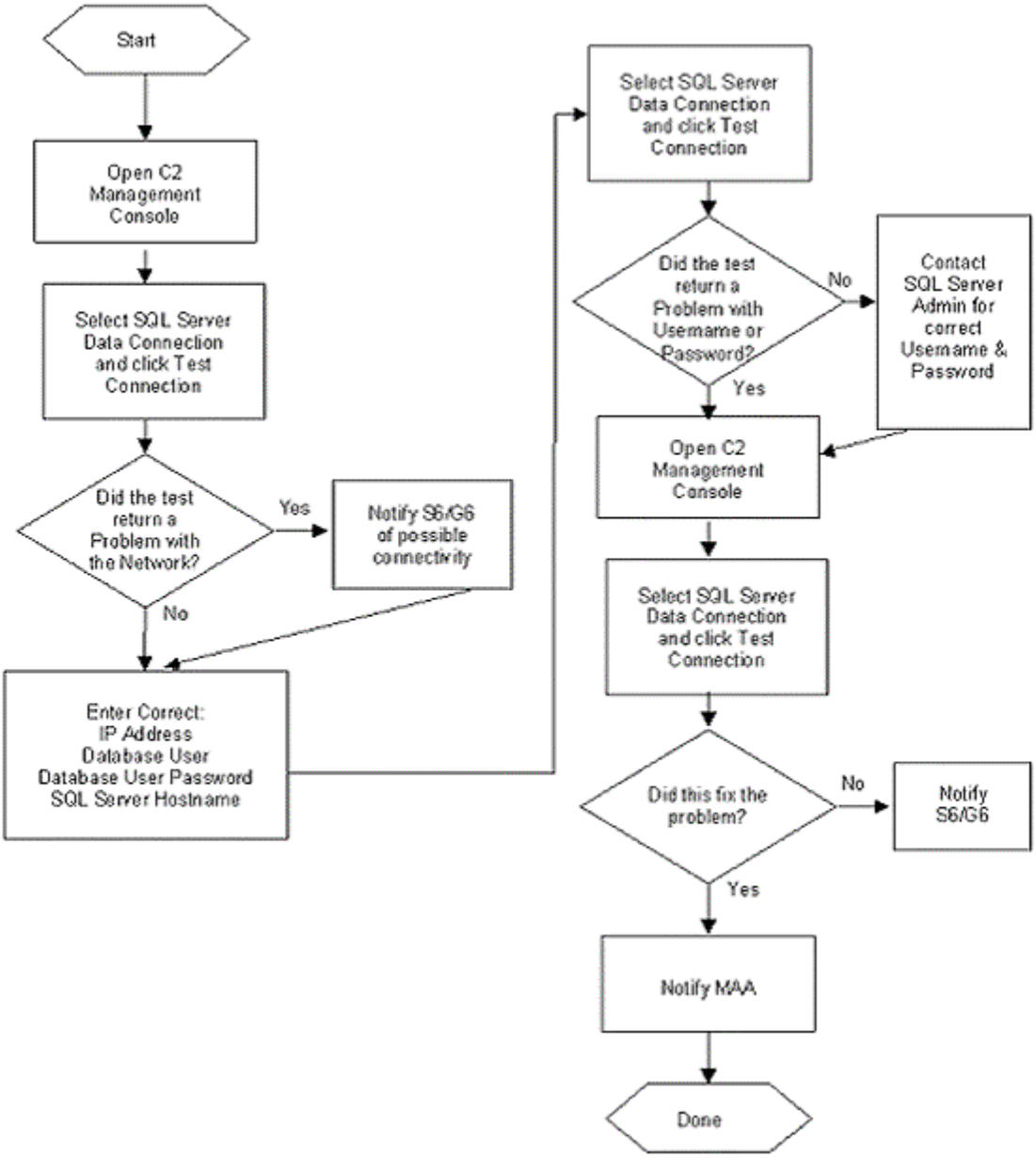


Figure 7-3 MAA Fault #2: Cannot Connect to the SQL Database

7-3 Fault #3: Cannot send messages using MCS Messaging

Information for Scenario Briefing:
The MAU has attempted to send messages to distant stations and received a CANTPRO in the GTCS Receive Log.

Fault Symptoms:
The MCS Workstation receives a CANTPRO “Addressee Unknown” when a message is sent to a distant station. The message does not arrive at the distant station.

Fault Solution:

MAU:

1. **Send** a test Loopback message to the MCS Workstation.
2. **Send** a test message to a known operational distant station. If message fails, contact the MAA.

MAA:

1. **Close** the Message Log (if open).
2. **Open** the *C2 Management Console* and select *Messaging Config* branch in the tree (Left Pane).
3. If *Messaging Config* area shows a listing of local files, use the *Messaging* pull-down menu in the menu bar, and select *Use C2R for Role Selection.*
4. **Enter** the correct IP Address for the C2R Server (Local PASS Server IP Address) and click *Connect to C2R*.
5. **Select** the correct *Domain, Unit,* and *Role* for the MCS Workstation.
6. **Click** the *C2 Management Console Configur*e button. The MCS Workstation will populate the messaging files with the correct information.
7. **Close** the *C2 Management Console.*
8. **Start** MCS Messaging.
9. **Send** a test message to a known operational distant station. If successful, notify the MAU to continue mission.
10. If a CANTPRO message is received in the *GTCS Receive Log*, **notify** the S6/G6 for MCS Tech support.

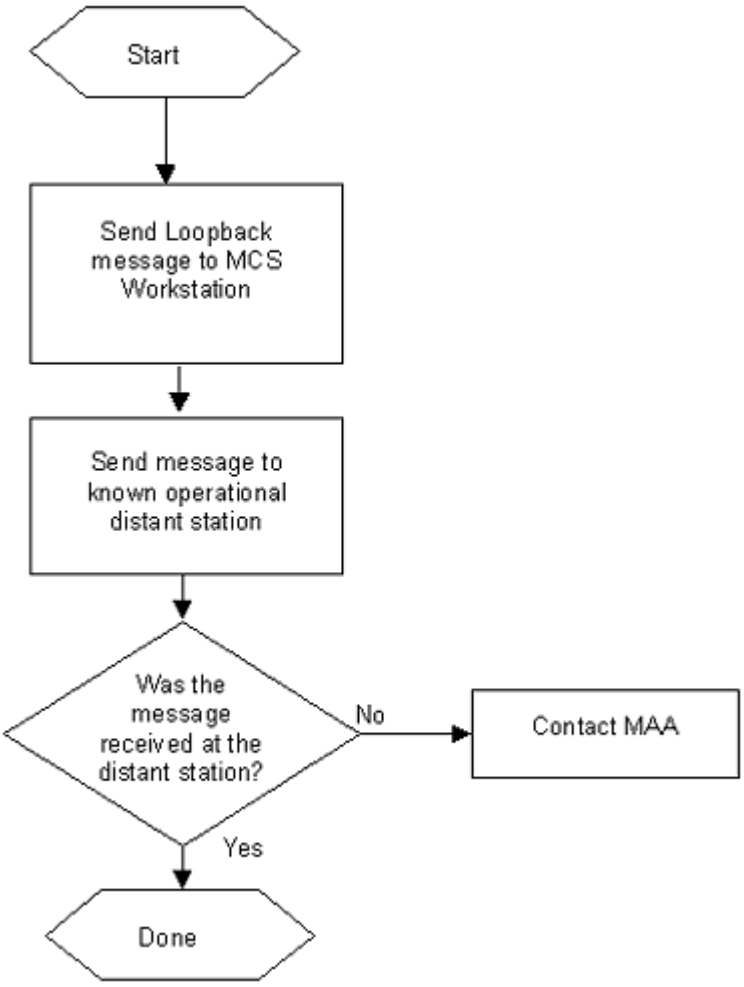

Start
Send Loopback message to MCS Workstation
Send message to known operational distant station
Was the message received at the distant station?
No
Contact MAA
Yes
Done

Figure 7-4 MAU Fault #3: Cannot Send Messages Using MCS Messaging

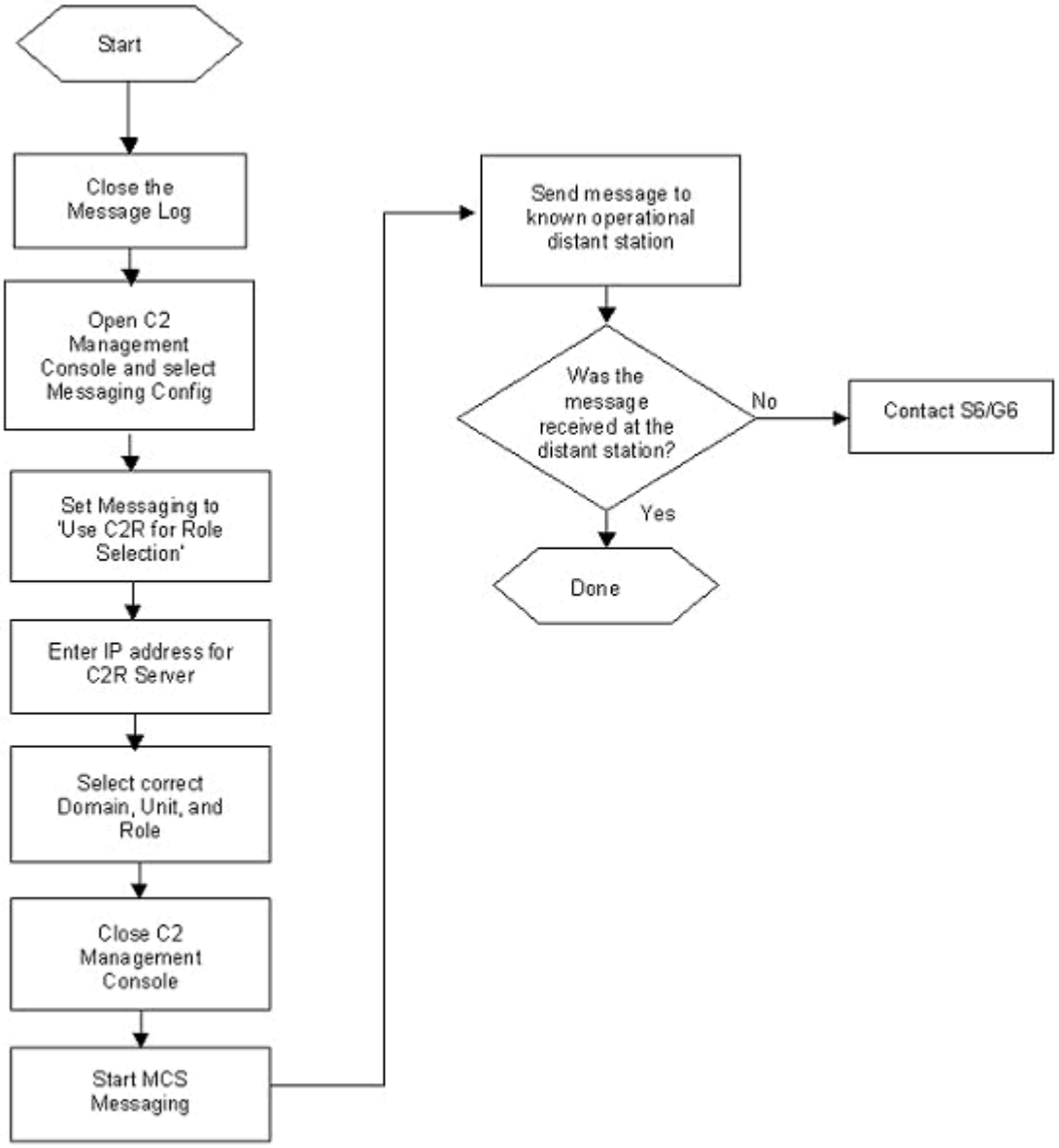


Figure 7-5 MAA Fault #3: Cannot Send Messages Using MCS Messaging

7-4 Fault #4: Cannot send messages using Microsoft Outlook

Information for Scenario Briefing:
The MCS MAU attempts to send an email message using Outlook and the distant station does not receive the message. Microsoft Outlook was previously configured to an Exchange Server.

Fault Symptoms:
Microsoft Outlook returns the error “Cannot contact the Exchange Server.”

Fault Solution:
MAU:

1. **Close** Microsoft Outlook.
2. **Open** the *Mail Preferences* in the *Windows Control Panel* (Start, Settings, Control Panel, Mail).
3. **Click** the *E-mail Accounts* button to open the E-mail Accounts Wizard.
4. Ensure the radio button for *View or Change existing e-mail accounts* is selected and **click** Next.
5. **Select** the appropriate e-mail account and **click** the *Change* button.
6. Ensure the Exchange Server name and user name are correct and **click** the *Check Name* button. The user name should become underlined. If not, contact the MAA.
7. **Click** the *More Settings* button. Set the Server Time-out to 180 seconds from the default of 30 seconds.
8. **Click** *OK*, *Next, and Finish* to close the *E-mail Accounts Wizard*.
9. **Click** *Close* to close the *Mail Setup* window.
10. Attempt to **send** an e-mail message to the local MCS and a distant station with a delivery receipt. If the attempt fails, contact the MAA.

MAA:

1. **Contact** the S6/G6 to confirm the Exchange Server hostname and domain.
2. In Mail Setup, **edit** the Exchange Server name to reflect the fully qualified domain name of the Exchange Server.
3. **Click** the *Check Name* button. The user name should become underlined. If not, contact the S6/G6 for possible network connectivity issues
.

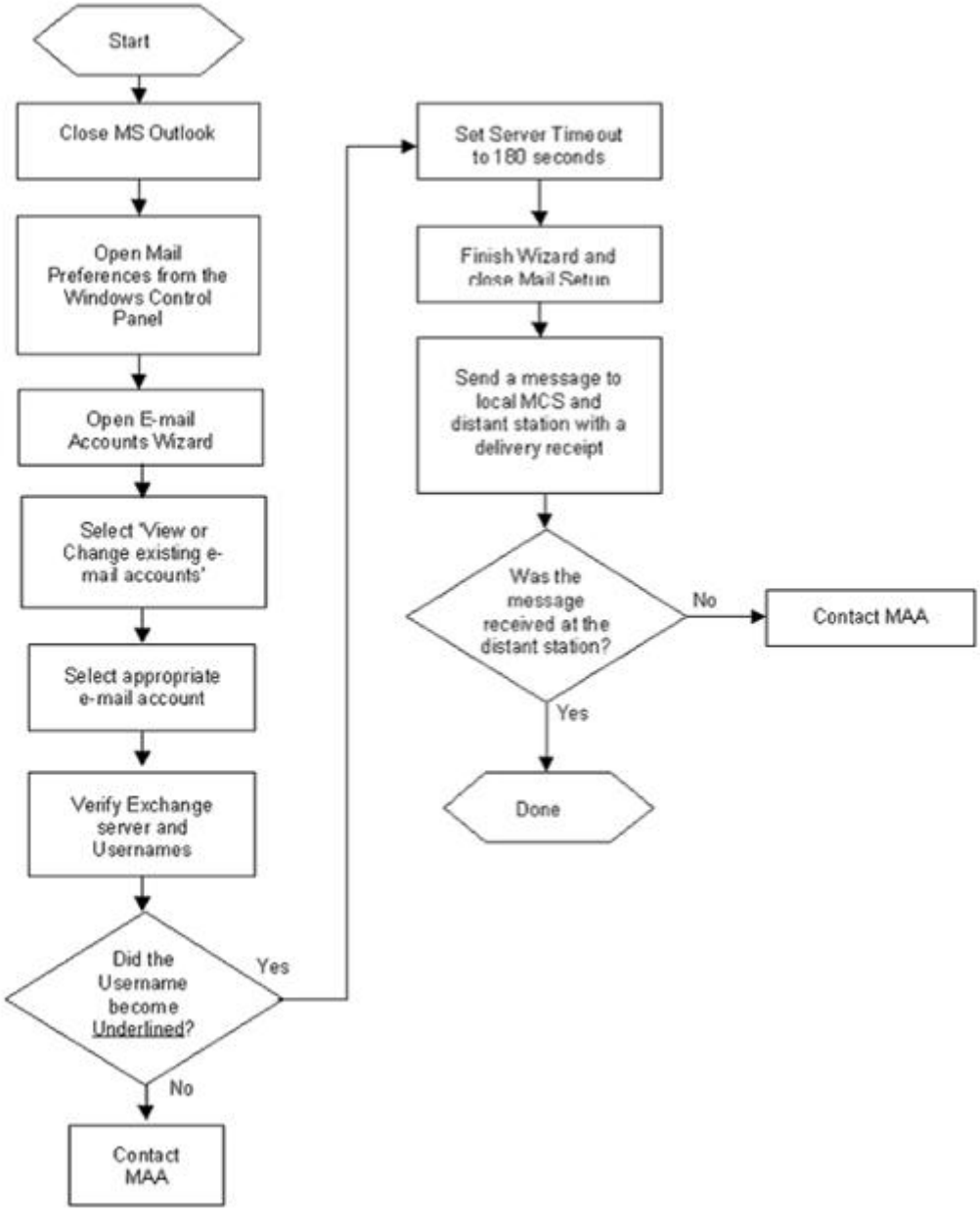


Figure 7-6 MAU Fault #4: Cannot Send Messages Using Microsoft Outlook

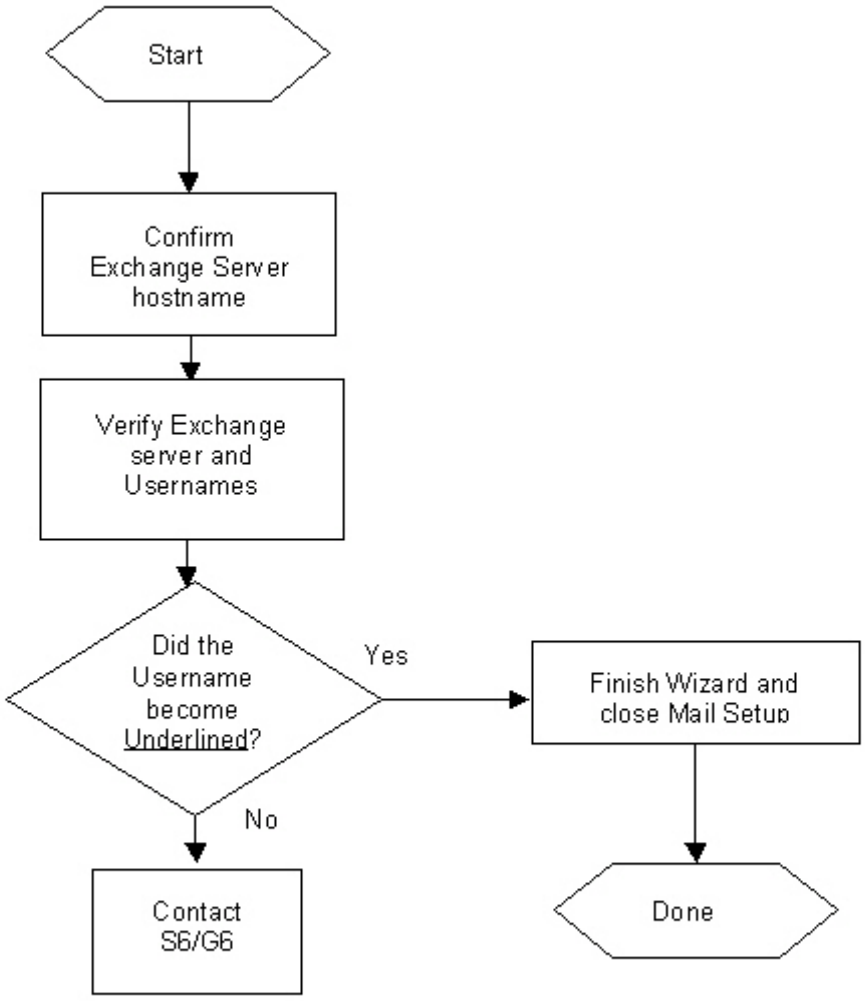


Figure 7-7 MAA Fault #4: Cannot Send Messages Using Microsoft Outlook

7-5 Fault #5: Cannot receive any Live Feed Information

Information for Scenario Briefing:
The MCS Gateway is properly configured and receiving Live Feed into the NRTS. Maps & Overlays are running on the MCS Workstation. The AFATDS, Blue, and Red Feeds are selected on the *Maps & Overlays Live Feed* tab.

Fault Symptoms:
No objects are visible under the *Live Feed* tab of *Maps & Overlays Mission Explorer.* All of the Live Feed categories are selected in the *Mission Explorer.*

Fault Solution:

MAU:

1. **Open** the *Options* window for Maps & Overlays (Tools, Options) and ensure that the applicable Live Feed options are selected. **Close** the *Options* window.
2. **Right-click** on one of the Live Feed categories in the *Mission Explorer* and select *Request All*.
3. In a short time (approximately 2 minutes), objects should appear in the applicable Live Feed categories. If not, **contact** the MAA.

