CommPower Enterprise NATO Extensible Markup Language (XML) Portal (NATO CP-EXP)

Co-Hosted, Standalone and Mid-Range/Enterprise NATO CP-EXP Installation Procedures

document version 1.0

Software version 1.1_01-28-08x or later

Model Number: CPXP-EXP-CAPI

CCATS #: G045852

Export Control Classification: 5D002 (ENC, NS1, AT1)

Agency: U.S. Department of Commerce

prepared:
November 30, 2007

prepared for:

NATO CP-EXP Installers

CommPower, Inc.
1040 Flynn Road
Camarillo, CA 93012

http:\\www.commpower.com

Copyright ©2002, 2003, 2004, 2005, 2006, 2007, 2008 Communications & Power Engineering, Inc.

All rights reserved. No part of this publication may be reproduced, transmitted, stored in a retrieval system, nor translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of the copyright owner, Communications & Power Engineering, Inc. Copyright infringement is a serious matter under the United States and foreign Copyright Laws.

Any copyrighted software that accompanies this document is licensed to the End User only for use in strict accordance with the governing End User License Agreement (EULA), which should be read carefully before commencing use of the software. Information in this document is subject to change without notice.

Use, duplication, or disclosure by the UNITED STATES GOVERNMENT is subject to restrictions as set forth in subparagraph (c) (1) of the COMMERCIAL COMPUTER SOFTWARE - RESTRICTED RIGHTS clause at FAR 52.227-19, or subparagraph (c) (1) (ii) of the RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE clause at DFARS 52.227-7013. The “Contractor/Manufacturer” is Communications & Power Engineering, Inc.

Table of Contents

Figures

Document Revision History

Document Release	Release Date	Comment
001	01/15/08	Initial Release as a separate document for Co-Hosted, Standalone and Mid-Range/Enterprise installations.

Foreword

Within NATO, many legacy systems are in operation that must co-exist within an X.400 network environment, yet are nowhere near enabled. For these systems, a generic gateway capability is needed that will process X.400 S/MIME v3 ESS messages in a compliant manner and then pass/receive them to/from the legacy system in a generic format. The NATO CP-EXP has been designed specifically to fulfill this need (i.e., providing X.400 to/from XML gateway support).

Other key NATO CP-EXP functions include X.500 directory access via an LDAP or SLDAP interface and message security label creation/validation via the CommPower Security Label Server.

The NATO CP-EXP operates in the Windows 2003 server environment and includes an embedded data labeling and exchange mechanism known as the Secure Network Queue Manager (SNQM) to provide data labeling in support of security/sensitivity processing.

The NATO CP-EXP is currently being offered as part of the Canadian Military Message Handling System (MMHS) program and is the sister product to the CP-EXP that is part of the U.S. Defense Message System (DMS) program. The CP-EXP belongs to a suite of CommPower messaging products that are currently in use within the U.S. Army, U.S. Navy, U.S. Air Force, the U.S. Defense Logistics Agency, the U.S. Federal Aviation Administration, and the U.S. Department of Commerce.

1. Overview

This document applies to the CommPower Enterprise NATO XML Portal (NATO CP-EXP) system and its software installation. The purpose of this document is to specify the steps necessary for the proper installation of a NATO CP-EXP system. This document provides specific instructions for each of the available implementations of the NATO CP-EXP: Co-Hosted, Standalone and Mid-Range/Enterprise.

1.1 Assistance

Telos AMHS Support Team
3655 Alamo Street, Suite 300
Simi Valley, CA 93065

(888) 453-3567 *(option 2)*
amhssupport@telos.com

1.1.1 Maintenance and Operations

For maintenance and operational problems that occur during installation or operation of this product, contact the Telos AMHS Support Team.

1.2 System Overview

The NATO CP-EXP is the gateway allowing communication to/from an X.400 network and a backside messaging system by rendering S/MIME v3 ESS X.400 messages to XML and XML messages to S/MIME v3 ESS X.400 messages. Additionally, the NATO CP-EXP can also relay input X.400 messages to the organization's X.400 mailbox.

There are four main parts to the NATO CP-EXP software. They include the DCL MTA software that provides the X.400 communications to other adjacent MTAs, the NATO CP-EXP application software that does the actual translation of messages to/from XML and relaying of the X.400 messages, the Inbound and Outbound Router services that direct X.400 and XML messages within the NATO CP-EXP operating environment and the Security Label Server that provides independent security label validation services to backside message system users.

1.3 System Implementation

The following are definitions of the various NATO CP-EXP implementations currently available.

- Co-Hosted: A system on which the NATO CP-EXP, Security Label Server and AMHS applications are installed on a single platform.
- Standalone: The NATO CP-EXP and AMHS applications are installed on two independent systems interfacing through network drive shares.
- Mid-Range/ Enterprise: One or more NATO CP-EXPs operating with an AMHS distributed environment.

1.4 Assumptions

The following assumptions are made:

- The installer has a working knowledge of Windows 2003 Server.
- The installer has administrator access to the host's operating system. The procedures will be completed using a domain account that has local system administrator privileges.
- The installer is familiar with the use of a Windows text editor (for example, "WordPad" or "Notepad").
- Unless specifically called out in the procedure, all window fields should be left to their default values.
- The installer must have a general knowledge of NATO CP-EXP and how it interacts with the AMHS application.

- The system is installed as a member server not on a Domain Controller. The exception to this is for a Co-Hosted installed system that will run in a standalone Workgroup. If this will be the case then whenever this document instructs the installer to logon as a domain user, logon instead as the local system administrator.
- If the Windows Server being used for the installation is joining an Active Directory Forest, please contact the site administrator to insure an authorized time source is being used for the Domain Controller's "Authoritative Time Server" (ATS). The authorized time source for the site is shown in the site's Detailed Design.