MAA:

1. **Close** Maps & Overlays on the MCS Workstation.
2. **Open** the MCS Workstation *C2 Management Console*.
3. **Select** *Gateway Config* and **ensure** the IP Address and Port settings match the NRTS.
4. **Select** *Security Config* and **ensure** the IP Address of the Time Sync server matches that of the MCS Gateway.
5. **Click** the *C2 Management Console Configure* button. When configuration is complete, close the *C2 Management Console*.
6. **Open** Maps & Overlays and **select** the appropriate mission.
7. **Select** the *Live Feed* tab in *Mission Explorer* and **turn on** *Blue Feed.*
8. In a short time (approximately 2 minutes), a "+" will appear next to *Blue Feed.* Expand *Blue Feed* and ensure units and platforms populate the folders.
9. If units and platforms do not appear, **right-click** on *Blue Feed* and **select** *Request All*. If units and platforms do not appear within five minutes, **close** Maps & Overlays and re-boot the MCS Workstation.
10. After re-boot, **check** Maps & Overlays Live Feed. If no success, **contact** the S6/G6 for MCS Tech support.

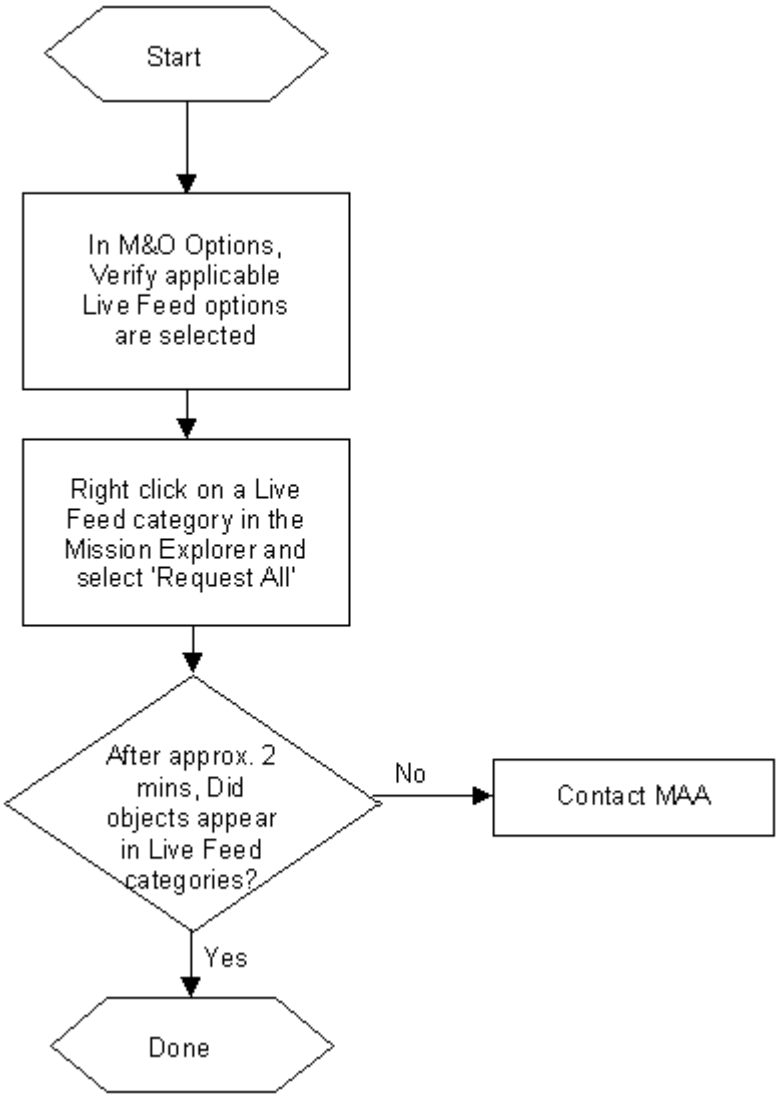


Figure 7-8 MAU Fault #5: Cannot Receive Any Live Feed Information

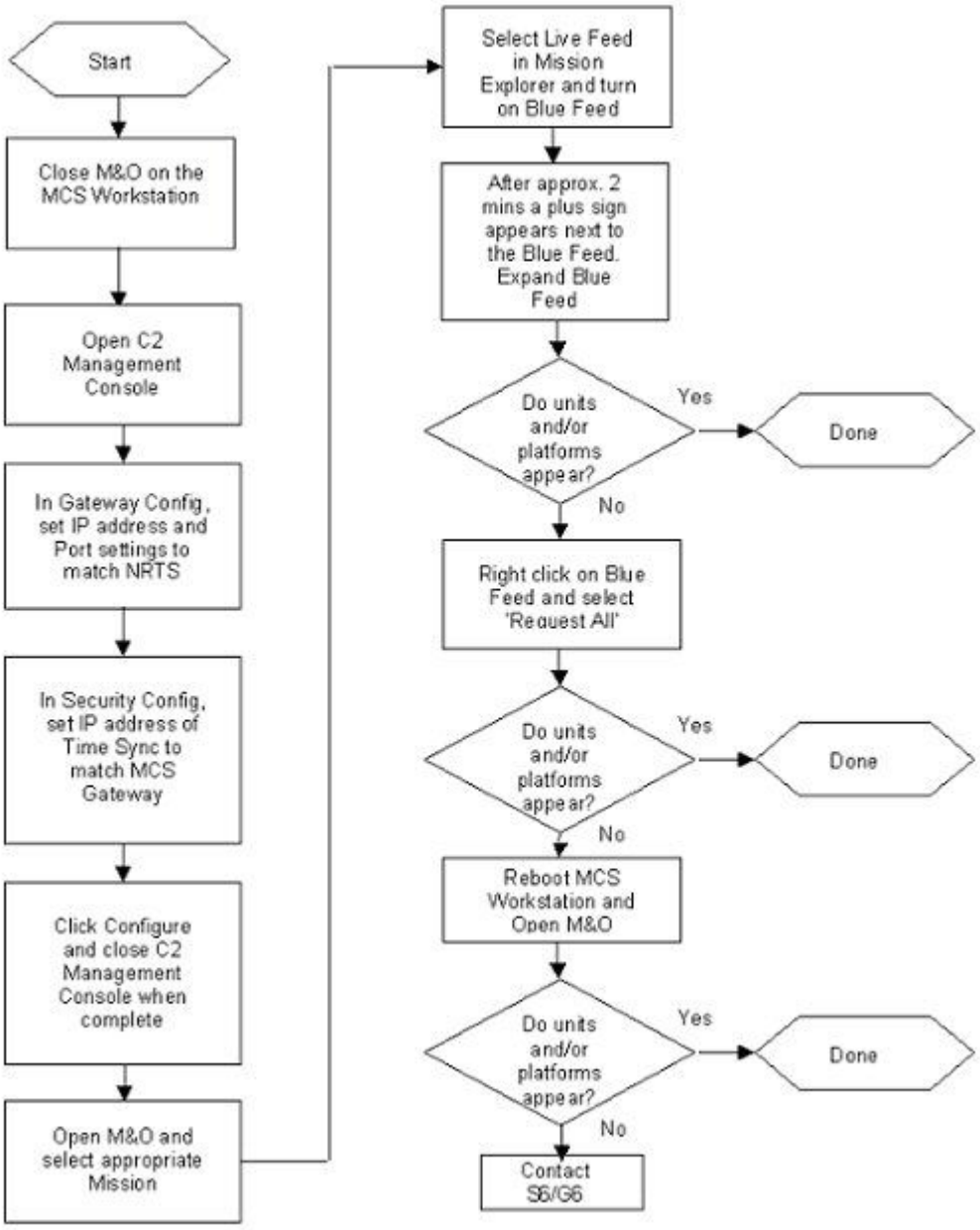


Figure 7-9 MAA Fault #5: Cannot Receive Any Live Feed Information

7-6 Fault #6: Cannot Connect to PASS

Information for Scenario Briefing:
The MCS was previously used in a different TOC, and cannot connect to the PASS in the current TOC.

Fault Symptoms:

The MCS cannot connect to the PASS using the *C2 Management Console* or *NRTS PASS Configuration.* The error message returned is “PASS threw an exception. Connection Failed.” MCS applications return various errors when the PASS connection fails.

Fault Solution:

MAU:

1. **Open** *Maps & Overlays*.
2. **Select** *Tools, Options* to **open** the *Options* window.
3. **Select** *PASS, Publishing* and **click** the *Verify* button.
4. If the PASS connection fails, **contact** the MAA.
5. **Open** the *Management Console* and **ensure** the settings for PASS are correct.

MAA:

1. **Ensure** the certificates are installed on the MCS. **Navigate** to the D:\MCS\Shared\Certificates folder.
2. **Right-click** on each certificate in the folder and **install** the certificates using the default options and locations.
3. **Open** Internet Explorer and in the *Address* box **enter** https://{IP ADDRESS OF PASS SERVER}:7443 and press *Enter.* A window will appear. Click the *View Certificate* button.
4. The *Certificate* window will appear, **click** the *Install Certificate* button and **use** the default choices to install the PASS Server certificate.
5. **Contact** the PASS operator for the correct IP Address and ports.
6. **Open** the *C2 Management Console*, **select** *PASS Config,* and **ensure** the settings are correct. Pay special attention to the password to ensure it is in the correct case.
7. **Click** the *connect* button to **check** connectivity to the PASS Server. If successful **inform** the MAU to continue mission.
8. If the PASS Server connection fails, **contact** the S6/G6 for MCS Tech support.

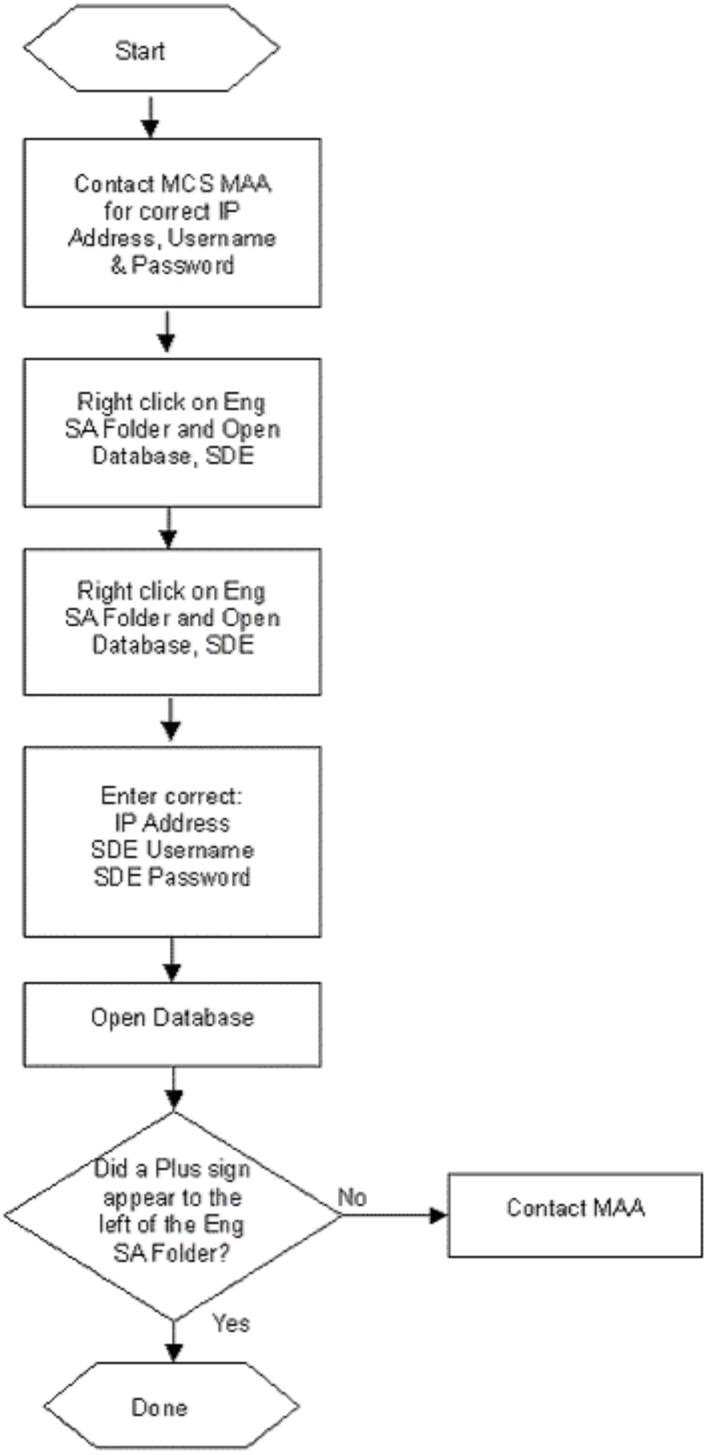


Figure 7-10 MAU Fault #6: Cannot Connect to PASS

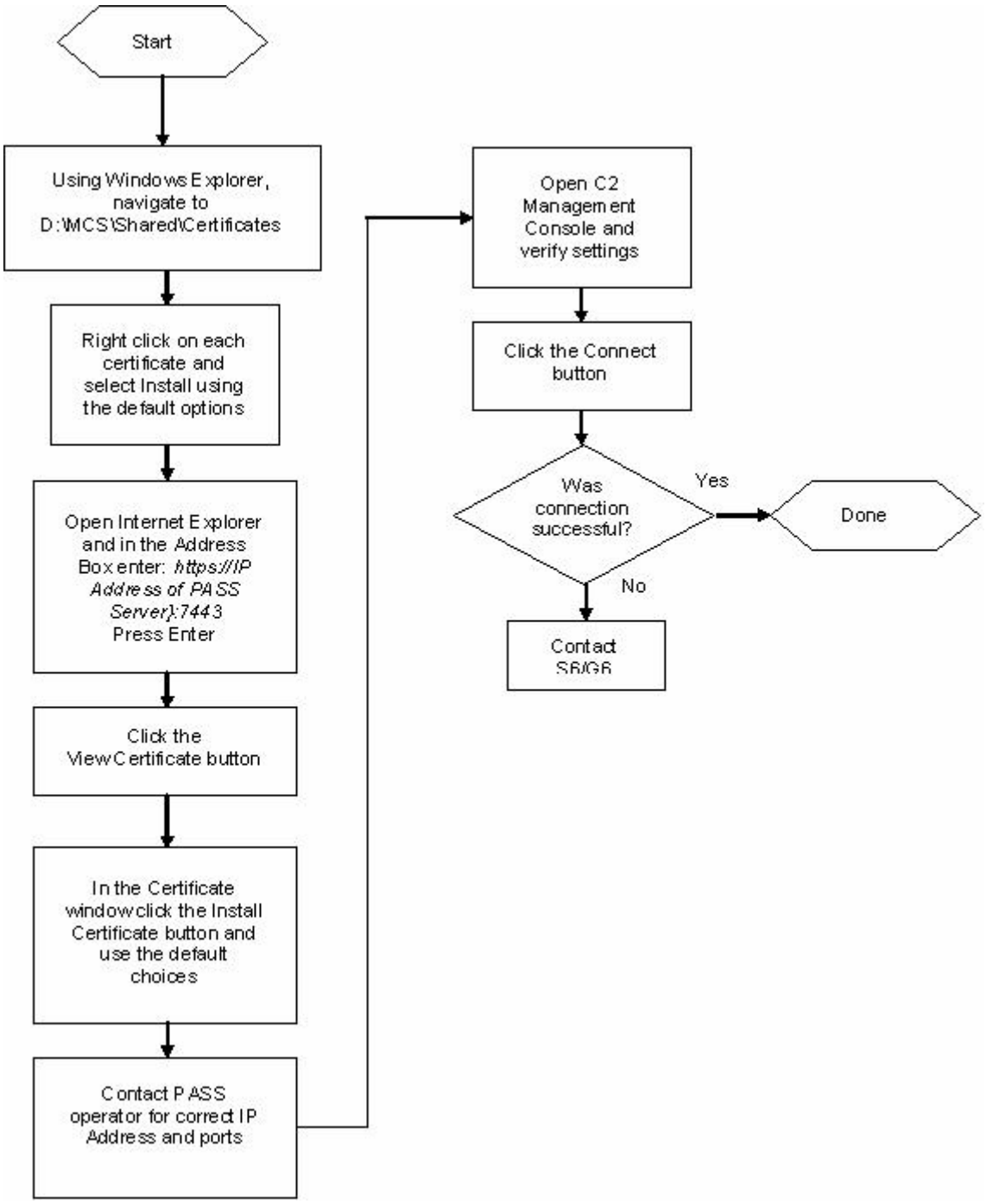


Figure 7-11 MAA Fault #6: Cannot Connect to PASS

7-7 Fault #7: Cannot Publish to PASS

Information for Scenario Briefing:

The MAU attempts to export overlay(s) to the PASS Server from the Maps & Overlays application. Upon clicking Export to PASS, the “Cannot connect to the selected PASS Server. Please re-start the selected PASS Server or select another one“ error message appears.

Fault Symptoms:

Cannot connect to the PASS Server through the MCS applications.

Fault Solution:

MAU:

1. **Open** Maps & Overlays.
2. **Select** *Tools, Options* to open the *Options* window.
3. **Select** P*ASS, Publishing* and **click** the *Verify* button.
4. If the PASS connection fails, **contact** the MAA.
5. Open the *C2 Management Console* and ensure the settings for the PASS are correct.

MAA:

1. **Contact** the S6/G6 to check network connectivity and settings for the PASS Server.
2. **Close** any open MCS applications.
3. **Open** the *C2 Management Console*, **select** *PASS Config* and ensure the settings are correct.
4. **Click** *Connect*, if an error message returns stating “PASS threw an exception”, **follow** the steps to install the DOD and PASS certificates on the MCS.
5. After installing the certificates, **click** *Connect*.
6. If PASS connection fails, **check** to ensure PASS is running.
7. If the PASS connection continues to fail when checking with *C2 Management Console*, **contact** the S6/G6 for MCS Tech support.

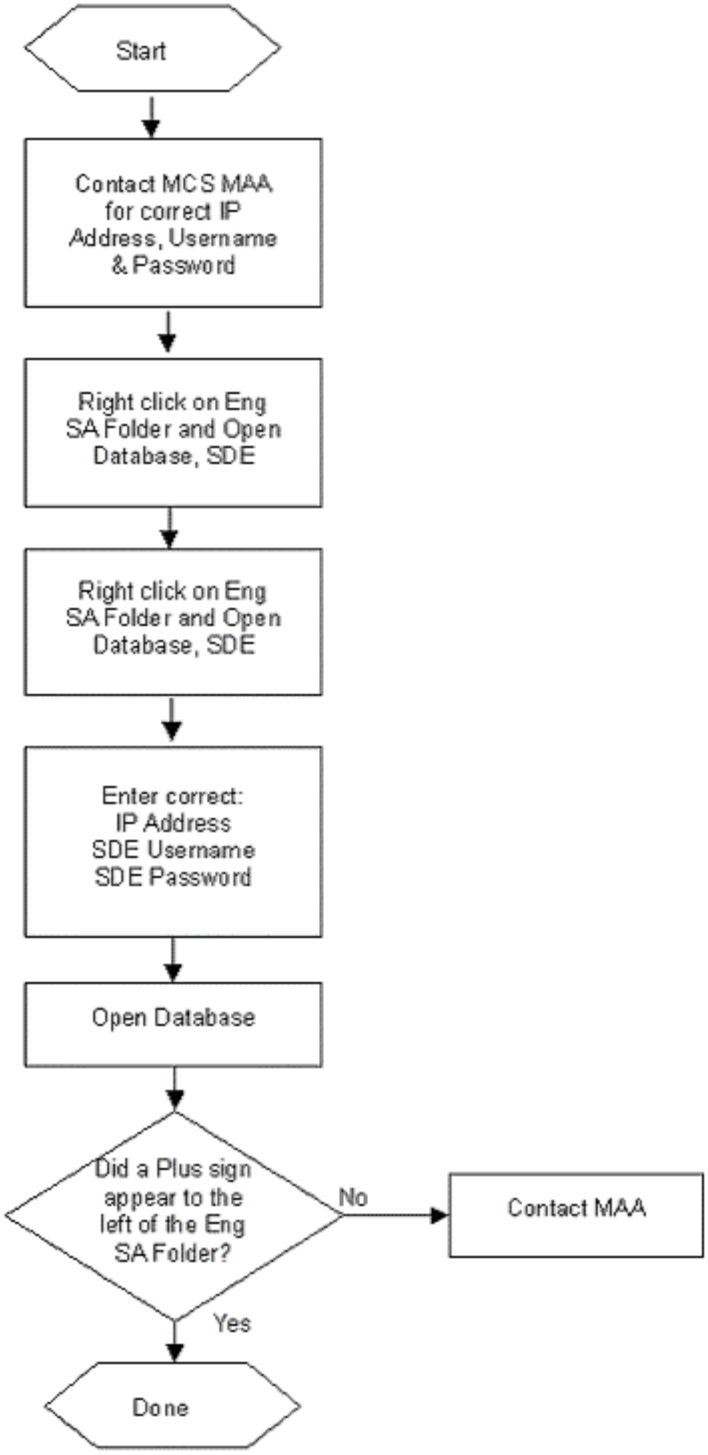


Figure 7-12 MAU Fault #7: Cannot Publish to PASS

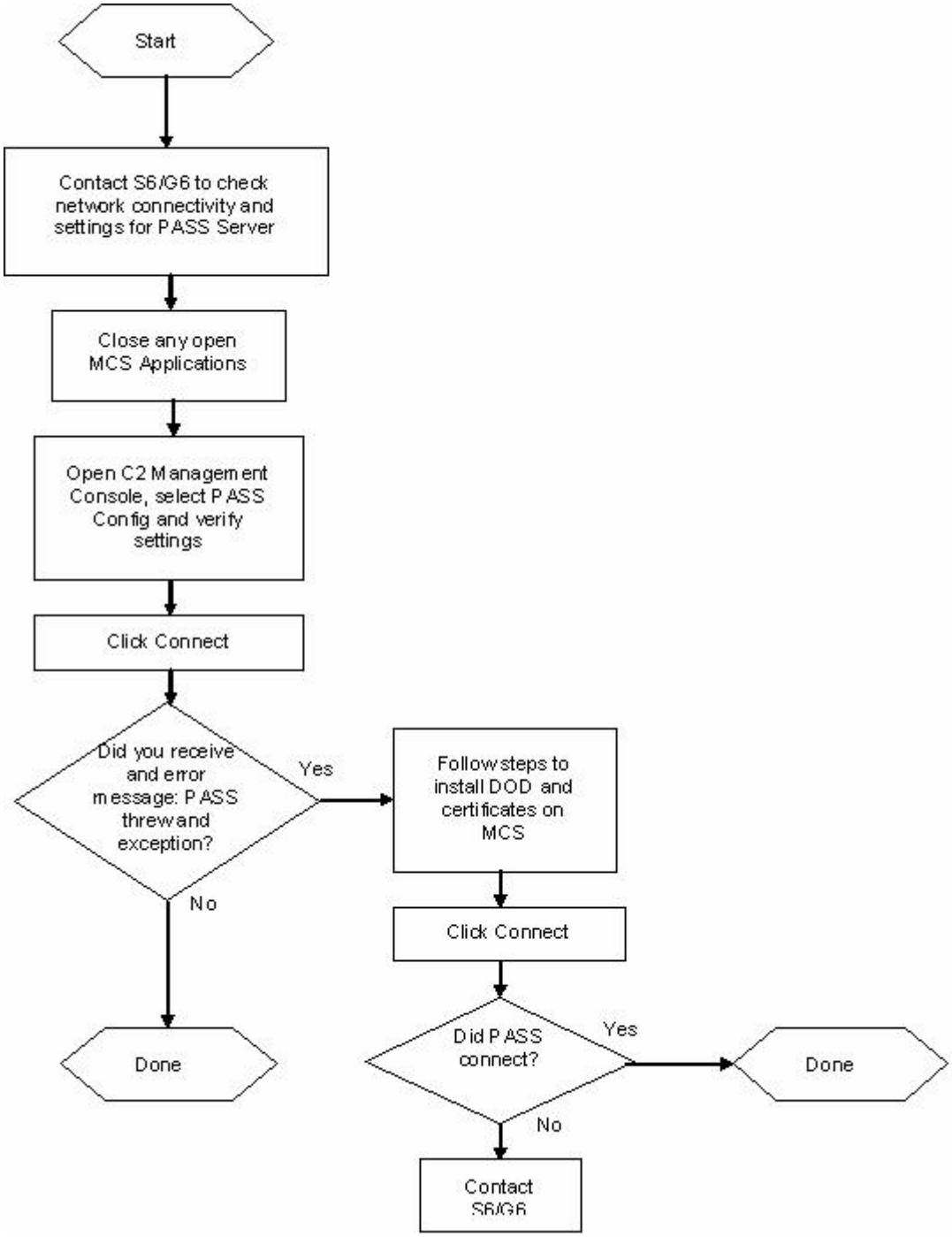


Figure 7-13 MAA Fault #7: Cannot Publish to PASS

7-8 Fault #8: Cannot Subscribe to PASS

Information for Scenario Briefing:
The MCS Gateway NRTS is used to subscribe to the PASS Server for various BFA data. The NRTS and PASS Data Provider are running.

Fault Symptoms:

1. *NRTS Server Console* and *PASS Data Provider* are running (Green) with no items shown next to *PASS Data Provider*.
2. *NRTS Server Console* and *PASS Data Provider* are running, but *PASS Data Provider* is red, with exclamation point shown.

Fault Solution:

MAU:

Fault is on MCS Gateway, MAU has no tasks.

MAA:

1. **Open** the *NRTS Configuration Manager* and **select** the PASS Configuration tab.
2. **Ensure** the PASS Server configuration is correct.
3. **Click** the *Test PASS Connection* button and observe the results. If other BFAs have published to the PASS, their topics will appear in the *PASS Connection Status* window. If not, the "Test PASS Connection is Failed!" error is returned with the result listed in the window.
4. If the connection fails, **contact** the MAA that is affiliated with PASS to check the status.
5. If BFA topics are listed, **click** *OK* on the *PASS Status* window and **select** the *Near Real-Time Server* tab.
6. **Select** the *PASS Data Provider* in the left pane; the *Subscription* box in the right pane will display the current topic subscriptions. If NRTS has not been properly configured, the *Subscription* box will display a large number of default topics.
7. If default topics exist, **select** the topics (check the corresponding box) and **click** the *Remove* button.
8. When the *Subscription* box is devoid of topics, **click** the *Refresh* button. After a short time (approximately 3 minutes), the currently available PASS topics will display in the *Available Topic* box.
9. **Select** the appropriate topic(s) and **click** the *Right Arrow* button to move the topic to the *Subscription Topic* box.
10. When all appropriate topics are listed in the *Subscription Topic* box, **click** the *Apply* button and *Yes* to the prompt to overwrite NRTS Properties.
11. **Click** the *Close* button to close the *Configuration Manager* button.
12. **Highlight** the *PASS Data Provider* and **click** the *Stop* button. When the *PASS Data Provider* shows a Stop sign, **click** the *Start* button to re-start the Data Provider.
13. The *PASS Data Provider* will show a running status (Green) and numbers of objects received should display.
14. If no objects appear in the *NRTS Server Console* window, **contact** the S6/G6 to determine the status of published items on the PASS.

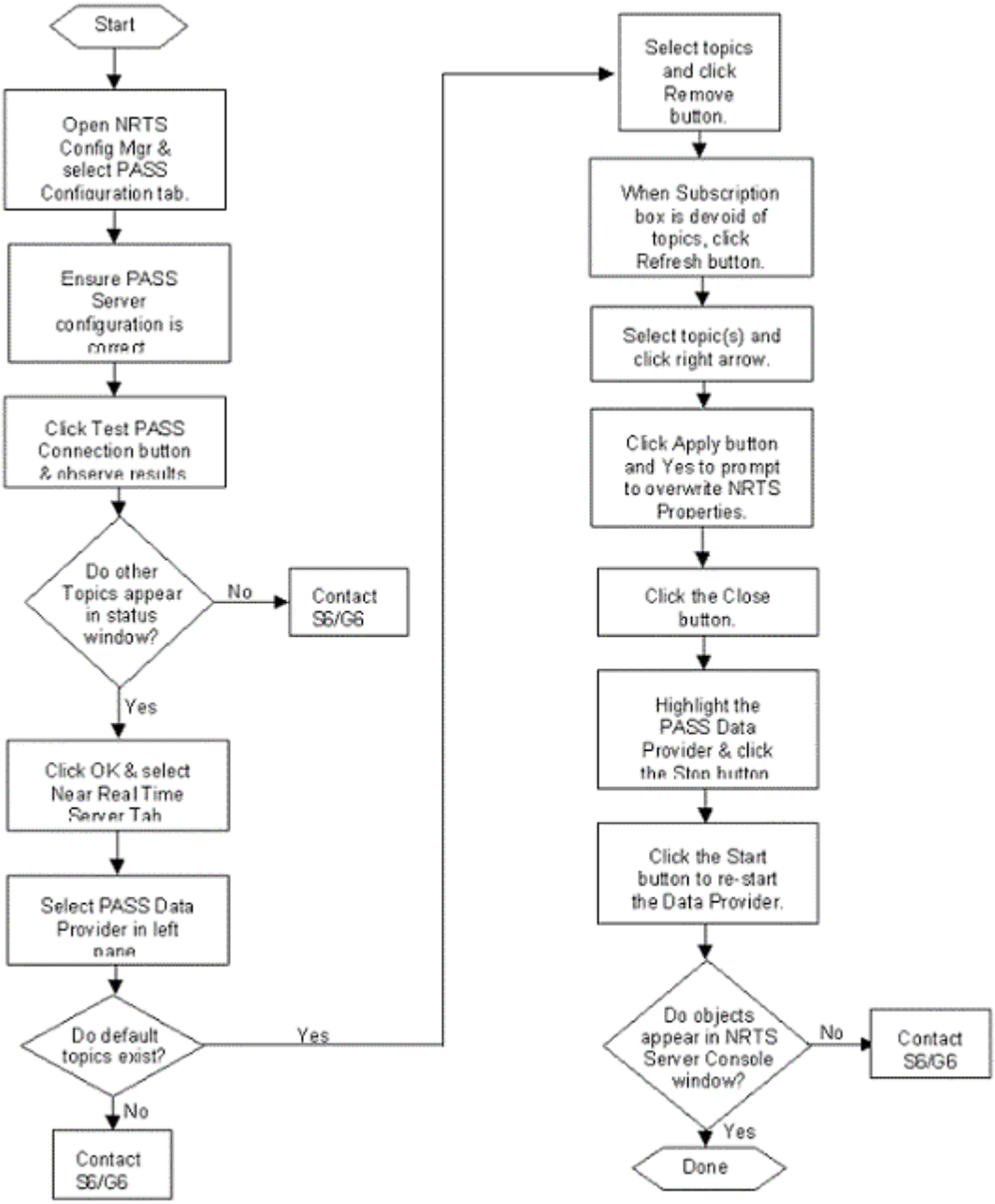


Figure 7-14 MAA Fault #8: Cannot Subscribe to PASS

7-9 Fault #9: Cannot connect to AFATDS using AFATDS AXE

Information for Scenario Briefing:
The MCS Gateway is properly configured to the appropriate AFATDS system. The AFATDS Feed has stopped.

Fault Symptoms:
The console window for AFATDS AXE shows a failure to connect to the AFATDS.

Fault Solution:
MAU:
The fault is on MCS Gateway. The MAU has no tasks.

MAA:

1. **Check** the *AFATDS AXE console* window to determine the cause of the failure.
2. **Contact** the AFATDS operator to determine the correct IP Address, Username, and Password.
3. **Open** the *Server Config* Console and select the *Incoming Data and Fires* from the tree.
4. **Enter** the correct information for the MCS user on the AFATDS.
5. **Click** *Configure*, and then *Exit* when complete.
6. **Click** on the X in the upper right corner of the *AFATDS AXE* console window to stop AFATDS AXE.
7. **Open** *Windows Explorer* and navigate to D:\MCS\AFATDS.axe.
8. **Double-click** on AXE.exe to start the AFATDS AXE.
9. **Monitor** the AFATDS AXE console window to ensure the AFATDS AXE connects to the appropriate AFATDS system.
10. After a short time (approximately 3 minutes), AFATDS objects should appear next to the *AFATDS Data Provider* in the *NRTS Server Console*.
11. If AFATDS objects do not appear, **contact** the S6/G6 for MCS Tech support.

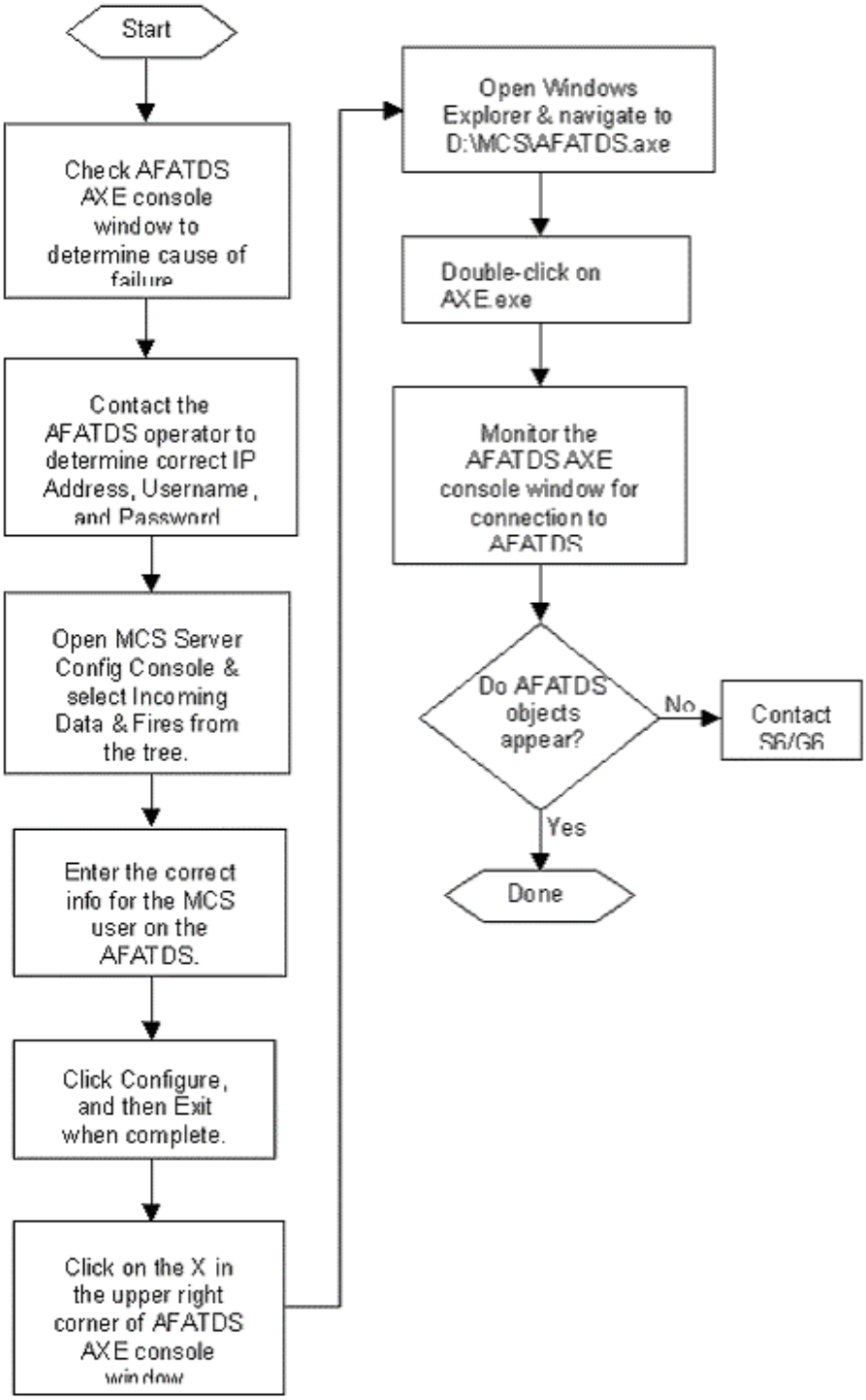


Figure 7-15 MAA Fault #9: Cannot Connect to AFATDS Using AFATDS AXE

7-10 Fault #10: Cannot receive SA information

Information for Scenario Briefing:
The MCS Gateway NRTS is running and receiving data from the PASS Data Provider. FBCB2 displays a number of platforms and units.

Fault Symptoms:
The *NRTS Server Console* shows no objects listed for the *SA Data Provider.*

Fault Solution:
MAU:
This is a MCS Gateway fault. The MAU has no tasks.

MAA:

1. **Open** the *NRTS Configuration* Manager.
2. **Select** the *SA Data Provide*r in the left pane. The *Multicast Address* box will display the current SA Multicast Groups and Multicast Ports
3. **Contact** the S6/G6 to obtain the correct Multicast Groups/Ports for the TOC.
4. **Edit** the SA Multicast Addresses to reflect the correct Multicast Groups/Ports.
5. When complete, **click** *Apply* and *Yes* to overwrite the NRTS Properties.
6. **Close** the *Configuration Manager* window.
7. **Select** the *SA Data Provider* and **click** *Stop*.
8. **Start** the *SA Data Provider.*
9. The *SA Data Provider* should list objects after a short time (approximately 5 minutes), if not, contact the S6/G6 for MCS Tech support.

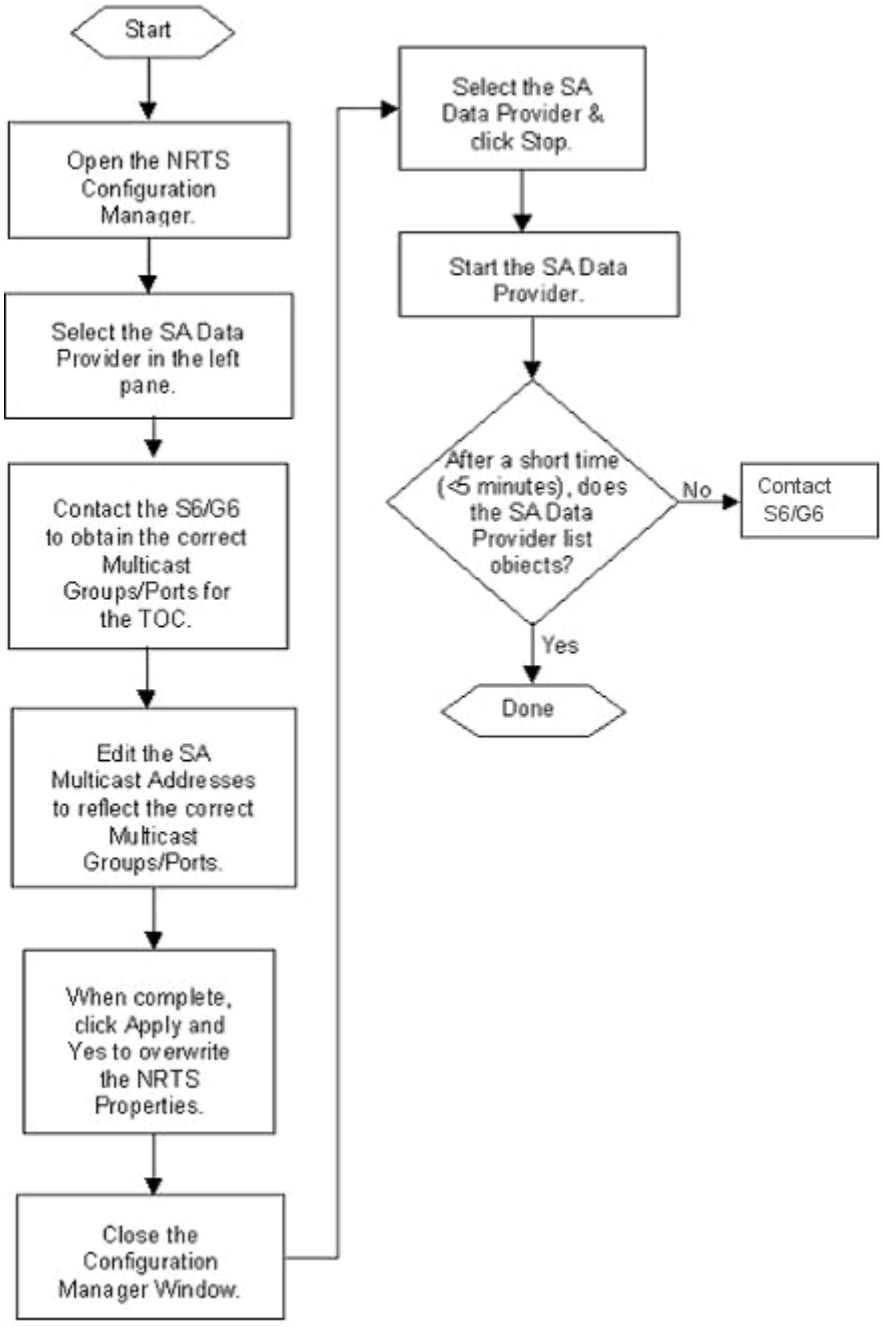


Figure 7-16 MAA Fault #10: Cannot Receive SA Information

7-11 Fault #11: No Network Connectivity

Information for Scenario Briefing:
The MCS is configured to a distant SQL Data Source.