  Sample procedures for setting the Domain Controller's ATS are provided in the following documents:

  Installation and Configuration for Microsoft Windows Server 2003 Operating System

  For detailed information, see Microsoft Knowledge Base Article – 216734 How to Configure an Authoritative Time Server in Windows 2000 and Microsoft Knowledge Base Article – 224799 Basic Operation of Windows Time Server.

1.5 Conventions Used in this Document

The procedures in this document use the conventions shown below. The examples shown are samples only and are used to illustrate what the reader will see throughout the text.

[ENTER]	Keyboard key to press (10pt Microsoft Sans-Serif UPPERCASE within square brackets [XXX])
Reload	Control in a dialog box or window to click or select, such as command buttons and radio/option buttons (10pt Bold Arial Narrow)
`Administrator`	Value to be typed exactly as shown inside a field `(Courier New 11pt expanded 1.5pt)`
password	Variable entry to be typed or selected from a list (italics)
{Device Name}	Item within curly brackets to be replaced with your system specific device or file
<your URL>	Item within angle brackets to be replaced with your specific URL
"*filename*"	The exact name of a required file in a file directory or path *11pt Italics Times New Roman "filename" within quotes*
"Document Title"	The exact title of a referenced document or CD *11pt Times New Roman Italics "Name of Document Title" within quotes*
NOTE: Note text here	Supplemental information relative to the preceding text. NOTES follow the applicable step or description.

TIP: Note text here	Information or suggestions for alternative methods that may not be obvious. Tips can also help the reader understand the benefits and capabilities of the product. TIPS follow the applicable step or description.
IMPORTANT: text	Instructions or requirements that are necessary for correct installation. IMPORTANT text may precede or follow the applicable step or description.
CAUTION: text…	Advisory information to prevent software malfunction or damage to equipment. CAUTIONS precede the applicable text.

2. System Requirements

This chapter describes the minimum hardware and system software requirements for installing and running the NATO CP-EXP on an Intel platform.

2.1 Facility Requirements

- Power and Network connections
- UPS Unit

2.2 Server Hardware

- Intel Dual Pentium IV 2.4 GHz CPU unit or better
- Windows 2003 Server (Standard or Enterprise Edition)
- 4GB of RAM
- 5 X 9 GB of hard disks (optional RAID array for availability/reliability)
- CD-ROM Unit
- 1024 x 768 pixel display
- Mouse
- 1 – 4 Ethernet ports depending on implementation

2.3 Server Software

- CD-ROM: Windows 2003 Server Software (core operating system). Additional add-on software from this CD-ROM may be needed.
- CD-ROM: This CD-ROM includes:
    - CommPower NATO CP-EXP software and FENs
    - Re-distributable installation for the Microsoft XML4 library/DLL
    - DCL MTA software and FENs
    - CommPower Security Label Server Utility software and FENs
- FEN: Windows 2003 Hotfixes 3.1.1-WIN2003OS-CD, Version 3.1.1.0 or higher (contains Windows 2003 server install documentation and software). The hotfixes are also available on a CDROM.
- FEN: Windows 2003 Security 3.1.2-SECURW2003, Version 3.1.2G.0 or higher. This is the Security FEN for Windows 2003.
- FEN: IAVA FEN installation in accordance with the FEN Applicability Matrix and FEN instructions.

Note:	Please refer to the FEN Applicability Matrix on DADS for the latest version of these FENs.

2.4 Information Required for Installation

Before beginning the installation process, fill in the table in Appendix A. This data will be used during the installation. This will provide a reference sheet with all of the required information that is needed while installing, configuring, and testing the NATO CP-EXP software.

2.5 Installation Planning

This installation has been streamlined as much as possible. For planning purposes it is suggested that up to eight hours be allocated for a new install. Please recognize that due to the commercial requirements there are four or five restarts for a new install during this process. If the desktop upon which the software is being installed requires considerable time to reboot, adjust the installation time planning estimate accordingly.

3. Installation Roadmap

Install the NATO CP-EXP on the largest drive available. Please review the FEN Applicability Matrix on DADS (look under "Approved FENS/Software" and select "Matrix") prior to the installation of this product to determine what non-CP-EXP FENs are needed. The Applicability Matrix identifies the specific software that must be installed. Please use the matrix for the latest CP-EXP available.

Table 3-1 is an overview of the steps required to properly install the NATO CP-EXP.

Table 3-1: Software Installation Roadmap

Required Steps	Initial Install
NATO CP-EXP Licensing	A license file is required for permanent systems. However, a 30 day demo mode is available for initial operation.
Install Windows 2003 Server Software (Core Operating System)	The Windows 2003 Core OS must be applied in all cases.
Install "Windows Hot Fixes and Service Packs" CD-ROM or FEN	Windows 2003 Hotfixes 3.1.1-WIN2003OS-CD software must be applied next. After completion, the DMS Product Version for WINDOWS 2003 must be: **3.1.1.0** or higher. To check the version, select **Start→Run,** Type: `dmsver`, select **OK**.
Get FENs from DADS	Download all applicable FENs; however, do not install them at this time. *Pay close attention to any FEN that may contain a replacement for this installation document and use it!* DADS websites: https://dkwwwefgv001.roscc1.disa.mil and https://whefl001.ncr.disa.mil (backup site) Note that these are secure servers ("https").
Section 4.1	Reference Documentation
Section 4.2	NATO CP-EXP System Must Be In An Active Directory Domain
Section 4.3	Verify Your Desktop Display
Section 4.4	System Time Synchronization And Configuration
Section 4.5	Verify Virtual Memory Settings
Section 4.6	DNS Hostname Verification
Section 4.8	Apply for your NATO CP-EXP Licenses
Section 4.9	AMHS and NAS Configurations
Section 4.10	NATO CP-EXP Pre-installation Procedures
Section 5.1	MTA Software Installation
Section 5.2	NATO CP-EXP Installation

Required Steps	Initial Install
Section 6	Security Label Server Installation
Section 7	XML Core Services 4.0 SP1 Installation
Section 8	General NATO CP-EXP Application Configuration
Section 9	Co-Hosted, Standalone, and Mid-Range/Enterprise System Specific Configuration
Section 10	Configuring the Security Label Server
Section 11	On-Line NATO CP-EXP Configuration
Section 12	Start the Security Label Server
Section 13	Configure Relay Addressing
Section 14	Configure the NATO CP-EXP MTA With the DC Config Utility
Section 15	Installation of the Anti-Virus FEN, Security FEN, and IAVA FENs

4. Pre-Installation Procedures and Configurations

4.1 Reference Documentation

The following documentation and reference material should be collected and reviewed prior to performing the installation of the NATO CP-EXP software.

- Refer to Appendix A for a list of data needed
- Site's detailed design
- The Windows 2003 Server and Hot Fixes installation instructions (DADS)
- The latest Security configuration instructions (DADS)
- Administrator's Guide

4.2 NATO CP-EXP System Must Be In An Active Directory Domain

Each Primary and Backup NATO CP-EXP must participate as a "Member Server" in the same Active Directory domain. A Domain Admin logon account must be provided prior to installing the NATO CP-EXP software.

The exception to this is for a Co-Hosted installation that will run in a standalone Workgroup. If this is the case then whenever this document instructs the installer to logon as a domain user, logon instead as the local system administrator.

4.3 Verify Your Desktop Display

The desktop display setting must be set for 1024 x 768 or higher. Verify the display settings as follows:

1. Select Start→Settings→Control Panel→Display→Settings tab.
2. In the Screen Resolution area set the display for 1024 x 768 pixels. Select Apply.
3. Select Yes to confirm that the bit map tested properly.
4. Select OK to close the Display Properties window.

4.4 System Time Synchronization And Configuration

It is imperative that system time and time zone of the NATO CP-EXP System are synchronized with the domain controller. Failing to do so will cause failures of the Inbound and Outbound Router services and possible message loss. If the Windows Server is part of an Active Directory Forest, please contact the site administrator to insure an authorized time source is being used as the Domain Controller's "Authoritative Time Server" (ATS). The authorized time source(s) for this site is shown in the site's Detailed Design document. Manual setting of the system time is acceptable for initial setup; however, prior to operation, the NATO CP-EXP System will require a reliable time synchronization configuration.

The system time must be set to Greenwich Mean Time (GMT) and the Time Zone set to "Casablanca, Monrovia". Please check it now and correct it, if necessary.

For a Co-Hosted installed systems that will run in a standalone Workgroup, follow the steps listed below to configure the Windows Time Service to use an approved DMS time source:

1. Select Start→Run.
2. Type `cmd` and select OK.
3. At the Command Prompt window type

   a. `w32tm /config /syncfromflags:manual /manualpeerlist:IP_Sync1, IP_Sync2, IP_Sync3`

   Where IP_Sync1, IP_Sync2 and IP_Sync3 are the IP addresses for the Primary, Secondary and Tertiary (if available) NTP Servers listed in the site's Detail Design document.

   b. `w32tm/config/update`

To determine if the system is time synchronized enter the following commands in the Command Prompt window that was used in the steps above:

1. `w32tm /stripchart /computer:IP_Sync1 /dataonly`

   Where IP_Sync1 is the IP address for the Primary NTP Server listed in the site's Detail Design document.

2. `Exit` (when finished)

The NTP software installed with the NATO CP-EXP will be configured at the time of NATO CP-EXP software installation.

4.5 Verify Virtual Memory Settings

In addition to the customizations outlined in the operating system (OS) instructions, the virtual memory settings must be set to specific parameters for the NATO CP-EXP. Follow the steps listed below to set the virtual memory parameters:

1. Log onto the NATO CP-EXP as the local system administrator.
2. Select Start→Settings→Control Panel→System→Advanced. In the Performance section select Settings. Select the Advanced tab.
3. Select Change under Virtual memory area to view the virtual memory settings.
4. With the C: drive selected in the top portion of the Virtual Memory window:

   a. Make the Initial Size (MB) = Physical System Memory

   b. Make the Maximum Size (MB) = 2X Physical System Memory

5. Select Set.

6. Select OK to close the Virtual Memory window.
7. Select OK to close the Performance Options window.
8. Select OK to close the System Properties window.
9. Select Yes if prompted to reboot the system.

4.6 DNS Hostname Verification

Verify the NATO CP-EXP's hostname is registered in DNS by performing the following:

1. Select Start→Run.
2. Type `cmd` and select OK.
3. At the Command Prompt window type nslookup <hostname>

Where <hostname> is the hostname of the local computer.

The hostname and IP address of the local host should be returned at the prompt. If not, contact the site's DNS administrator to register the NATO CP-EXP's hostname and IP address in the local DNS server.

> IMPORTANT! Do not continue the installation until the hostname and IP address are properly registered.

4.7 Obtain the Organizational Certificate Files (.p12) and Trust Point Certificate File (.cer)

The NATO CP-EXP supports the configuration of up to 2000 organizational .p12 certificate files. Obtain these files from the appropriate Certificate Authority prior to installation. If the files are password protected, knowledge of each password will also be required for proper configuration.

Each Trust Point public certificate file (self-signed certificate) for each organizational certificate that is configured will be needed to complete the certificate configuration. Obtain each from the appropriate Certificate Authority prior to installation.