Fault Symptoms:
The MCS cannot connect to any system.

Fault Solution:

MAU:

1. **Open** Maps & Overlays.
2. **Select** *Tools, Options* to open the *Options* window.
3. **Select** *PASS, Publishing*, and **click** the *Verify* button.
4. If the PASS connection fails, **contact** the MAA.

MAA:

1. **Open** the *Local Area Connection Status* window and **click** the *Properties* button.
2. **Highlight** Internet Protocol (TCP/IP) in the window and **click** the *Properties* button.
3. **Contact** the S6/G6 to ensure the network settings are correct and **edit** the settings if required.
4. **Close** the *Local Area Connection Properties* and *Local Area Connection Status* windows.
5. **Open** the *C2 Management Console* and **select** *Data Source Config*. **Select** the SQL Server Data source.
6. **Click** either the *Test* button from the *C2 Management Console* toolbar, or the *Test Data Source* button.
7. If the network connection to the server is poor or non-existent, **trace** the LAN cable to the Hub/Switch.
8. **Ensure** the Hub/Switch displays a link light for the MCS.
9. If no link light is present, **exchange** the LAN cable.
10. If no link light is present after the cable exchange**, notify** the S6/G6 for MCS Tech support

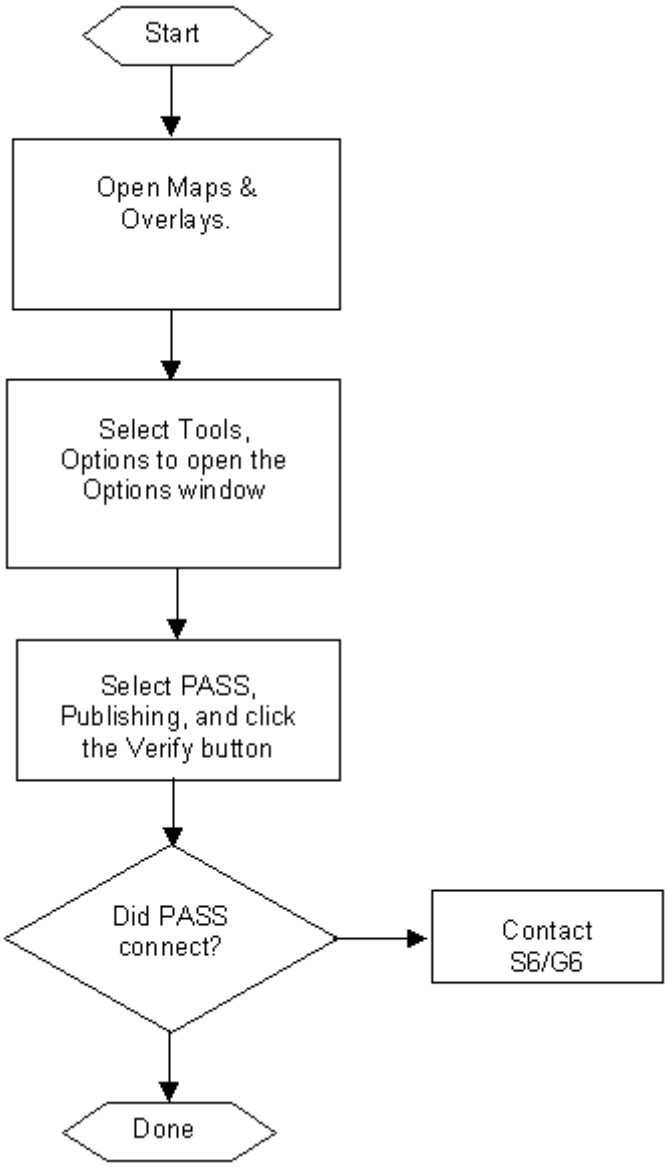


Figure 7-17 MAU Fault #11: No Network Connectivity

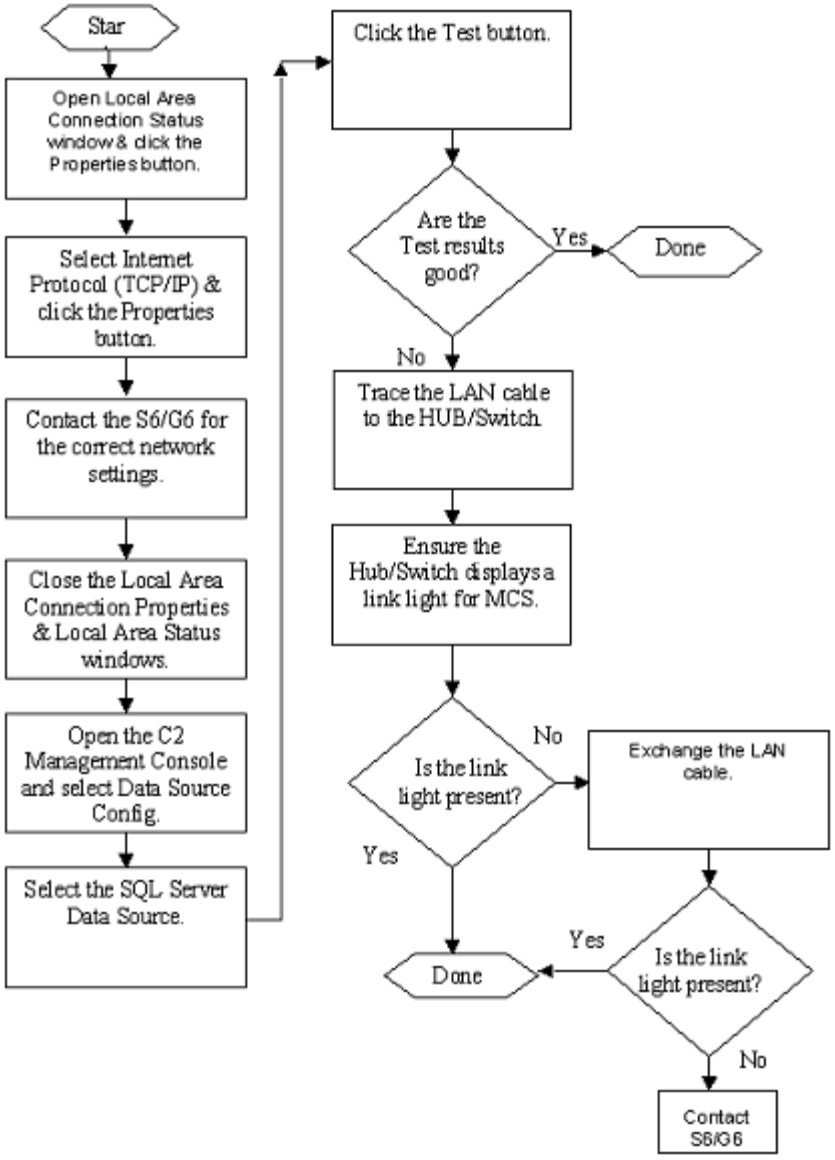


Figure 7-18 MAA Fault #11: No Network Connectivity

7-12 Fault #12: Cannot connect to Exchange Server using Microsoft Outlook

Information for Scenario Briefing:
The MCS workstation is connected across the LAN to the PASS Server and SQL Server.

Fault Symptoms:
After starting, Outlook returns error: Incorrect username or password.

Fault Solution:
MAU:

1. **Close** Outlook.
2. **Contact** the *S6/G6* and **confirm** the *Exchange Server* hostname, username and password.

3. **Open** the *Mail Settings* from the *Windows Control Panel* and **click** the *E-mail Accounts* button.
4. **Select** the user option button for *View or Change Existing E-mail Accounts* and **click** *Next*.
5. **Select** the appropriate e-mail account and **click** the *Change* button.
6. **Verify** the *Exchange Server* hostname and username are correct and **click** the *Check Name* button. The user name is underlined.
7. If a window appears prompting for the username and password, **enter** the correct information and **click** *OK*.
8. If the username is not underlined, **contact** the S6/G6 for MCS Tech support.

MAA:

No task for MAA unless the fault occurs on the MCS Gateway

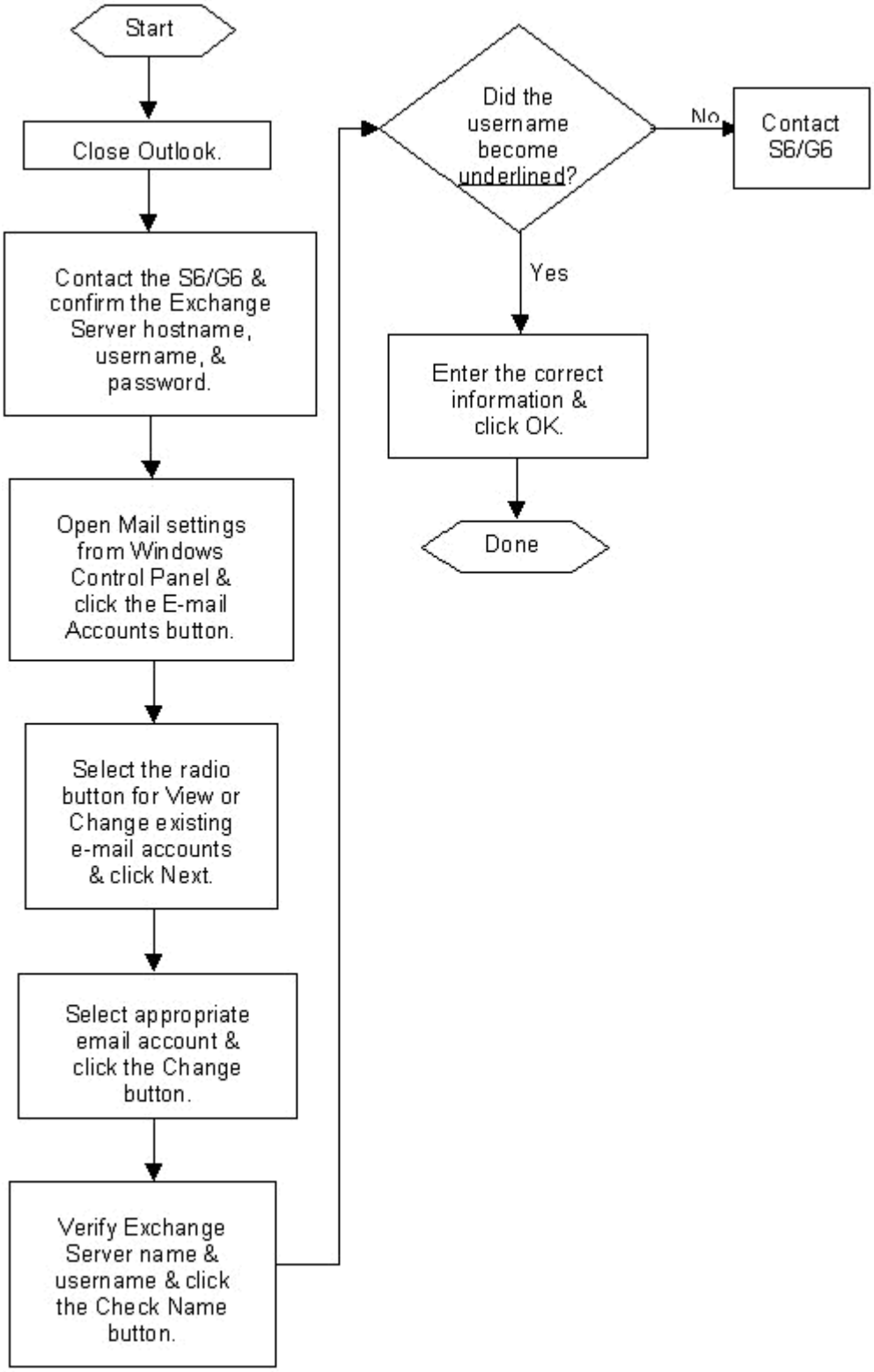


Figure 7-19 MAU Fault #12 Cannot Connect to Exchange Server Using Microsoft Outlook

7-13 Fault #13: System will not boot (start)

Information for Scenario Briefing:
The MCS system was shutdown prior to shift change.

Fault Symptoms:

1. The MCS workstation displays the error messages “Operating System Not Found.”
2. The MCS workstation displays the error messages ”NTLDR Missing.”
3. The MCS workstation starts with an operating system other than Windows XP Professional.

Fault Solution:
MAU:

1. **Check** the *CD-ROM* drive to ensure no media present.
2. If the *CD-ROM* drove is empty, **restart** the system using either the Crtl-Atl-Del keys or the power button.
3. If the system fails start, **contact** the MAA.

MAA:

1. **Restart** the system if halted with error.
2. **Press** *F2* to enter the system setup at Panasonic screen. The Setup Utility will display.
3. **Use** the arrow keys to **navigate** to *Boot* options.
4. **Ensure** the boot order is: CS-ROM Drive, Hard Disk Drive, LAN, Floppy Drive.
5. **Press** *F10* to save and exit the Setup Utility.
6. If the system starts to Windows XP Professional and *MCS,* **inform** the MAU to continue the mission.
7. If the system fails to start, **contact** the *S6/G6*

.

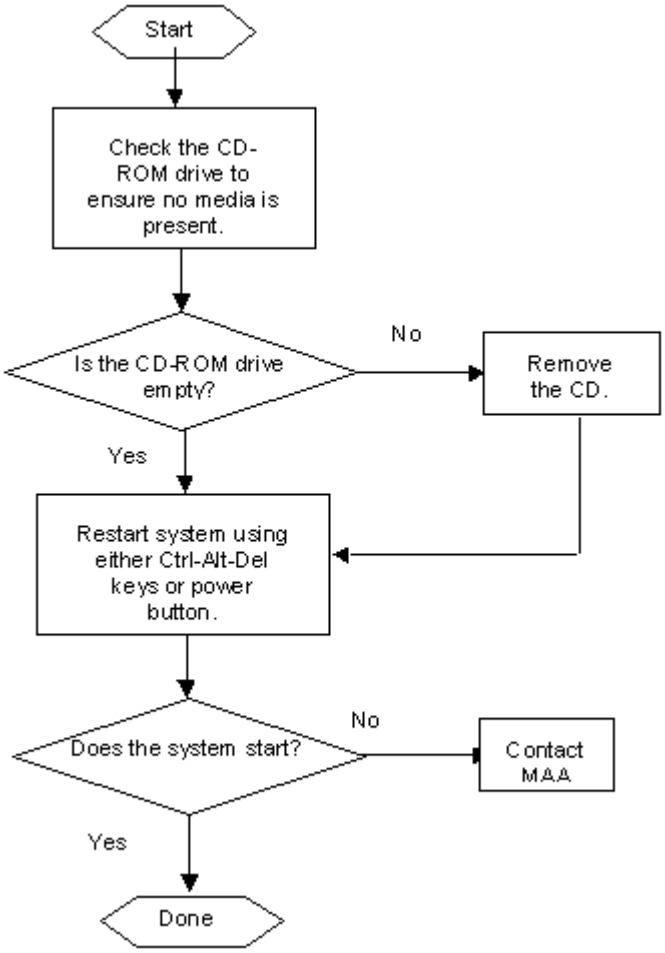


Figure 7-20 MAU Fault #13: System Will Not Boot (Start)

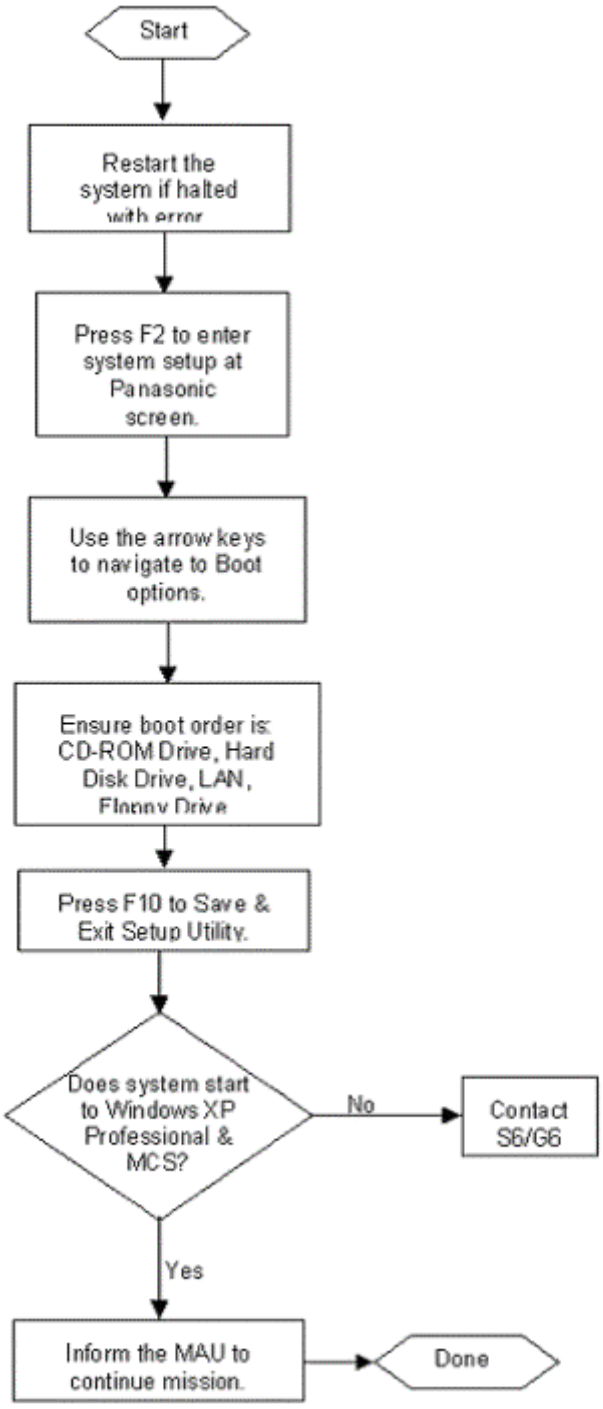


Figure 7-21 MAA Fault #13: System Will Not Boot (Start)

7-14 Fault #14: Create New Task Organization (TO) is unavailable in the Application

Information for Scenario Briefing:
The MCS Workstation is properly configured to the PASS and SQL Servers.

Fault Symptoms:
When the Task Organization application is opened, the *Create New* menu option and the toolbar icon are grayed out.

Fault Solution:
MAU:

1. **Contact** the MAA.

MAA:

1. **Close** all MCS applications.
2. **Open** the *C2 Management Console* and **select** *Org ID Config*.
3. **Ensure** that the *My Ownership Role* reflects *CDR*, *G3* or *S3*, and that the correct unit is selected.
4. **Click** the *C2 Management Console Configure* button.
5. **Close** the *C2 Management Console*.
6. **Open** *Regedit*.
7. **Select** *HKEY_LOCAL_MACHINE\SOFTWARE\Army\MCS*.
8. **Ensure** the *My Ownership Role,* selected and configured using the C2 Management Console, is reflected in the *Org_Role* key (i.e. S3).
9. If the *Role* is incorrect, **notify** the S6/G6 for MCS Tech support.
10. If the *Role* is correct, **close** *Regedit*.
11. **Open** the *Task Organization* application. The *Create New* menu option and toolbar icon are available for use. If not, **contact** the S6/G6 for MCS Tech support.