4.8 Apply for your NATO CP-EXP Licenses

Determine the hard-coded machine ID for your machine by executing the following commands:

1. Select Start→Run.
2. Type `cmd` and select OK.
3. Type: `ipconfig /all [ENTER]`

Only some items from the command's printout follow:

> "Windows 2003 IP Configuration"
>
> Host Name . . . . . : kyhftz03.lmdms.com.
>
> Physical Address. . . . . : 00-10-4B-9B-EC-04.

Look for the Physical Address. It will look like 00-10-4B-9B-EC-04 where the physical address is a twelve digit alpha-numeric number. This number along with the eight digit alpha-numeric hostname must be used to obtain the license file. This information is used by the DMS Help Desk to request a new license file. Contact the Telos AMHS Support Team (refer to Section 1.1 - Assistance) with this information to obtain a NATO CP-EXP license.

If multiple network interface cards (NIC) are installed, information regarding each NIC is returned in the output from the "ipconfig /all" command. Please include the Physical Address for each NIC card in the license request.

To close the command window when finished, type `Exit`.

Note: A 30 day demo license is built into the installation and is available if a permanent license has not been acquired by the time of software installation.

4.9 AMHS and NAS Configurations

The AMHS is software provided by the Telos Corporation. The AMHS software must be installed prior to installing the NATO CP-EXP. Verify that the AMHS administrator users are part of the Administrators Group on the local system(s) that is hosting an AMHS.

Please perform the following configurations as they apply to the type of NATO CP-EXP installation that is being performed.

4.9.1 Standalone Installation

The following procedures will set the share permissions on the **<install drive>:\Telos\Data** directory on the AMHS system. Perform these procedures on all systems hosting an AMHS.

1. Log on to the AMHS system as a user with domain administrator privileges.
2. Using a Windows Explorer browse to **<install drive>:\Telos**.
3. Right click the **Data** folder and choose Sharing and Security.
4. Select Share the folder.
5. Under the Sharing tab, select Permissions.
6. If listed, select Authenticated Users and Everyone. Select Remove.
7. Select Add. Select Object Types... and verify/select Computers, select OK.
8. In the Enter the object names to select section enter the hostname of the NATO CP-EXP and the hostname of the AMHS (separate the hostnames with a semi-colon), select OK.
9. For each hostname added in the step above, highlight the hostname in the Group or user names: section and select Full Control in the Permissions for ... section.
10. Select Add.
11. In the Enter the object names to select section enter `Domain Admins`, select OK.
12. Select Domain Admins in the Group or user names: section and select Full Control in the Permissions section.
13. Select Add.
14. Select Locations and then select the AMHS hostname from the top of the list, select OK.
15. Enter the local Amhsdba and VerityAdmin accounts separated by a semi-colon, select OK.
16. For each account added in the above step, select the accounts in the Group or user names: section and select Full Control in the Permissions section.
17. Select OK.

18. Select the Security tab; ensure Authenticated Users is present with the following permission: Modify, Read & Execute, List Folder Contents, Read, and Write.
19. If not, select Add, under Enter the object names to select enter `Authenticated Users`, select OK. Set the permissions as above.
20. Select OK.

4.9.2 Mid-Range/Enterprise Installation

The AMHS Mid-Range/Enterprise System (i.e. all AMHS, IIS, NAS, etc... systems) is required to be installed and participating in an Active Directory Domain. Perform the following procedures to set the required Share Permissions on the NAS folders used by the NATO CP-EXPs in the Mid-Range/Enterprise system.

Set the share permissions on the AMHSDATA cluster share as follows:

1. Log on to a NAS node as a user with administrator privileges.
2. Start the Cluster Administrator application.
3. In the left window select the **Resources** folder.
4. Right click **AMHSDATA** name item in the right window and choose Properties.
5. Under the Parameters tab, select Permissions.
6. If listed, select Authenticated Users and Everyone. Select Remove.
7. Select Add. Select Object Types... and verify/select Computers, select OK.
8. In the Enter the object names to select enter the hostname(s) of the all the NATO CP-EXPs, the hostname(s) of the AMHS(s), and the hostname(s) of the IIS host(s) (separate the hostnames with a semi-colon), select OK.

Note: The IIS hosts and the AMHS host maybe the same system.

Note: Any other host that has the CommPower Security Label Server installed will have to be added to the list.

9. For each host added in the step above, select the host in the Group or user names: section and select Full Control in the Permissions section.
10. Select Add.
11. In Enter the object names to select enter `Domain Admins`, select OK.
12. Select the Domain Admins in the Group or user names: section and select Full Control in the Permissions section.
13. Select OK.
14. Select OK.
15. Select OK.
16. Select File→Exit, to close the Cluster Administrator.

4.10 NATO CP-EXP Pre-installation Procedures

Perform the following steps to set the required User Rights and Service startup configuration.

4.10.1 User Rights Setting

1. Log on to the system as a domain user that has local system administrator rights.
2. Select Start→Programs→Administrative Tools→Local Security Policy.
3. At the Local Security Settings window, select Security Settings→Local Policies→User Rights Assignment.
4. Double-click on Act as part of the operating system.
5. Select Add User or Group.
6. Type the current logged on domain user's name, and select Check Names.
7. Select OK. At the Act as part of the operating system properties window, select OK.
8. Double-click on Log on as a service.
9. Select Add User or Group.
10. Type the current logged on domain user's name, and select Check Names.
11. Select OK. At the Log on as a service properties window, select OK.
12. Right click Security Settings in the left hand pane and select Reload.
13. Close the Local Security Settings window.
14. Log out and log in as the above domain user.

4.10.2 Secondary Logon

1. Select Start→Programs→Administrative Tools→Services.
2. Ensure the Secondary Logon service Startup Type is set to Automatic.
3. If necessary, start the Secondary Logon service.

5. NATO CP-EXP Application Software

The following section provides the installation steps for all implementations of the NATO CP-EXP. Individual installation and configuration steps required for each implementation are provided within separate sections of this document.

Prior to installing the NATO CP-EXP application, ensure the following:

1. Complete the Pre-Installation Checklist.
2. Review and refer to your detailed design to record site information. Refer to Appendix A for the data needed from the detail design documentation.

During the installation:

3. Install all software on the largest drive available.
4. Read and follow the on-screen instructions carefully along with the procedure steps included herein.
5. During the installation process, move to the next screen by selecting Next, move back to the previous screen by selecting Back, or cancel out of the installation by selecting Cancel.
6. The installation is completed as a domain user that has local system administrator rights. Make certain that this user is included in the local system's Administrators group. The exception to this is for a Co-Hosted installed system that will run in a standalone Workgroup. If this will be the case then whenever this document instructs the installer to logon as a domain user, logon instead as the local system administrator.
7. Each Primary, Backup or Enterprise NATO CP-EXP must participate as a "Member Server" in the same Active Directory domain prior to installing any NATO CP-EXP software. The exception to this is for a Co-Hosted installed system that will run in a standalone Workgroup.

5.1 MTA Software Installation

Perform the steps listed in the sections below to install the Message Transfer Agent (MTA). These sections include instructions on DSA installation and the MTA configuration utility installation.

5.1.1 DSA Installation

Full instructions for installing the Directory Server Agent (DSA) are provided in the DC Directory Administrator's Guide.

The directory server, DC Directory, is required to provide directory service to support the DCL MTA. To install DC Directory, perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights.
2. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on DCL MTA\DSA\setup.exe. The Welcome window is displayed.
3. Select Next on the Welcome window. The CD Key window is displayed.
4. Enter the CD Key as 013-9704-97251 and then select Next on the CD Key window. The Select Components window is displayed.
5. Confirm all component check boxes are selected. Select any that is not checked.
6. Select Browse and the Choose Folder window is displayed. Enter the Path as D:\dcdsrvr (where D: represents the drive letter for the largest drive available on the system) and select OK.
7. If prompted to create this folder, select Yes on the Setup window. The Select Components window is displayed.

8. Select Next and the Enter Admin Node window is displayed.
9. Select Normal if not selected and enter a country value of US. Leave the remaining fields blank. Select Next and the Specify Server Name window is displayed.
10. If the Server Name value is not correct, enter the correct value as seen in the site's Detail Design document. Enter a Port Number of 104 (Note: be sure to change this from the default value of 102).
11. Select Next and the Enter Organization Name window is displayed.
12. Enter the site's organization name and select Next. The Enter Password window is displayed.
13. Enter the password of the logged on user in the Enter Password window and select Next. The Select Program Folder window is displayed.
14. Select Next on the Select Program Folder window. The Customize DC Directory Server Configuration? window is displayed.
15. Make sure the Customization option is NOT checked and select Next on the Customize DC Directory Server Configuration? window. The Start Copying Files window is displayed.
16. Select Next on the Start Copying Files window. Software installation begins. Installation progress is displayed via a progress bar in the Setup window. When the installation has completed, an Information window is displayed.
17. Select OK on the Information window. The Information window is closed and the installation is complete.
18. Select Start -> Run, Type: cmd and select OK. A Command Prompt window is displayed.
19. Enter the following two commands:
    a. sctcompd cds128 [ENTER]
    b. sctcopyd cds128 [ENTER]

5.1.2 Administrative Directory User Agent (ADUA) Installation

To install the ADUA perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights. This must be the same account that was used during the DC Directory installation.
2. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **DCL MTA\ADUA\setup.exe**. The Welcome window is displayed.
3. Select Next and the Choose Destination Location window is displayed.
4. Select Browse and enter the Path: as **D:\Program Files\Data Connection\DC Directory Admin** on the Choose Folder (where D: represents the drive letter for the largest drive available on the system) window and then select OK. If asked to create the folder, select Yes on the Setup window.
5. The Choose Destination Location window is displayed. Select Next and the software is installed. Installation progress is displayed via a progress bar in the Setup window.
6. Select OK on the Information window to complete the installation.
7. Manually restart the system. The DC Directory Service will start automatically following restart of the system.

Note: After restarting the system, check the Services to determine if the DC Directory Service started. If it did not start, re-enter the password for this Service using the Services window and then manually restart the DC Directory Service.

5.1.3 Bootstrap the DSA

When installed with Access Control enabled, the DSA must be "Bootstrapped" prior to performing the MTA portion of the install. Follow the steps listed below to Bootstrap the DSA.

1. Select Start→All Programs→DC Directory Administrator and the Log on to DC Directory Admin – Step 1 of 2 window is displayed.
2. Select Next and the DC Directory Admin – Set 2 of 2 window is displayed. Enter the Directory Server name as the hostname of the CP-EXP, set the Auth Level to `None` and then select Advanced.
3. Set the Port to a value of `104`, select OK and then Finish. The DC Directory Admin window is displayed.
4. Select OK and the DC Directory Admin: Configure First Server – Step 1 of 3 window is displayed.
5. Enter the logged on user's password and then select Next. The DC Directory Admin: Configure First Server – Step 2 of 3 window is displayed.
6. Select Next and the DC Directory Admin: Configure First Server – Step 3 of 3 window is displayed.
7. Enter the Administrator Name as `mtaadmin` and the Password as that of the logged on domain user.
8. Select Finish and the DC Directory Admin window is displayed.
9. Select File→Exit to complete the Bootstrap process.