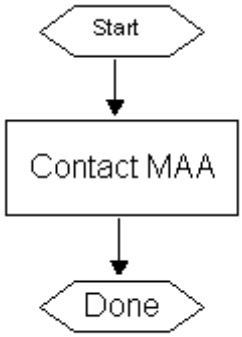


Figure 7-22 MAU Fault #14: Create New Task Organization is Unavailable in the Task Organization Application

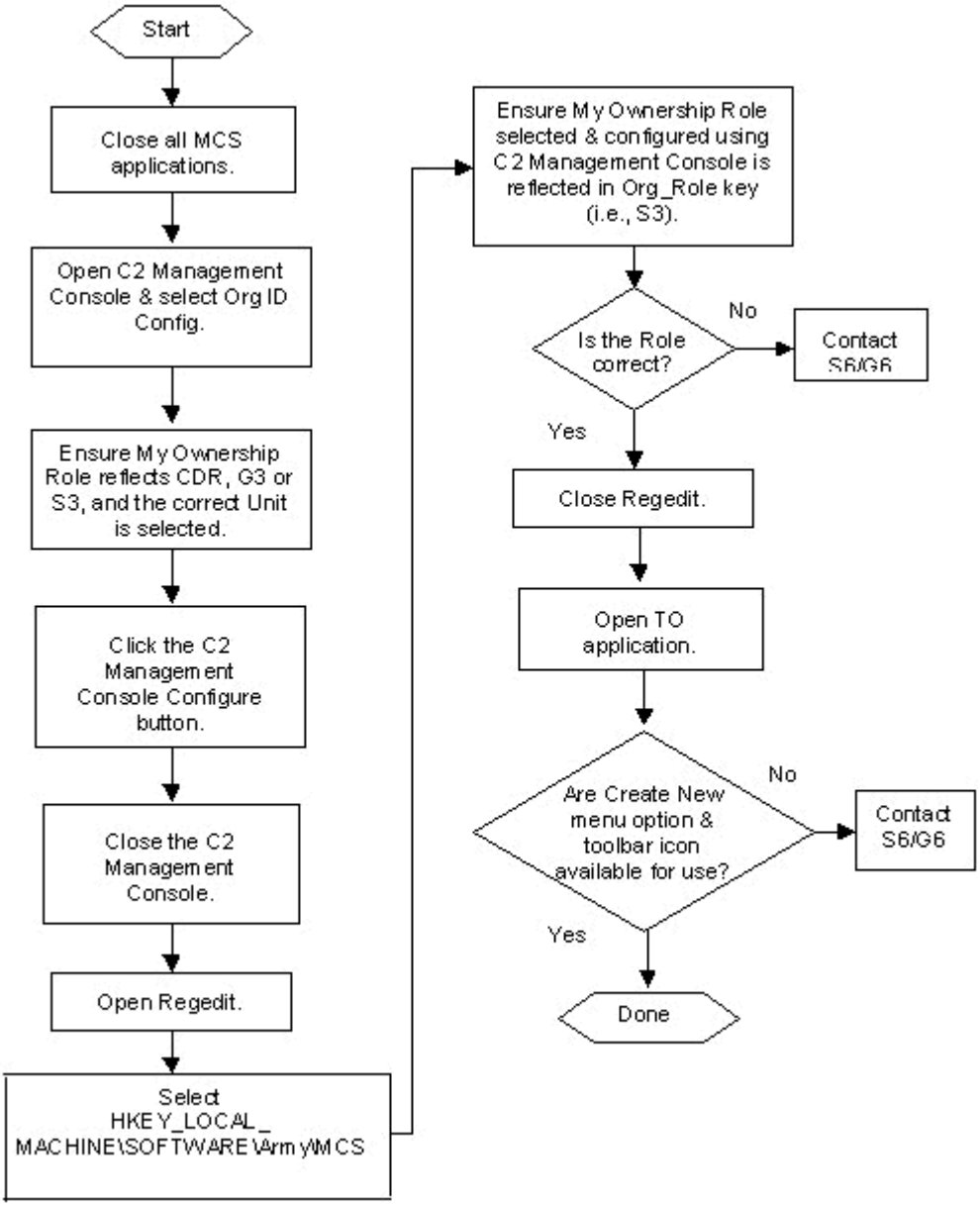


Figure 7-23 MAA Fault #14: Create Task Organization is Unavailable in Task Organization Application

7-15 Fault #15: MDMP Assistant Fails To Post to Unit Web Server

Information for Scenario Briefing:
The MCS Workstation is configured and has network connectivity.

Fault Symptoms:
The error “Publish to PASS Server could not post plan data to web server. Please make sure FTP settings are correct” or “Transfer failed. Please make sure FTP settings are correct” is returned.

Fault Solution:

MAU:

1. **Contact** the MAA.

MAA:

1. **Contact** the *S6/G6* to obtain the correct web server IP Address, folder, username, and password.
2. **Open** the *C2 Management Console* and **select** *Planning Config*.
3. **Ensure** that the *FTP (Web server)* settings are correct.
4. **Click** the *C2 Management Console Configure* button.
5. **Close** the *C2 Management Console* and start the *MDMP Assistan*t.
6. If successful, **inform** MAU to continue the mission.
7. If post to unit website fails, **contact** the S6/G6 for MCS Tech support

.

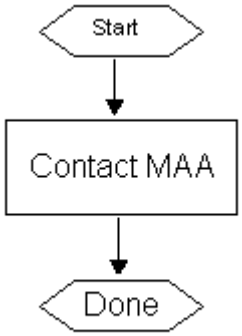


Figure 7-24 MAU Fault #15: MDMP Assistant Fails to Post to Unit Web Server

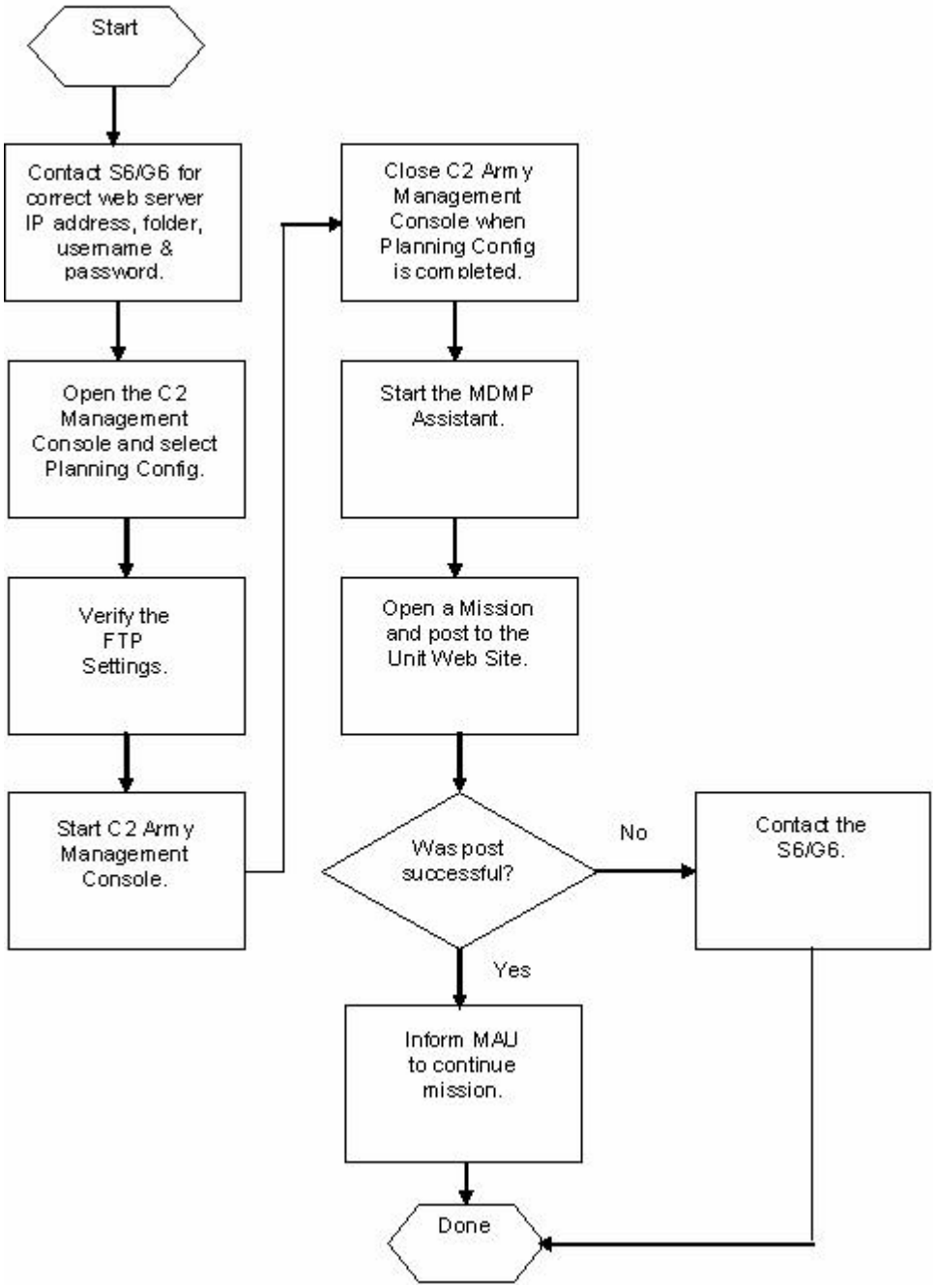


Figure 7-25 MAA Fault #15: MDMP Assistant Fails to Post to Web Server

7-16 Fault #16: System attempts to synchronize time to 1.2.3.4 and fails

Information for Scenario Briefing:
The MCS Workstation is properly configured for the LAN.

Fault Symptoms:

The MCS workstation or gateway displays a significantly different time from other BFA systems in the TOC.

Fault Solution:

MAU:

1. **Inform** the MAA that the time is not correct.

MAA:

1. **Close** all MCS applications.
2. **Open** the *C2 Management Console* and select *Time Config*.
3. **Enter** the *IP Address* of the appropriate time server, usually the PASS Server.
4. **Click** the *C2 Management Console Configure* button.
5. **Observe** the system time in the bottom right of the screen.
6. **Check** the time against the *Time Server* time. If correct, **inform** the MAU to continue the mission.
7. If the time sync fails, **contact** the S6/G6 for MCS Tech support.

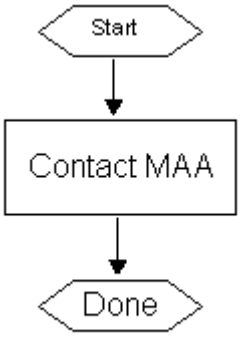


Figure 7-26 MAU Fault #16: System Attempts to Synchronize Time to 1.2.3.4 and Fails

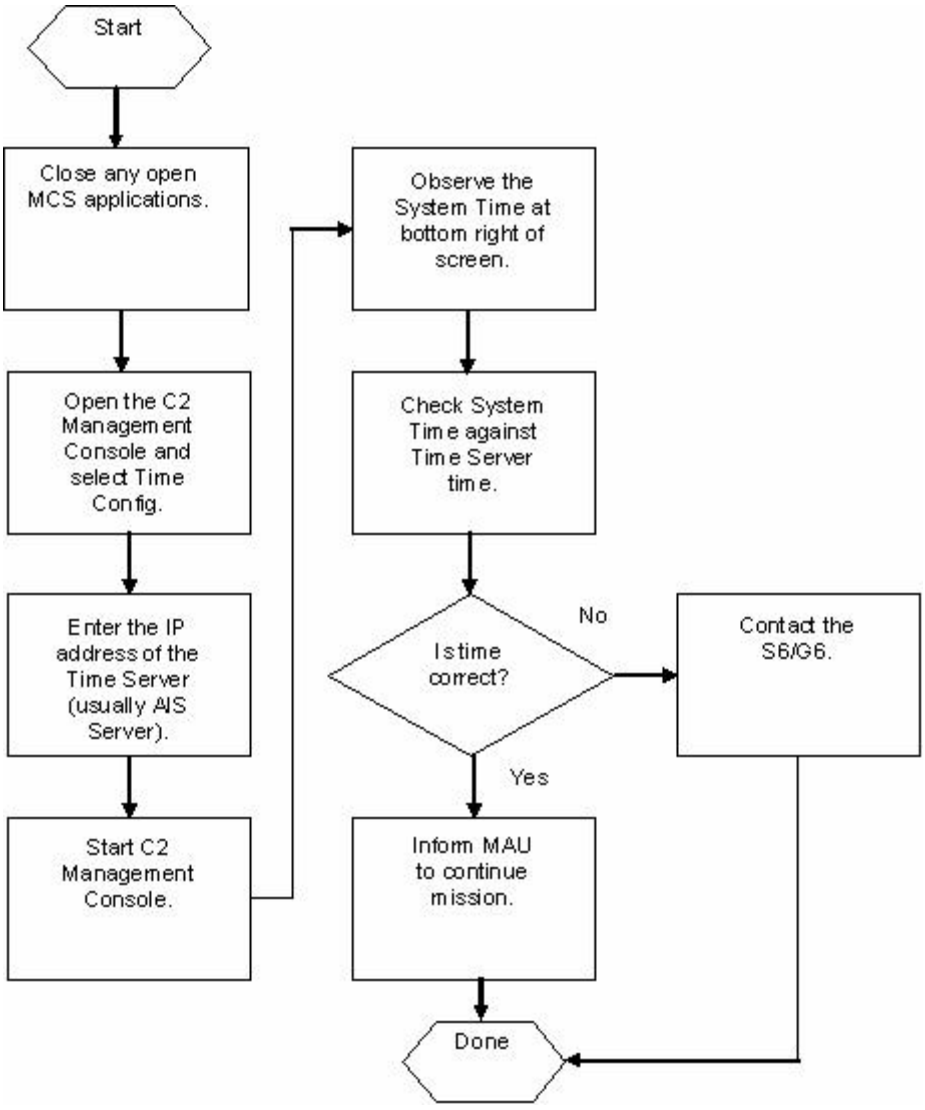


Figure 7-27 MAA Fault #16: System Attempts to Synchronize Time to 1.2.3.4 and Fails

7-17 Fault #17: JAVA error "Windows cannot find Javaw..."when attempting to start AFATDS

Information for Scenario Briefing:
The MCS Workstation was re-started prior to shift change and on start up displayed multiple JAVA errors.

Fault Symptoms:
MCS displays multiple JAVA errors similar to "Windows cannot find Javaw..." and all applications that use JAVA are inoperable.

Fault Solution:
MAU:

1. **Contact** the MAA.

MAA:

1. **Close** all MCS applications on the affected workstation.
2. **Open** *Windows Explorer* and navigate to C:\Program Files\Java\j2re1.4.1_05\bin. Ensure the jave.exe and javaw.exe files exist.
3. If the java files or directories do not exist, **open** *Windows Control Panel, Add* or *Remove Programs*, to check the Java 2 Runtime installation.
4. If Java 2 Runtime is shown, **highlight** the Java 2 Runtime Environment and **click** the *Change/Remove* button.
5. **Click** *OK* to confirm the file deletion.
6. **Insert** the MCS Installation CD 2 (CD 1a) or 4 of 5 (CD 2) into the CD-ROM drive.
7. Using *Windows Explorer*, **navigate** to the JRE141 folder on the CD-ROM.
8. **Double-click** *j2re-1_4_1_05-windows-i586.exe* and use the typical settings to install the Java 2 Runtime Environment.
9. When J2RE installation is complete, **reboot** *MCS*.
10. Upon restart, **check** the functionality of the *MCS* applications. If successful, **inform** the MAU to continue the mission.
11. If JAVA errors continue to appear, **contact** the S6/G6 for MCS Tech support.

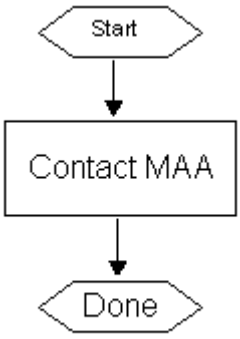


Figure 7-28 MAU Fault #17: System Displays Java Error “Windows cannot find javaw...” When Attempting to Start AFATDS

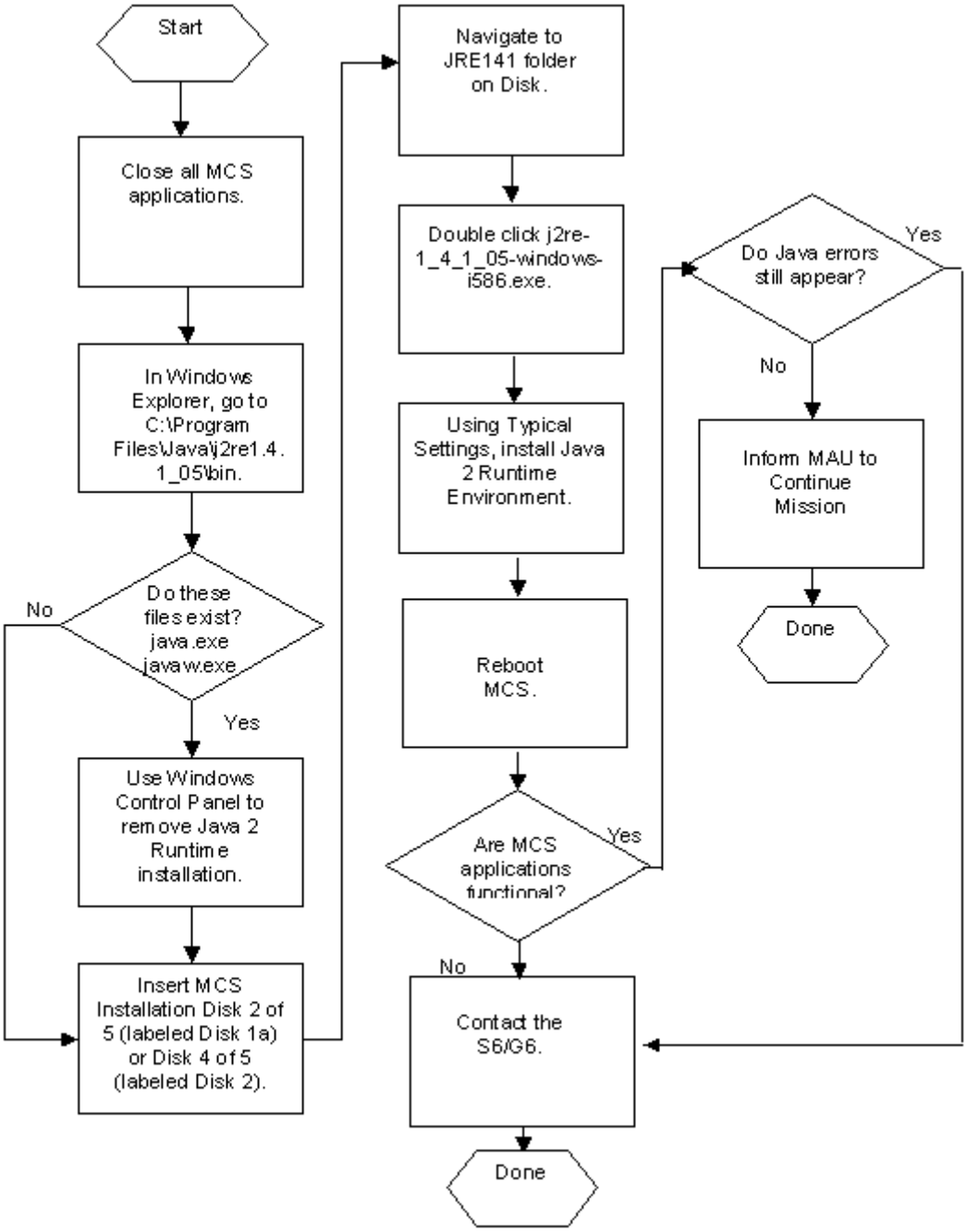


Figure 7-29 MAA Fault #17: System Displays Java Error, "Windows cannot find Javaw..." When Starting AFATDS.AXE

7-18 Fault #18: Maps missing from Map Manager, but available on the Hard Disk Drive

Information for Scenario Briefing:
The MCS workstation is properly configured for the TOC

Fault Symptoms:

Upon opening a Maps & Overlays Mission, the map background is gray and no maps are available with a right-click on the map area.

Fault Solution:

MAU:

1. **Open** Windows Explorer and **navigate** to the location of the maps (D:\Maps or D:\Emaps).
2. **Check** to ensure that sub-folders exist and that map files exist in the sub-folders (i.e. 0000v1r3.on2, etc.…). If sub-folders or files do not exist, contact the MAA.
3. **Open** Maps & Overlays if closed.
4. **Open** the *Map Manager,* if maps are not listed in the left pane, Maps; click the *Find Maps* icon in the toolbar.
5. **Navigate** in the *Browse* window for *Folder* area to the map folder location.
6. **Select** the folder and click *OK.* The *Map Manager* will read in the maps. The process of reading maps can take an extended period, depending on the number of maps on the system.
7. Once the process is complete, maps are shown in the left pane and shaded areas are shown in the right pane of the *Map Manager*.
8. If no maps or shaded areas appear, or if the process takes a very long time (approximately 30 minutes **contact** the *MAA*.

MAA:

1. If notified by the MAU that a map folder does not exist on the MCS, **use** the Map CD-ROMs to load maps in the appropriate sub-folders in D:\Maps or D:\Emaps.
2. **Utilize** the *Map Manager* to read in the appropriate maps.
3. When complete, **use** *Maps & Overlays* to ensure maps are available to the MAU. **Inform** the MAU to continue mission.
4. If maps fail to load into the *Map Manager* or the hard drive, **notify** the S6/G6 for MCS Tech support.