5.1.4 MTA Installation

To install the DCL MTA, perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights. This must be the same account that was used during the DC Directory installation.
2. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **DCL MTA\MTA\setup.exe**. The Welcome window is displayed.
3. Select Next on the Welcome window. The CD Key window is displayed.
4. Enter the CD Key as `013-0714-16984` if not already filled in and then select Next on the CD Key window. The Select Components and Destinations window is displayed.
5. Make sure that all components are selected and then select Browse.
6. Enter the Path: as **D:\DCIMS** (where D: represents the drive letter for the largest drive available on the system) on the Choose Folder window and then select OK. If asked to create the folder, select Yes on the Setup window. The Select Components and Destinations window is displayed.
7. Select Next on the Select Components and Destinations window. The Windows NT Service Logon Password window is displayed.
8. Enter the password of the logged on user and select the Next button in the Windows NT Service Logon Password window. The Global Domain Identifier window is displayed.
9. Enter the required values in the Country, ADMD, and PRMD fields and then select the Next button on the Global Domain Identifier window. The Presentation Address and Port Configuration window is displayed.
10. Enter the required values in the P-Selector, S-Selector, and T-Select fields and set the Port to a value of `102`. Select Next on the Presentation Address and Port Configuration window. The Server Name window is displayed.

Note: Typical values for DMS are A100, A200 and A300, respectively. Typical values for MMHS are X400-88 for the TSAP parameter only. Check the site's Detail Design document for the specifics values.

11. Confirm that all displayed information is correct. If any is incorrect, make changes as required. Enter the Local Name and Local Credentials as the 12 character CP-EXP component name as seen in the site's Detail Design document. Select Next and the DC IMS Administrator window is displayed.
12. Enter the Account Name as `/c=us/cn=mtaadmin` and the logged on user's password. Select the Next button and the Administration Point window is displayed.
13. Select Next on the Administration Point window and the Check Setup Information window is displayed.
14. Select Next in the Check Setup Information window. Software installation begins. Installation progress is displayed via a progress bar in the Setup window.
15. Select OK in the Information window to complete the installation. It may take several minutes before the Information window is displayed.

Note: Any information entered during the MTA installation can be changed later, if desired, via the MTA configuration utility, DCConfig.

5.1.5 MTA Configuration Utility Installation

The DCL Configuration Tool is required to complete/change the MTA configuration and to create/change the MTA routing rules. To install the DCL Configuration Tool, perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights. This must be the same account that was used during the DC Directory installation.
2. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **DCL MTA\DCConfig\setup.exe**. The Welcome window is displayed.
3. Select Next in the Welcome window. (No CD Key is required for this portion of the installation.) The Choose Destination Location window is displayed.
4. Select Browse and enter the Path: as **D:\Program Files\Data Connection\DC Config** (where D: represents the drive letter for the largest drive available on the system) on the Choose Directory window and then select OK. If asked to create the folder, select Yes on the Setup window.
5. The Choose Destination Location window is displayed. Select Next and the Directory Search Node window is displayed.
6. Select Next in the Directory Search Node window. The Select Program Folder window is displayed.
7. Select Next in the Select Program Folder window. The Check Setup Information window is displayed.
8. Select Next in the Check Setup Information window. Software installation begins. Installation progress is displayed via a progress bar in the Setup window. The DC Config window is displayed.
9. Select Finish in the DC Config window. The DC Config window is closed and an Information window is displayed.
10. Select OK in the Information window to complete the installation.

5.2 NATO CP-EXP Installation

To install the NATO CP-EXP, perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights.

2. Exit all Windows programs.
3. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **NATO CP-EXP\SMIME_CP-EXP.msi**. The Welcome to the CommPower XML Portal (CP-EXP) NATO Installation Setup Wizard window is displayed.
4. Select Next . The License Agreement window is displayed.
5. If you agree to the terms and conditions of the license agreement, select the I Agree option and then select Next in the License Agreement window. The Select Installation Drive window is displayed.
6. Enter the Drive as D (where D represents the drive letter for the largest drive available on the system). The install will not accept a ":" following the drive letter. Select Next.
7. The Confirm Installation window is displayed. Select Next to proceed with the software installation.
8. The License File Options window is displayed. If a license file has been obtained, accept the default selection of Use license file. Otherwise, select the 30 day trial option to allow the system to install and run for a 30 day trial period.
    a. If the default option and Next button were selected, the Setup needs CPXP License Disk window is displayed.
    b. Select Browse to select the folder that contains the license file (filename of license.lic).
    c. Select Next to continue the software installation.

    Or

    d. If the 30 day trial option was selected, highlight the item under Select License Type.
    e. Select Next to continue the software installation.
9. Select Close in the Installation Complete window to complete the installation.
10. Select Yes on the CommPower XML Portal window to restart the system.
11. To configure the CP-EXP, go to section 8, General NATO CP-EXP Application Configuration.

6. Security Label Server Installation

The NATO CP-EXP does not need to have the Security Label Server (SLS) installed to run and process messages.

6.1 Co-Hosted Installation

To install the Security Label Server co-hosted with the NATO CP-EXP, perform the following steps:

1. Log onto the system as a domain user that has local system administrator rights.
2. Exit all Windows programs.
3. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **NATO CP-EXP\Security Label Server\SL_Server_NATO.msi**. The CommPower NATO Security Server Installation Setup Wizard window is displayed.
4. Select Next. The License Agreement window is displayed.
5. If the terms and conditions of the license agreement are acceptable, select the I Agree option on the License Agreement window and then select Next .
6. Select Next in the Confirm Installation window. Software installation begins. The Installation Complete window is displayed.

7. Select Close on the Installation Complete window.
8. Select Yes on the CommPower NATO Security Label Server window to restart the system.
9. To configure the Security Label Server, go to section 10, Configuring the Security Label Server.

Note: Upon system restart, the Security Label Server Service may fail to start. This is expected as it may not be completely configured.

6.2 Standalone and Mid-Range/Enterprise Installation

To install the Security Label Server, perform the following steps:

1. Logon to the system as domain user that has local system administrator rights where the Security Label Server will run. This is not the system running the NATO CP-EXP for a Standalone or Mid-Range/Enterprise Configuration. The system typically used is an AMHS server or IIS server.
2. Exit all Windows Programs.
3. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **NATO CP-EXP\Security Label Server\SL_Server_NATO.msi**. The CommPower NATO Security Server window is displayed.
4. Select Next. The License Agreement window is displayed.
5. If the terms and conditions of the license agreement are acceptable, select I Agree option on the License Agreement window and then select Next. The Select Destination Drive window is displayed.
6. Designate the required drive letter (largest drive on the system) and select Next on the Select Destination Drive window.
7. Select Next on the Confirm Installation window. Software installation begins. The Installation Complete window is displayed.
8. Select Close on the Installation Complete window.
9. Select Yes on the CommPower NATO Security Label Server window to restart the system.
10. To configure the Security Label Server, go to section 10, Configuring the Security Label Server.

Note: Upon system re-start, the Security Label Server Service will fail to start. This is expected as it has not yet been configured.

7. XML Core Services 4.0 SP1 Installation

The NATO CP-EXP requires that MSXML 4.0 Core Services be installed on the system. To determine if these services are installed look for the following files in the C:\Windows\system32\ folder:

msxml4.dll

msxml4.inf

msxml4a.dll

msxml4r.dll

If these files exist, move to section 5. If they do not, then install them following the steps below:

1. Log onto the system as a domain user that has local system administrator rights.
2. Create a folder called **C:\temp\XML**.
3. Insert the installation CD. Via a Windows Explorer, navigate to and double-click on **MSXML4\msxmlcab.exe**". This is a re-distributable installation available from Microsoft.
4. If the terms and conditions of the End-User License Agreement are acceptable, select Yes and browse to the **C:\temp\XML**\ folder. Select OK to extract the "msxml4.cab" file to the **C:\temp\XML**\ folder.
5. From a Windows Explorer, browse to the **C:\temp\XML**\ folder and double-click on msxml4.cab.
6. Highlight the following 4 files via WinZip:

   msxml4.dll

   msxml4.inf

   msxml4a.dll

   msxml4r.dll

7. Right mouse click over the highlighted files and select extract. Extract the files to the **C:\Windows\system32**\ folder.
8. Open a Command Prompt and enter the following commands:

   a. `cd C:\Windows\system32\ [ENTER]`

   b. `regsvr32 msxml4.dll [ENTER]`

8. General NATO CP-EXP Application Configuration

8.1 Installing a Permanent License File

The License Manager has a 30-day demo mode available. This feature allows the administrator to install and run the NATO CP-EXP for up to 30 days without installing a license. A permanent license file can be installed at any point during or after the 30 day trial period.

If a valid/permanent NATO CP-EXP license was received after installation, perform the following steps. If a valid/permanent license file is not available, refer to the Administrator's Guide for instructions on how to start the NATO CP-EXP in Enterprise Mode with a demo license.

1. Log on to the NATO CP-EXP as a domain user that has local system administrator rights.
2. Stop the NATO CP-EXP if it is running.

3. Copy the permanent license into **<install drive>:\cpe\csci\mfg\bin\lmgr** directory.
4. Open the license.lic file in NotePad and verify that the Hostname is correct. If the hostname is incorrect edit the hostname to the proper value.
5. Select File→Save and exit NotePad.
6. Start the NATO CP-EXP.

8.2 Configure the NATO CP-EXP

This version of the NATO CP-EXP, known as the Multi-Channel NATO CP-EXP, supports up to 10 channels; one X.400 channel, and up to 9 XML channels. The following convention will be used:

- Channel 1 will support input/output of X.400 (X.400) messages
- Channel 2 will support all input XML messages coming from any backside XML Server (AMHS).
- Channel 3 will support all output XML messages going to the AMHS.
- Channels 4 – 10 can be configured to support XML message output to additional backside XML Servers, if desired.

Caution: If running in Co-Hosted mode, the CommPower Security Server service must be stopped before starting the NATO CP-EXP Configuration Utility.

Stop the CommPower Security Server service by selecting Start→Programs→Administrative Tools→Services. Right-click on the CommPower Security Server service to select the Stop menu item. This step is not necessary if running in Standalone or Mid-Range/Enterprise mode of operation

Perform the following steps to complete the configuration:

1. Logon to the system as a domain user that has local system administrator rights.
2. Select Start→ CommPower XML Portal→Configure CP-EXP.

Note: This command starts the NATO CP-EXP Configuration Utility graphical user interface (GUI). When editing, information is presented via dialog boxes. Typing new information does not replace the current configuration information until that information has been saved and installed. If a mistake is made, retype the information or simply quit without saving and edit again.

8.2.1 Select the SYSTEM Tab→Parameters button

1. For the Cache Expiration (days), enter a number 1.
2. For the Inbound Message Configuration select the One message for all recipients radio button.
3. Select OK to save changes and return to the SYSTEM menu.

8.2.2 Select the SYSTEM Tab→Trust Points button

1. In the list box, click the row with entry 1.
2. Select the ellipsis box ...
   a. The Select Trust Point Public Certificate File window is displayed. Browse to and highlight the Trust Point file. Select Open.
3. Select the Enable checkbox.
4. Select Apply.

5. Select OK to return to the SYSTEM Menu

8.2.3 Select the SYSTEM Tab→Network Access button

1. Enter the Username of the local administrator.
2. Enter the Password of the local administrator.
3. Enter the hostname of the NATO CP-EXP in the Domain field.
4. Select OK to return to the SYSTEM menu.