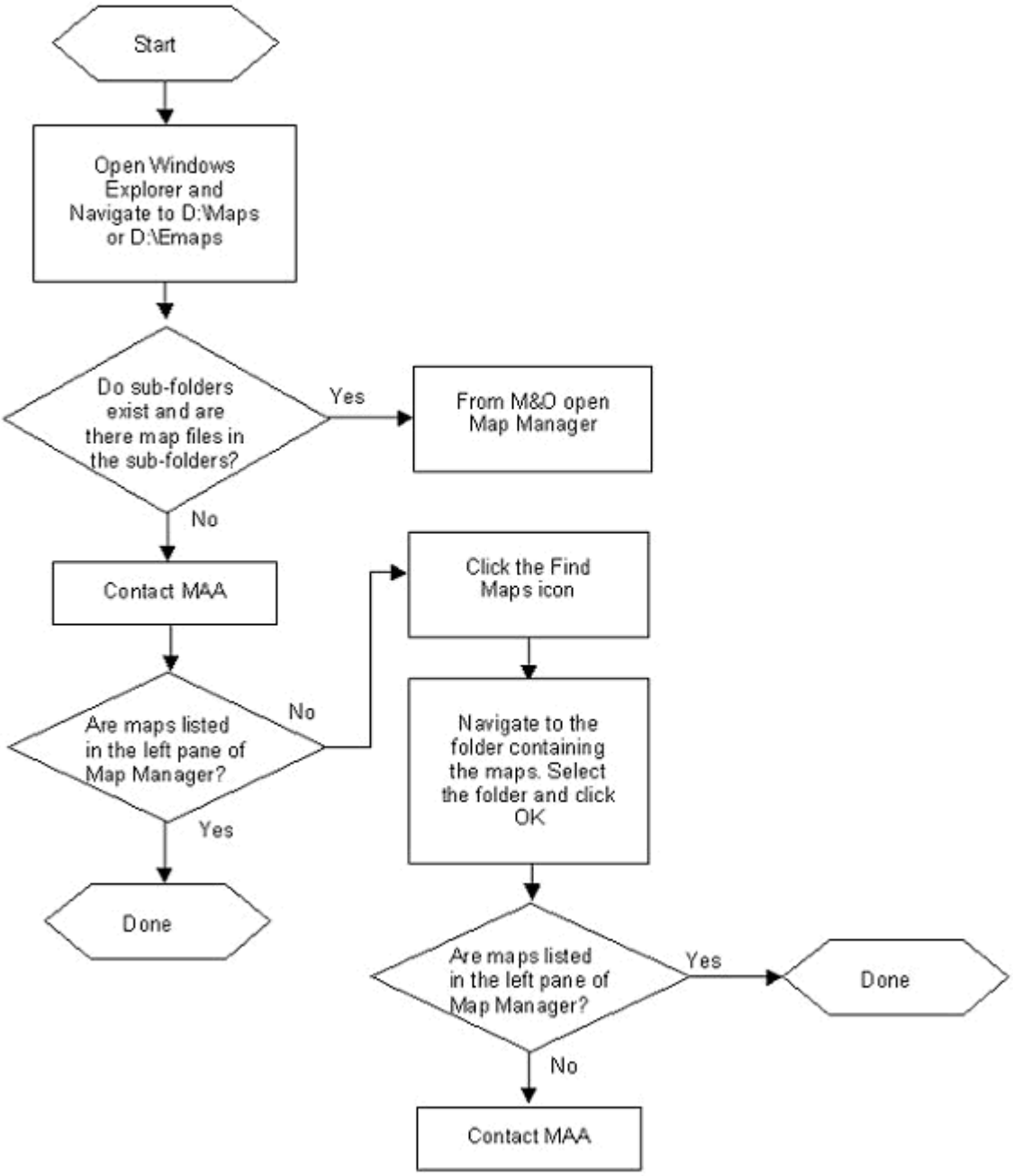


Figure 7-30 MAU Fault #18: Maps are Missing from Map Manager, But are Available on the System Hard Drive

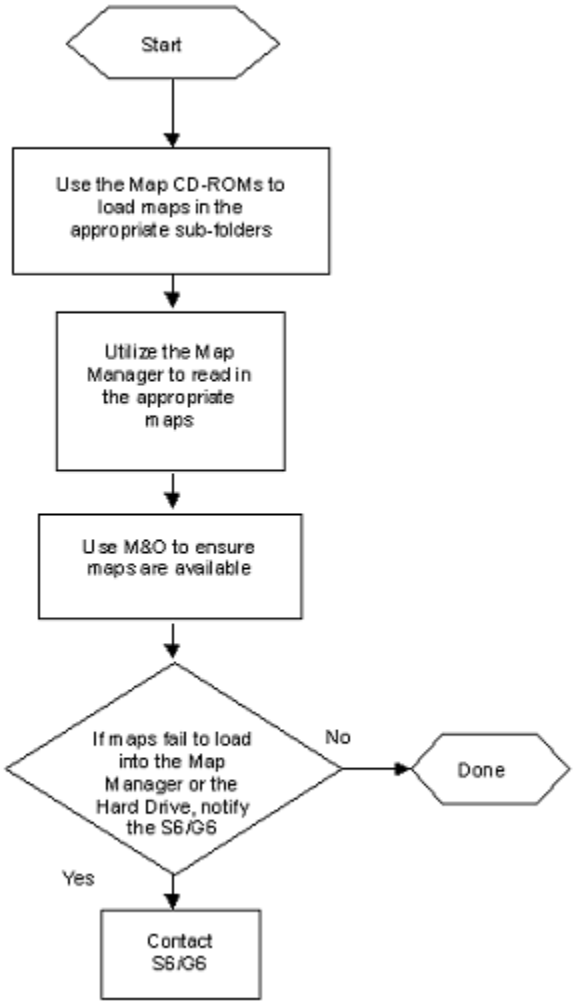


Figure 7-31 MAA Fault #18: Maps are Missing from Map Manager, But Available on the System Hard Drive

7-19 Fault #19: System Network Interface is disabled

Information for Scenario Briefing:
The MCS is properly configured for the TOC.

Fault Symptoms:
The MAU is unable to connect to any external data source.

Fault Solution:
MAU:

1. **Open** *Maps &* Overlays.
2. **Select** *Tools*, *Options* to open the *Options* window.
3. **Select** *PASS*, *Publishing*, and **click** the *Verify* button.
4. If the *PASS* connection fails, **contact** the MAA.

MAA:

1. **Close** all open applications.
2. Use the *Windows Control Panel*, *Network Connections* to **enable** the *Network Interface*.
3. Open the *C2 Management Console* and **select** *Data Source Config*.
4. **Select** the external *SQL Server Data Source* and **click** the *Test Data Source* button.
5. If the network connection is good, **inform** the MAU to continue mission.
6. If the network connection fails, **troubleshoot** the system LAN cabling and **contact** the S6/G6 for MCS Tech support.

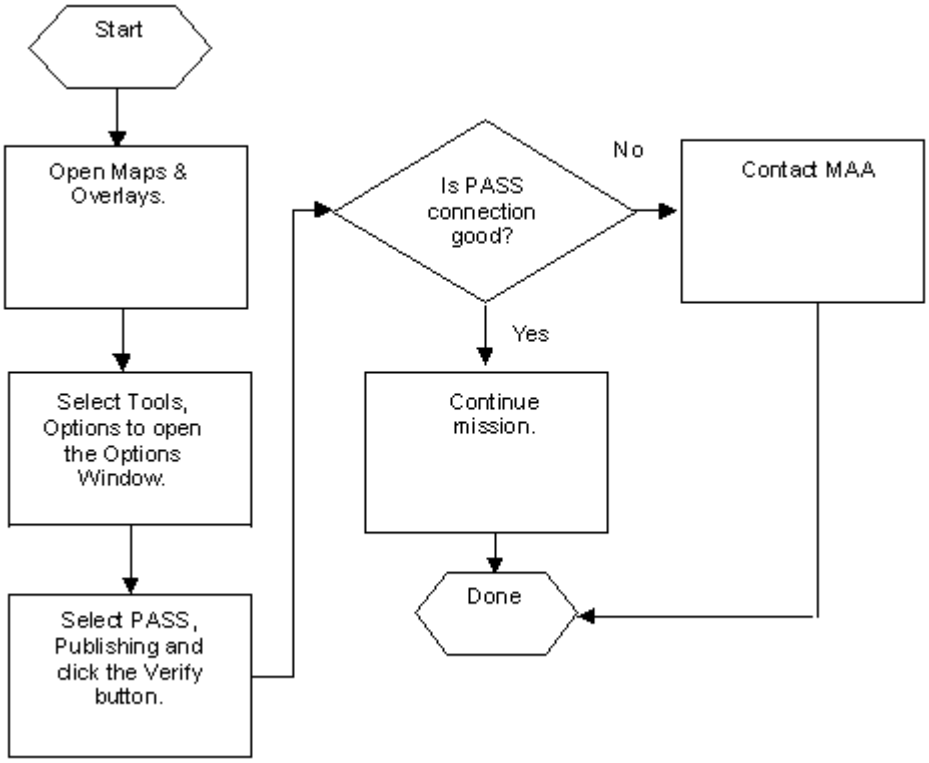


Figure 7-32 MAU Fault #19: System Network Interface is Disabled

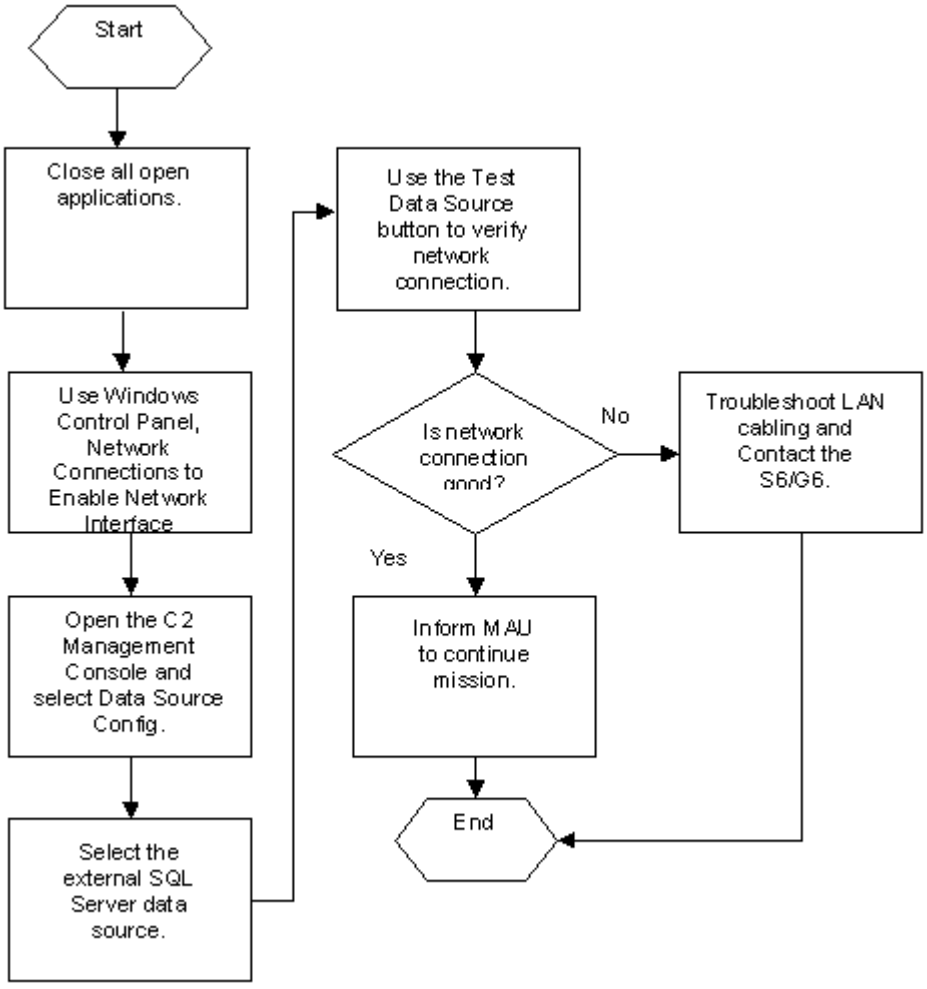


Figure 7-33 MAA Fault #19: System Network Interface is Disabled

7-20 Fault #20: Cannot receive Live Feed from C2PC/GCCS-A

Information for Scenario Briefing:
The MCS Gateway is properly configured to the TOC LAN.

Fault Symptoms:
The *NRTS GCCS Data Provider* displays zero objects received when viewed in the *NRTS Server Console*.

Fault Solution:
MAU:
This is a MCS Gateway fault. The MAU has no tasks.

MAA:

1. **Contact** the *C2PC/GCCS-A* operator to obtain the correct IP Address, username, and password for the MCS Gateway.
2. **Open** the *C2PC Gateway Manager* and select the *C2PC Gateway Options* (Tools, Options).
3. The *Master Password* should be blank, **click** *OK* to open the *C2PC Gateway Options*.
4. **Select** the *Data Source* tab.
5. **Select** the appropriate *Data Source*. The connection to the distant *C2PC or MCS Gateway* utilizes the *Gateway-to-Gateway* data source.
6. The *Gateway-to-Gateway* parameters are display in the bottom pane. **Highlight** the data source and click Edit.
7. **Ensure** the *Gateway Host IP*, *Type*, *Type Address*, and *Gateway Host Name* are correct for the distant C2PC/MCS Gateway.
8. If no *Gateway Host* is present, **click** the *Add* button.
9. **Enter** the correct *Gateway Host IP Address* and *Subnet Mask*.
10. **Click** the *Resolve* button. If the *DNS Server* can resolve the *C2PC/MCS Gateway IP Address*, the *Host Name* will populate, if not unknown will populate the *Host Name* box.
11. **Click** the *Add* button then click the *Apply* button to submit the changes.
12. **Click** the *OK* button and the *Gateway Options* window will close.
13. **Observe** the *C2PC Gateway Manager*, Gateway Status box.
14. If the connection is correct, the status will list *Connected* and the host name of the *C2PC/MCS Gateway*. If the *Status* switches from *Connecting to Not Connected*, **contact** the S6/G6 for MCS Tech support.
15. Once the *C2PC Gateway* is connected to the distant station, **right-click** the *TMS Broker* icon in the system tray and **select** *Send Full Picture*. **Enter** the appropriate user name and password if prompted.
16. **Observe** the *NRTS Server Console*, *GCCS Data Provider* to ensure the *Data Provider* processes incoming messages
17. The *NRTS GCCS Data Provider* should display objects in a short time (approximately 3 minutes), if not, **contact** the S6/G6 for MCS Tech support.

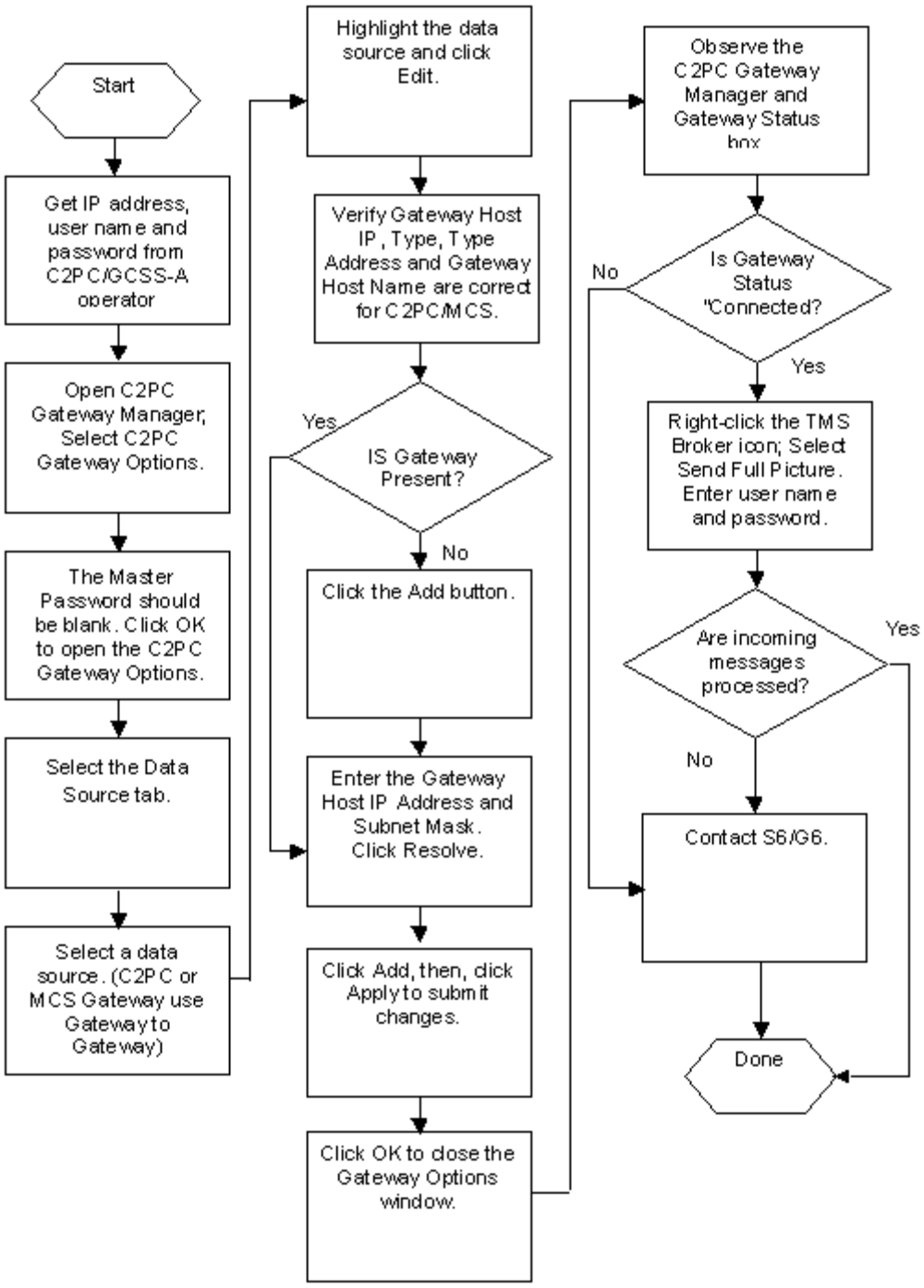


Figure 7-34 MAA Fault #20: Cannot Receive Live Feed from C2PC/GCCS-A

7-21 Fault #21: Cannot Import Overlay file (.xml) from ASAS-L

Information for Scenario Briefing:
The MCS Workstation is properly configured for the TOC.

Fault Symptoms:
No objects are available in the imported ASAS-L overlay.

Fault Solution:
MAU:

1. **Save** the *ASAS-L* overlay file to a location on the hard drive for the MAA.
2. **Inform** the MAA.

MAA:

1. **Open** *Windows Explorer* and **navigate** to the location of the saved *ASAS-L* overlay.
2. **Double-click** on the *overlay.xml* file to open with the default application, Internet Explorer.
3. **Check** the contents of the *ASAS-L overlay.xm*l to ensure the following words do not exist: *ELT Only.* Use *Find* to check for *ELT.*
4. If the words *ELT Only* exist in the *overlay.xml* file, the overlay was not exported to MCS format.
5. **Inform** the ASAS operator that he/she must export the file to MCS-Light format.
6. **Receive** the exported *ASAS-L* overlay and attempt to import and open the overlay in Maps & Overlays.
7. If the overlay is successfully imported and view, **inform** the MAU to continue mission.
8. If the overlay is not successfully imported and viewed, **contact** the S6/G6 for MCS Tech support

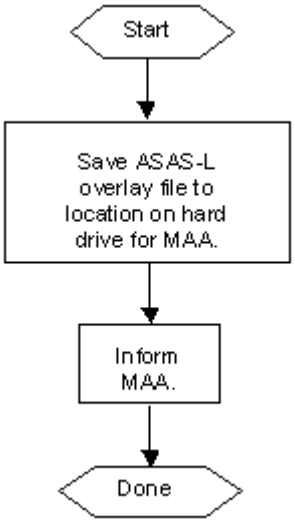


Figure 7-35 MAU Fault #21: Cannot Import Overlay File(.XML) from ASAS-L

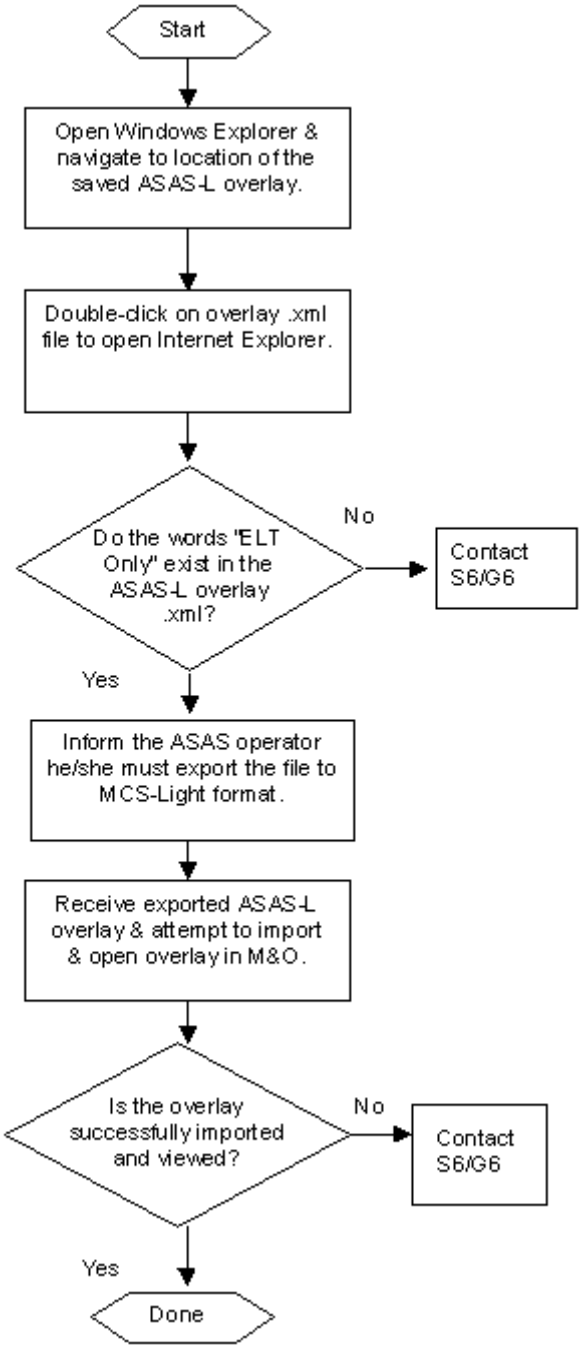


Figure 7-36 MAA Fault #21: Cannot Import Overlay File(.XML) from ASAS-L

7-22 Fault #22: System immediately shuts down on power up

Information for Scenario Briefing:
The TOC has just completed a jump. The MCS was properly configured to the TOC prior to the jump.

Fault Symptoms:

The MCS system immediately shuts down or does not finish powering up.

Fault Solution:
MAU:

1. **Check** the power supply to ensure the power supply is properly installed, and connected to a power source and the system.
2. **Check** the battery to ensure the battery is properly attached to the system and locked in place.
3. Attempt to **start** the system using the power button.
4. If system fails to start or immediately shuts down, **check** to ensure the proper power supply is in use.
5. If power supply is not correct, **replace** with proper power supply.
6. If power supply is correct and system will not start, **replace** with alternate correct power supply.
7. Attempt to **start** system using the power button.
8. If system fails to start, immediately shuts down, or continuously re-boots, **contact** the S6/G6 for MCS Tech support.

MAA:
No task for the MAA unless the system is the MCS Gateway.

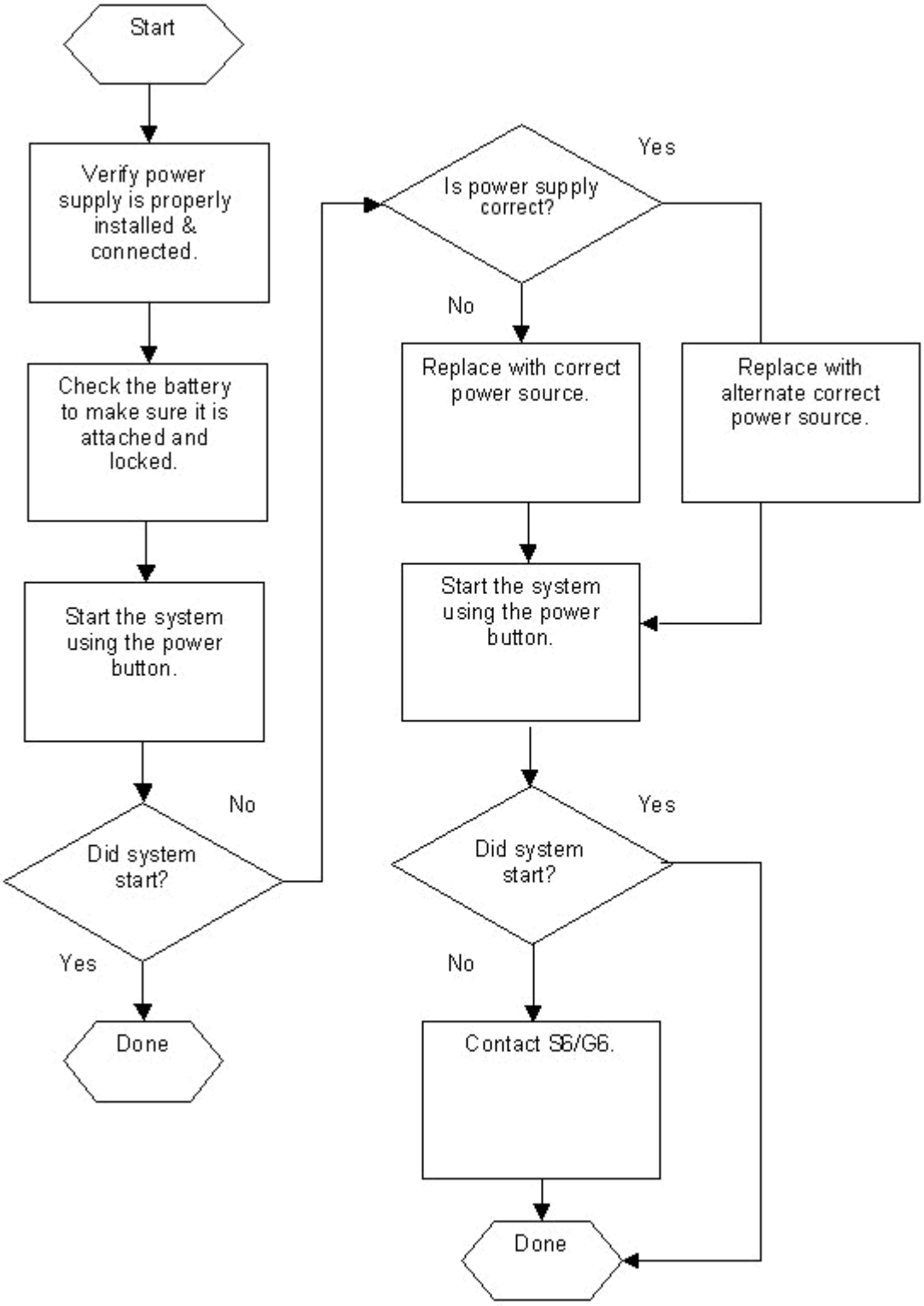


Figure 7-37 MAU Fault #22: System Immediately Shuts Down Upon Power Up

7-23 Fault #23: Prevent and Recover from Catastrophic Loss of Data

Information for Scenario Briefing:
The MCS is properly configured for the TOC. The S6/G6 has network storage available to the MAA.

Fault Symptoms:
Possible imminent failure of MCS HDD.

Fault Solution:
MAU:
No MAU tasks.

MAA:

1. **Coordinate** with the *S6/G6* for network storage.
2. **Map** a network drive to the location of the network storage.
3. **Start** the *Microsoft Backup Utility* (*Accessories, System Tools, Backup*).
4. **Click** *Next* to use the *Backup* or *Restore Wizard*.
5. **Select** the radio button for *Backup files and settings* and **click** *Next*.
6. **Select** the radio button for *Let me choose what to back up* and **click** *Next*.
7. **Select** the *D:\MCS\Shared\Data* folder, ensure that the complete contents of the folder are selected, and **click** *Next*.
8. **Browse** for the mapped network storage location.
9. **Enter** a descriptive name for the backup file (i.e. MCSG3OPS1), and **click** *Next*.
10. **Ensure** that the information shown in *Completing the Backup or Restore Wizard* is correct and **click** *Finish*.
11. **Backup** will start and display the progress of the backup job.
12. When *Backup and Restore* is complete, **view** the report to ensure that the folders/files were backed up without errors.
13. **Close** the *Backup* window.
14. **Notify** the S6/G6 of the backup.

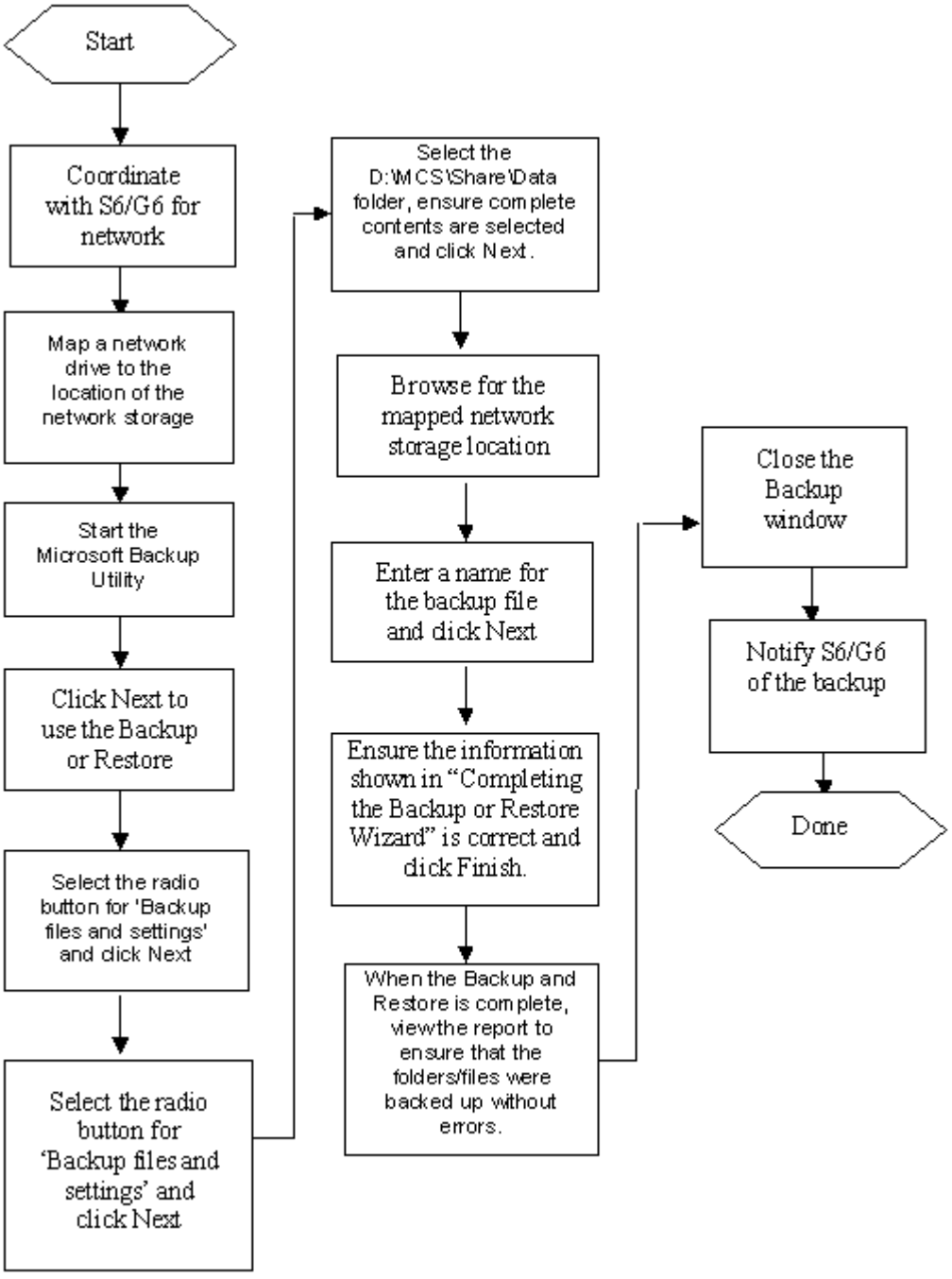


Figure 7-38 MAA Fault #23: Prevent and Recover from Catastrophic Loss of Data

MCS Configuration Preparation Check List

Configuring the MCS system requires site dependent information to ensure the correct operation of MCS. The following table provides a list of the required configuration parameters. Completing this list of site dependent parameters prior to installing MCS is highly recommended. The SA will provide the necessary information to the MAA to complete the installation of the MCS gateway and workstation.

Table 1-1 MCS Installation Path Workstation

MCS Installation Configuration Parameters	Site dependent parameter setting
MCS - Installation path	

MCS Installation Path - Workstation

Table 1-2 MCS Data Source Access DB - Workstation

Data Source (Access DB)	Site dependent parameter settings
DataSource, DataSourceLocation DataSourceName	
Database Settings, DatabaseName DatabaseType SchemaDefinition	

Data Source ACCESS DB - Workstation

Table 1-3 MCS Data Source SQL DB - Workstation

Data Source (SQL DB)	Site dependent parameter setting
Data Source DataSourceLocation DataSourceName	
Database Settings DatabaseName DatabaseType OdbcDatabase SchemaDefinition	

Server Settings, DatabasePwd DatabaseUserName ServerHostName ServerIpAddress	

Data Source (SQL DB) - Workstation

Table 1-4 MCS Organization ID - Workstation

Org ID Configuration Settings	Site dependent parameter settings
TO Data Source	
TO Name	
My Ownership Role	
Service	
Country	
My Unit	
Add Roles	
Delete Roles	

Org ID setting - Workstation

Table 1-5 Messaging from local hostlist.txt file - Workstation

Messaging Configuration Settings	Site dependent parameter settings
Role	
URN	
Long Hostname	
OR Name	
Group	

BFA	

Table 1-6 Messaging from C2R - Workstation

Messaging Configuration Settings	Site dependent parameter settings
C2R Server IP Address	
DNS Server Address	
C2R Settings Domain Unit Role	

Messaging from C2R Server - Workstation

Table 1-7 MCS Gateway Configuration - Workstation

Gateway Configuration Settings	Site dependent parameter settings
NRTS IP Address	
NRTS MCast IP Address	
Full Picture Port (TCP)	
Update Port (UDP)	
Injection Port	

Gateway Configuration - Workstation

Table 1-8 MCS PASS Configuration - Workstation

PASS Configuration Settings	Site dependent parameter settings
Pass Client Configuration	
Pass Server IP Address	
Pass SSL Port	
User Name	

User Password	
LAN Settings Proxy Server Address: Port: Bypass proxy server for local address Local IP Addresses Use SSL Authentication Pass Server Port	

PASS Client Settings - Workstation

Table 1-9 MCS Planning - Workstation

Planning Configuration Settings	Site dependent parameter settings
Web Server Settings	
Web Server	
Directory	
User ID	
Password	

Planning Settings - Workstation

Table 1-10 MCS Security Settings - Workstation

Security Configuration Settings	Site dependent parameter settings
Directories:	
c:\	
c:\h\	
c:\Temp\	
c:\Program Files\	
c:\WINDOWS\system32\	
c:\WINDOWS\system32\drivers\etc\	
d:\MCS\	

Files:	
c:\autoexec.bat	
c:\ntldr	
c:\WINDOWS\regedit.exe	
c:\WINDOWS\system32\regedt32.exe	
Registry Keys:	
HKEY_LOCAL_MACHINE\SOFTWARE\ARMY	
HKEY_LOCAL_MACHINE\SOFTWARE\BCS3 Client	
HKEY_LOCAL_MACHINE\SOFTWARE\Bruhn NewTech	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes	
HKEY_LOCAL_MACHINE\SOFTWARE\COE	
HKEY_LOCAL_MACHINE\SOFTWARE\DTSS	
HKEY_LOCAL_MACHINE\SOFTWARE\ESRI	
HKEY_LOCAL_MACHINE\SOFTWARE\ FutureSkies	
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft	
HKEY_LOCAL_MACHINE\SOFTWARE\MapInfo	
HKEY_LOCAL_MACHINE\SOFTWARE\MCS Engineer	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman Information Technology, TASC	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman TASC	

HKEY_LOCAL_MACHINE\SOFTWARE\ODBC	
HKEY_LOCAL_MACHINE\SOFTWARE\PM Common Software	
HKEY_LOCAL_MACHINE\SOFTWARE\PE C3S	
HKEY_LOCAL_MACHINE\SOFTWARE\Schlumberger	
HKEY_LOCAL_MACHINE\SOFTWARE\Secure	
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec	
HKEY_LOCAL_MACHINE\SOFTWARE\Stingray Software, Inc.	
HKEY_LOCAL_MACHINE\SOFTWARE\US ARMY CECOM	
HKEY_LOCAL_MACHINE\SOFTWARE\Army\ MCS	
System Classification	
Banner Classification Label Text	

Security Settings - Workstation

Table 1-11 MCS Time Sync Server - Workstation

Time Configuration Settings	Site dependent parameter settings
Enable Time Sync	
Server IP Address	
Time Sync Role	
Client	
Server	
Slave Server	

Time Sync Server - Workstation

Table 1-12 MCS Autosetup Utility - Workstation

AutoSetup Utility Settings	Site dependent parameter settings
Configure Multicast Address: Multicast Port: Broadcast Server Test Interval Fail Over After Minutes of Bad Comms	

DataSources
Database:
HostName:
Ip_Address:
Provider:
Server_type_name:
SourceName:
Username:

NRTS
Primary
Host IP Address:
Injection Port:
Full Picture Port:
Update Port:
MultiCast Address:
Secondary
Host IP Address:
Injection Port:
Full Picture Port:
Update Port:
MultiCast Address:

PASS
Primary
Host IP Address:
HTTP Port:
HTTP Port:
Use Pass Authentication and SSL
Secondary
Host IP Address:
HTTP Port:
HTTP Port:
Use Pass Authentication and SSL

Other
Time Server IP:
Web Server URL:
Security Classification:
Banner Label:

Table 1-13 MCS Installation Path - Gateway

MCS Installation Configuration Parameters	Default parameter setting	Site dependent parameter setting
MCS - Installation path	d:\MCS	

MCS Installation Path - Gateway

Table 1-14 MCS Data Source Access DB - Gateway

Data Source (Access DB)	Site dependent parameter settings
DataSource, DataSourceLocation DataSourceName	
Database Settings, DatabaseName DatabaseType SchemaDefinition	

Data Source ACCESS DB - Gateway

Table 1-15 MCS Data Source SQL DB - Gateway

Data Source (SQL DB)	Site dependent parameter setting
Data Source DataSourceLocation DataSourceName	
Database Settings DatabaseName DatabaseType OdbcDatabase SchemaDefinition	
Server Settings, DatabasePwd DatabaseUserName ServerHostName ServerIpAddress	

Data Source (SQL DB) - Gateway

Table 1-16 MCS Organization ID - Gateway

Org ID Configuration Settings	Site dependent parameter settings
TO Data Source	

TO Name	
My Ownership Role	
Service	
Country	
My Unit	
Add Roles	
Delete Roles	

Org ID setting - Gateway

Table 1-17 MCS Gateway Configuration - Gateway

Gateway Configuration Settings	**Site dependent parameter settings**
NRTS IP Address:	
Full Picture Port (TCP):	
Injection Port:	
NRTS MCast IP Add:	
Update Port (UDP):	
MaxMCast Pkt Size:	
C2PC Gateway:	
Gateway IP Address:	
TCP/UDP Port:	
Subnet Mask:	
Multi-tiered TCP/UDP Port:	

Multicast IP Address:	
Multicast TCP/UDP Port:	
Use IP Multicast	
Password	

Gateway Configuration - Gateway

Table 1-18 MCS PASS Configuration - Gateway

PASS Configuration Settings	Site dependent parameter settings
Pass Client Configuration	
PASS Server IP Address	
Pass SSL Port	
User Name	
User Password	
LAN Settings Proxy Server Address: Port: Bypass proxy server for local address Local IP Addresses Use SSL Authentication Pass Server Port	

PASS Client Settings - Gateway

Table 1-19 MCS Planning - Gateway

Planning Configuration Settings	Site dependent parameter settings
Web Server Settings	
Web Server:	
Directory:	
User ID:	
Password:	

Planning Settings - Gateway

Table 1-20 MCS Security Settings - Gateway

Security Configuration Settings	Site dependent parameter settings
Directories:	
c:\	
c:\h\	
c:\Temp\	
c:\Program Files\	
c:\WINDOWS\system32\	
c:\WINDOWS\system32\drivers\etc\	
d:\MCS\	
Files:	
c:\autoexec.bat	
c:\ntldr	
c:\WINDOWS\regedit.exe	
c:\WINDOWS\system32\regedt32.exe	
Registry Keys:	
HKEY_LOCAL_MACHINE\SOFTWARE\ARMY	
HKEY_LOCAL_MACHINE\SOFTWARE\BCS3 Client	
HKEY_LOCAL_MACHINE\SOFTWARE\Bruhn NewTech	

HKEY_LOCAL_MACHINE\SOFTWARE\Classes	
HKEY_LOCAL_MACHINE\SOFTWARE\COE	
HKEY_LOCAL_MACHINE\SOFTWARE\DTSS	
HKEY_LOCAL_MACHINE\SOFTWARE\ESRI	
HKEY_LOCAL_MACHINE\SOFTWARE\ FutureSkies	
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft	
HKEY_LOCAL_MACHINE\SOFTWARE\MapInfo	
HKEY_LOCAL_MACHINE\SOFTWARE\MCS Engineer	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman Information Technology, TASC	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman TASC	
HKEY_LOCAL_MACHINE\SOFTWARE\ODBC	
HKEY_LOCAL_MACHINE\SOFTWARE\PM Common Software	
HKEY_LOCAL_MACHINE\SOFTWARE\PE C3S	
HKEY_LOCAL_MACHINE\SOFTWARE\Schlumberger	
HKEY_LOCAL_MACHINE\SOFTWARE\Secure	
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec	
HKEY_LOCAL_MACHINE\SOFTWARE\Stingray Software, Inc.	
HKEY_LOCAL_MACHINE\SOFTWARE\US ARMY CECOM	

HKEY_LOCAL_MACHINE\SOFTWARE\Army\ MCS	
System Classification	
Banner Classification Label Text	

Security Settings - Gateway

Table 1-21 MCS Time Sync Server - Gateway

Time Configuration Settings	Site dependent parameter settings
Enable Time Sync	
Server IP Address	
Time Sync Role	
Client	
Server	
Slave Server	

Time Sync Server – Gateway

Table 1-22 AutoSetup - Gateway

AutoSetup Utility Settings	Site dependent parameter settings
Run EZ PASS on this Server	Do not connect NRTS to PASS / Connect NRTS to PASS Server
PASS Server Settings	
HTTPS Port	
IP Address	
User Name	
Password	

The following parameters are located using the Server Configuration Console.

Table 1-23 Configure PASS Server – Gateway

PASS Configuration Settings	Site dependent parameter settings
Run EZ PASS on this Server	
HTTPS Port	
Persist PASS Data to Disk:	
HTTP Port:	
Require Authentication:	

Authentication Type:

NT Domain:

PASS Read Group:

PASS Write Group:

LDAP Host:

LDAP Port:

LDAP Base DN:

Table 1-24 Configure NRTS Server - Gateway

NRTS Configuration Settings	Site dependent parameter settings
Multicast (UDP) Settings IP Address: Update Port: Packet Size: Time to Live (TTL)	
TCP Settings Full Picture Port: Injection Port:	
NRTS to PASS Network Settings Connect NRTS to PASS Server IP Address HTTPS Port Username Password	

Table 1-25 Incoming Data, Lower Echelons (FBCB2) - Gateway

Lower Echelons Configuration Settings	Site dependent parameter settings
Receive FBCB2 Data From	None PASS SA (Multicast Data0) [select one]
Type of objects to receive from FBCB2	UNIT_PLATFORM GEO_REPORT SPOT [select 0 to 3]
Multicast Group Settings IP Address: Port:	

Add Multicast Group(s)

Remove Multicast Group(s)

Table 1-26 Incoming Data, Higher Echelons (GCCS) - Gateway

Higher Echelons Configuration Settings	Site dependent parameter settings
Receive GCCS Data From	None PASS Gateway Manager [select one]
Topics	

Table 1-27 Incoming Data, Fires (AFATDS) - Gateway

Fires Configuration Settings	Site dependent parameter settings
Receive AFATDS Data From	None PASS AFATDS Client (AXE interface) [select one]
Type of objects to receive	UNIT TARGET GEOMETRY AIR_SUPPORT_REQUEST [select 0 to 4]
Network Settings NRTS Listening Port: AXE Listening Port: AFATDS Server IP Address: Username: Password: AFATDS Server Classification:	

Table 1-28 Incoming Data, AMDWS Data Provider - Gateway

Air Defense (AMDWS)	Site dependent parameter settings
Receive AMDWS Air Defense Data From:	None PASS AMDWS Client [select one]
Types of objects to receive from AMDWS:	AIRCRAFT MISSLE [select one]
AMDWS Client Configuration AMDWS Server IP Address: Port: AMDWS Admin Tool Web Site:	
AMDWS Client Ports Air Breather(AB) Listen Port: Tactical Ballistic Missile(TBM) Listen Port:	

Table 1-29 Incoming Data, Correlated Enemy (ASAS) - Gateway

Correlated Enemy Configuration Settings	Site dependent parameter settings
Receive ASAS Data From	None PASS [select one]
PASS ASAS Topic(s) to subscribe to	

Table 1-30 Outgoing Data, Lower Echelons (FBCB2) - Gateway

Lower Echelons Configuration Settings	Site dependent parameter settings
Type of object to inject into FBCB2:	UNIT PLATFORM NBC_ALERT SPOT OBSTACLE GEOMETRY [select 0 to all]
Messaging Settings Use Messaging URN Originating URN Injection TTL:	
Multicast Group Settings IP Address: Port: Message Header Type: ADD Multicast IP Address(s) Remove Multicast IP Address(s)	

Table 1-31 Outgoing Data, Higher Echelons (GCCS) - Gateway

Higher Echelons Configuration Settings	Site dependent parameter settings
Type of system data to inject into GCCS:	FBCB2 AFATDS BCS3 COALITION AMDWSUNIT MCS [select 0 to all]
Type of objects to inject into GCCS:	UNIT SPOT PLATFORM

	OBSTACLE NBC_ALERT GEOMETRY [select 0 to all]

Table 1-32 Outgoing Data, PASS - Gateway

PASS Outgoing Data Configuration Settings	Site dependent parameter settings
Type of objects to inject into PASS	UNIT PLATFORM NBC_ALERT SPOT OBSTACLE GEOMETRY
ADD PASS Topic(s)	
Remove PASS Topic(s)	

Table 1-33 Server Startup Options - Gateway

Set Server Startup Options	Site dependent parameter settings
Run the MCS Services Startup tool automatically when you login to this computer	
Create a desktop shortcut for the MCS Services Startup Tool	
Automatic Startup Selection Message Data Replicator Live Feed Database Utility PASS Service Database Management Utility PASS Administrator NRTS Service	

Table 1-34 MCS Installation Path - Server

MCS Installation Configuration Parameters	Site dependent parameter setting

MCS - Installation path	

MCS Installation Path - Server

Table 1-35 MCS Data Source Access DB - Server

Data Source (Access DB)	Site dependent parameter settings
DataSource, DataSourceLocation DataSourceName	
Database Settings, DatabaseName DatabaseType SchemaDefinition	

Data Source ACCESS DB - Server

Table 1-36 MCS Data Source SQL DB - Server

Data Source (SQL DB)	Site dependent parameter setting
Data Source DataSourceLocation DataSourceName	
Database Settings DatabaseName DatabaseType OdbcDatabase SchemaDefinition	
Server Settings, DatabasePwd DatabaseUserName ServerHostName ServerIpAddress	

Data Source (SQL DB) - Server

Table 1-37 MCS Organization ID - Server

Org ID Configuration Settings	Site dependent parameter settings
TO Data Source	

TO Name	
My Ownership Role	
Service	
Country	
My Unit	
Add Roles	
Delete Roles	

Org ID setting - Server

Table 1-38 MCS Gateway Configuration - Server

Gateway Configuration Settings	**Site dependent parameter settings**
NRTS IP Address:	
Full Picture Port (TCP):	
Injection Port:	
NRTS MCast IP Add:	
Update Port (UDP):	
MaxMCast Pkt Size:	
C2PC Gateway:	
Gateway IP Address:	
TCP/UDP Port:	
Subnet Mask:	
Multi-tiered TCP/UDP Port:	

Multicast IP Address:	
Multicast TCP/UDP Port:	
Use IP Multicast	
Password	

Gateway Configuration - Server

Table 1-39 MCS PASS Configuration - Server

PASS Configuration Settings	Site dependent parameter settings
Pass Client Configuration	
PASS Server IP Address	
Pass SSL Port	
User Name	
User Password	
LAN Settings Proxy Server Address: Port: Bypass proxy server for local address Local IP Addresses Use SSL Authentication Pass Server Port	

PASS Client Settings - Server

Table 1-40 MCS Planning - Server

Planning Configuration Settings	Site dependent parameter settings
Web Server Settings	
Web Server:	
Directory:	
User ID:	
Password:	

Planning Settings - Server

Table 1-41 MCS Security Settings - Server

Security Configuration Settings	Site dependent parameter settings
Directories:	
c:\	
c:\h\	
c:\Temp\	
c:\Program Files\	
c:\WINDOWS\system32\	
c:\WINDOWS\system32\drivers\etc\	
d:\MCS\	
Files:	
c:\autoexec.bat	
c:\ntldr	
c:\WINDOWS\regedit.exe	
c:\WINDOWS\system32\regedt32.exe	
Registry Keys:	
HKEY_LOCAL_MACHINE\SOFTWARE\ARMY	
HKEY_LOCAL_MACHINE\SOFTWARE\BCS3 Client	
HKEY_LOCAL_MACHINE\SOFTWARE\Bruhn NewTech	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes	
HKEY_LOCAL_MACHINE\SOFTWARE\COE	

HKEY_LOCAL_MACHINE\SOFTWARE\DTSS	
HKEY_LOCAL_MACHINE\SOFTWARE\ESRI	
HKEY_LOCAL_MACHINE\SOFTWARE\ FutureSkies	
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft	
HKEY_LOCAL_MACHINE\SOFTWARE\MapInfo	
HKEY_LOCAL_MACHINE\SOFTWARE\MCS Engineer	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman Information Technology, TASC	
HKEY_LOCAL_MACHINE\SOFTWARE\Northrop Grumman TASC	
HKEY_LOCAL_MACHINE\SOFTWARE\ODBC	
HKEY_LOCAL_MACHINE\SOFTWARE\PM Common Software	
HKEY_LOCAL_MACHINE\SOFTWARE\PE C3S	
HKEY_LOCAL_MACHINE\SOFTWARE\Schlumberger	
HKEY_LOCAL_MACHINE\SOFTWARE\Secure	
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec	
HKEY_LOCAL_MACHINE\SOFTWARE\Stingray Software, Inc.	
HKEY_LOCAL_MACHINE\SOFTWARE\US ARMY CECOM	
HKEY_LOCAL_MACHINE\SOFTWARE\Army\ MCS	
System Classification	

Banner Classification Label Text	

Security Settings - Server

Table 1-42 MCS Time Configuration Settings - Server

Time Configuration Settings	Site dependent parameter settings
Enable Time Sync	
Server IP Address	
Time Sync Role	
Client	
Server	
Slave Server	

Time Sync Server - Server

Table 1-43 Configure PASS Server - Server

PASS Configuration Settings	Site dependent parameter settings
Run EZ PASS on this Server	
HTTP Port	
HTTPS Port:	
Persist PASS Data to Disk:	
Require Authentication:	
Authentication Type:	
NT Domain:	
PASS Read Group:	
PASS Write Group:	
LDAP Host:	

LDAP Port:	
LDAP Base DN:	

Table 1-44 Configure NRTS Server - Server

NRTS Configuration Settings	Site dependent parameter settings
Multicast (UDP) Settings IP Address: Update Port: Packet Size: Time to Live (TTL)	
TCP Settings Full Picture Port: Injection Port:	
NRTS to PASS Network Settings Connect NRTS to PASS Server IP Address HTTPS Port Username Password	

Table 1-45 Incoming Data, Lower Echelons (FBCB2) - Server

Lower Echelons Configuration Settings	Site dependent parameter settings
Receive FBCB2 Data From	None PASS SA (Multicast Data0) [select one]
Type of objects to receive from FBCB2	UNIT_PLATFORM GEO_REPORT SPOT [select 0 to 3]
Multicast Group Settings IP Address: Port:	
Add Multicast Group(s)	

Remove Multicast Group(s)

Table 1-46 Incoming Data, Higher Echelons (GCCS) - Server

Higher Echelons Configuration Settings	Site dependent parameter settings
Receive GCCS Data From	None PASS Gateway Manager [select one]
Topics	

Table 1-47 Incoming Data, Fires (AFATDS) - Server

Fires Configuration Settings	Site dependent parameter settings
Receive AFATDS Data From	None PASS AFATDS Client (AXE interface) [select one]
Type of objects to receive	UNIT TARGET GEOMETRY AIR_SUPPORT_REQUEST {select 0 to 4]
Network Settings NRTS Listening Port: AXE Listening Port: AFATDS Server IP Address: Username: Password: AFATDS Server Classification:	

Table 1-48 Incoming Data, Air Defense (AMDWS) - Server

Air Defense Configuration Settings	Site dependent parameter settings

Receive AMDWS Air Defense data from	None PASS AMDWS Client [select one]
Types of objects to receive from AMDWS	AIRCRAFT MISSILE {select 0 to 2]
AMDWS Client Configuration AMDWS Server IP Address Port	
AMDWS Client Ports Air Breather(AB) Listen Port Tactical Ballistic Missile(TBM) Listen Port	

Table 1-49 Incoming Data, Correlated Enemy (ASAS) - Server

Correlated Enemy Configuration Settings	**Site dependent parameter settings**
Receive ASAS Data From	None PASS [select one]
PASS ASAS Topic(s) to subscribe to	

Table 1-50 Outgoing Data, Lower Echelons (FBCB2) - Server

Lower Echelons Configuration Settings	**Site dependent parameter settings**
Type of object to inject into FBCB2:	UNIT PLATFORM NBC_ALERT SPOT OBSTACLE GEOMETRY [select 0 to all]
Messaging Settings Use Messaging URN Originating URN Injection TTL:	

Multicast Group Settings IP Address: Port: Message Header Type: ADD Multicast IP Address(s) Remove Multicast IP Address(s)	

Table 1-51 Outgoing Data, Higher Echelons (GCCS) - Server

Higher Echelons Configuration Settings	**Site dependent parameter settings**
Type of system data to inject into GCCS:	FBCB2 AFATDS BCS3 COALITION AMDWSUNIT MCS [select 0 to all]
Type of objects to inject into GCCS:	UNIT SPOT PLATFORM OBSTACLE NBC_ALERT GEOMETRY [select 0 to all]

Table 1-52 Outgoing Data, PASS - Server

PASS Outgoing Data Configuration Settings	**Site dependent parameter settings**
Type of objects to inject into PASS	UNIT PLATFORM NBC_ALERT SPOT OBSTACLE GEOMETRY
ADD PASS Topic(s)	
Remove PASS Topic(s)	

Table 1-53 Startup Options - Server

Set Server Startup Options	**Site dependent parameter settings**

Run the MCS Services **Startup tool automatically when you login to this computer**	
Create a desktop shortcut for the MCS Services Startup Tool	
Automatic Startup Selection Message Data Replicator Live Feed Database Utility PASS Service Database Management Utility PASS Administrator NRTS Service	

Acronyms

AB	Air Breather
ABCS	Army Battle Command System
ADSI	Air Defense Systems Integrator
AFATDS	Advanced Field Artillery Tactical Data System
AMDWS	Air and Missile Defense Workstation
AOI	Area of Interest
ATCCS	Army Tactical Command & Control System
ASAS	All Source Analysis System
BCS	Battle Command Server
BAS	Battlefield Automated System
BCS3	Battle Command Sustainment Support System

BCTID	Battle Command Training and Integration Division
BFA	Battlefield Functional Area
BFT	Blue Force Tracker
BOS	Battlefield Operational Specialty
C2	Command and Control
C2PC	Command and Control Personal Computer
C2R	Command and Control Registry
C3	Command, Control, and Communications
C41	Command, Control, Communications, Computers, and Intelligence
CADRG	Compressed ARC Digitized Raster Graphics
CAPES	Combined Arms Planning & Execution Monitoring System
CECOM	Communications and Electronics Command
CFPD	Color Flat Panel Display
CIB	Controlled Image Base
CJMTK	Common Joint Mapping Toolkit
CIB	Controlled Image Base
CLF	Common Look and Feel

CMP	Command Message Processor
COA	Course of Action
COE	Common Operating Environment
CONOPS	Continuous Operations
COP	Common Operational Picture
COTS	Common Off The Shelf
CSSCS	Combat Service Support Control System
DAS	Data Acquisition System
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DII COE	Defense Information Infrastructure Common Operating Environment
DMS	Degrees, Minutes, Seconds
DNS	Domain Name Server/Service
DoD	Department of Defense
DTCC	Datum Transformation and Coordinate Conversion
DTD	Digital Terrain Data
DTED	Digital Terrain Elevation Data

DTG	Date Time Group
DTS	Display Terminal Service Command
DTSS	Digital Topographical Support System
EAC	Echelons Above Corps
EHFA	IMAGINE Extremely High Frequency Appliqué
EIR	Equipment Improvement Recommendations
EMP	Electromagnetic Pulse
EOB	Enemy Order of Battle
ERDAS	Earth Resources Data Analysis System
EZ PASS	EZ Publish and Subscribe Services
FBCB2	Force XXI Battle Command Brigade and Below
FIPR	Flash, Immediate, Priority, Routine (Message)
FM	Field Manual
FRAGO	Fragmentary Order
FTP	File Transfer Protocol
GCCS	Global Command and Control
GCCS-A	Global Command and Control System - Army
GCCS-M	Global Command and Control System - Maritime

GCC2	Ground Combat Command and Control System
GMT	Greenwich Mean Time
GPU	General Purpose User
GSALT	GCSS (Global Combat Support System) System Administration and Log Tool
GSD	Graphical Situation Display
GTCS	Ground Tactical Communications Software
GUI	Graphical User Interface
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ICD	Interface Control Document
IETM	Interactive Electronic Technical Manual
IIS	Internet Information Service
IOT&E	Initial Operational Test & Evaluation
IP	Internet Address
ISYSCON	Information System Control
JAAS	Java Authentication and Authorization Service
JMPS	Joint Message Processing System
JVMF	Joint Variable Message Format

JWARN	Joint Warning and Reporting Network
KPT	Key Personnel Training
LAN	Local Area Network
LDIF	LDAP (Lightweight Directory Access Protocol) Data Interchange Format
M&O	Maps and Overlays
MAA	Mission Application Administrator
MAU	Mission Application User
MCS	Maneuver Control System
MDMP-A	Military Decision Making Process Assistant
MDR	Message Data Replicator
MGRS	Military Grid Reference System
MIL-STD	Military Standard
MIP	Multilateral Interoperability Program
MSL	Map Specification Library
MTS	Missile Tracking System
MUL	Master Unit List
NBC	Nuclear, Biological and Chemical

NDS	Netscape Directory Server
NGA	National Geospatial-Intelligence Agency
NIMA	National Imagery and Mapping Agency
NITF	National Imagery Transmission Format
NPT	Network Time Protocol
NRTS	Near Real Time Server
NTLDR	New Technology Loader (Microsoft Windows)
ODBC	Open Database Connectivity
OS	Operating System
PASS	Publish and Subscribe Services
PLGR	Plugger
PMCS	Preventative Maintenance Checks and Services
RHDD	Removable Hard Disk Drive
RPF	Raster Product Format
SA	Situational Awareness, or System Administrator
SAM	System Administration Manual
SEC	Software Engineering Center
SK	Secondary Key

SMS	System Management Services
SOP	Standing Operating Procedure
SQL	Structured Query Language
SSL	Secure Sockets Layer
STCCS	Strategic Theater Battle Management System
SUM	Software User Manual
SVD	Software Version Description
TAC	Tactical Command Post
TCP/IP	Transmission Control Protocol/Internet Protocol
TDBM	Track Database Management
TBM	Tactical Ballistic Missile
TBMS	Theater Ballistic Missile System
TM	Technical Manual
TMS	Track Management System
TO	Task Organization
TOC	Tactical Operations Center
TSAPR	Time Synchronization and Position Reporting
TPSD	Training Program Structure Document

TSM	TRADOC (Training and Doctrine Command) System Manager
TSP	Training Support Package
TTL	Time to Live
UDHF	Unit Designation Higher Formation
UDP	Update Port
UIC	Unit Identification Code
USMTF	United States Message Text Format
URL	Uniform Resource Locator
URN	Unit Reference Number
UTO	Unit Task Organization
UTM	Universal Transverse Mercator
UTR	Unit Task Reorganization (as in UTR message)
UTC	Universal Server Time
VMF	Variable Message Format
VPF	Vector Product Format
WAN	Wide Area Network
WGS84	World Geodetic System 1984
XML	Extensible Markup Language

Index