8.2.4 Select the SYSTEM Tab→X500 button

1. Select the Access X.500 Directory checkbox.
2. Enter the IP address of the primary DSA (e.g., 206.37.161.140).
3. Enter the IP address of the secondary DSA (e.g., 206.37.161.140). (optional)
4. Select LDAP for Connection Type.
5. Select DIT Top DN
6. Set the Country (C), Organization (O), Organization Unit (OU), Location (L) and/or Common Name (CN) parameters as required.
7. Reorder the DN entries utilizing the Move Up and Move Down buttons so that the DIT top is in LDAP, reverse ORAddress order.
8. Select OK
9. Select Additional X500 Attributes tab.
10. Click the drop-down arrow of the first row in User Certs frame to select mmhsSecurityDomainName-2.16.124.101.1.259.5.4.1.8, and select Instead Of.
11. Click the drop-down arrow of the second row in User Certs frame to select mmhsDeliveryGateway-2.16.124.101.1.259.5.4.1.5, and select Addition To.
12. Click the drop-down arrow of the third row in User Certs frame to select mmhsOtherDeliveryGateway-2.16.124.101.1.259.5.4.1.6, and select Addition To.
13. Click the drop-down arrow of the fourth row in User Certs frame to select mmhsAlternateDelivery-2.16.124.101.1.259.5.4.1.4, and select Addition To.
14. Select the drop-down arrow on first row of User O/R frame to select mmhsOtherMhsOrAddress-2.16.124.101.1.259.5.4.1.3.
15. Select OK

8.2.5 Select the SYSTEM Tab→X400 button

1. Set the MTS Local ID field to the local hostname of the NATO CP-EXP (maximum of ten characters).
2. Set the MTA Name field to NATO CP-EXP MTA. (If multiple NATO CP-EXPs are on site, place an identifier at the end. (e.g., NATO CP-EXP MTA1))
3. At the Global Domain Identifier fields, enter the Country, ADMD, and PRMD (if needed) of the NATO CP-EXP address (e.g. country = CA, ADMD = GOVMT.CANADA, PRMD = DNDMMHS.MDNSTMM).
4. Select OK to save changes and return to the SYSTEM menu.

8.2.6 Select the SYSTEM Tab→MMHS Settings button

1. Use the up arrow in the Crypto Configurations frame to set the Number of Slaves to 6.
2. Select Load From X.500 in top row of the SPIF Locations frame.
3. Browse the DSA to the location of the first English SPIF that will be used and highlight the entry. Choose Select and then Close . If no English SPIF will be used, do not perform this step or the next two steps.
4. Browse the DSA to the location of the second English SPIF that will be used and highlight the entry. Choose Select and then Close . If only one English SPIF will be used, do not perform this step.
5. Browse the DSA to the location of the third English SPIF that will be used and highlight the entry. Choose Select and then Close . If only two English SPIFs will be used, do not perform this step.
6. Browse the DSA to the location of the first non-English SPIF that will be used and highlight the entry. Choose Select and then Close If no non-English SPIF will be used, do not perform this step or the next two steps.
7. Browse the DSA to the location of the second non-English SPIF that will be used and highlight the entry. Choose Select and then Close . If only one non-English SPIF will be used, do not perform this step.
8. Browse the DSA to the location of the third non-English SPIF that will be used and highlight the entry. Choose Select and then Close . If only two non-English SPIFs will be used, do not perform this step.
9. Select OK to return to NATO CP-EXP Configuration Utility.

8.2.7 Select the SYSTEM Tab→Postmaster button

The NATO CP-EXP has two options for the Postmaster mailbox configuration. An external X.400 mailbox or an AMHS mailbox associated with an organizational DN. The configuration of a Local AMHS Postmaster provides a single point of messaging services within the NATO CP-EXP/AMHS system.

Non-Delivery Notifications (NDNs) that are generated by the NATO CP-EXP or received by the NATO CP-EXP relating to configured System Relay and Client Relay recipients are NOT delivered to an AMHS message originator. The Postmaster mailbox acts as the repository for these NDNs and provides the ability to monitor these notifications.

Note: A valid Postmaster address, either External or Local, must be configured even if System Relay and Client Relay addresses are not configured

8.2.7.1 External Postmaster Configuration

To configure an external Postmaster account, a valid X.400 mailbox must be available.

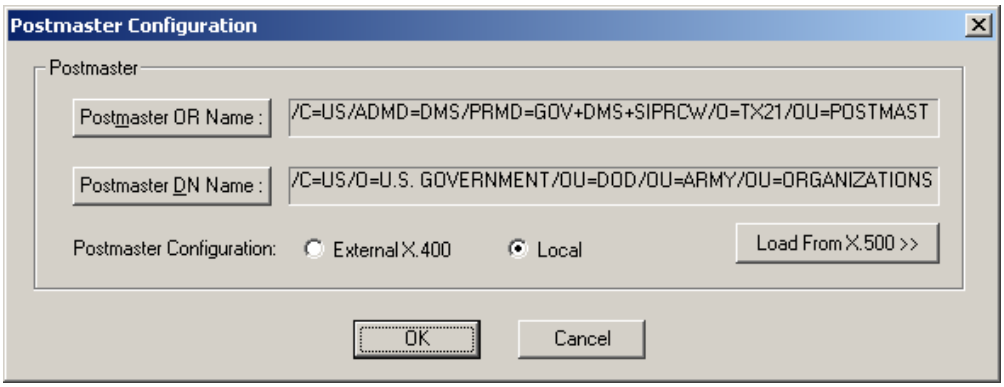

Figure 8.2.6.1-1 Postmaster Configuration

1. On the NATO CP-EXP Configuration Utility window under the System tab, select Postmaster.
2. Select External X.400.
3. Select Postmaster OR Name and enter the X.400 address fields of the External Postmaster account.

Note: The Postmaster DN Name button will be inaccessible.

4. Select OK.
5. Select OK to exit the Postmaster Configuration window.

8.2.7.2 Local Postmaster Configuration

To configure a Local Postmaster use the following procedure to configure a Local AMHS Postmaster account:

Note: DO NOT use a DN on a configured .p12 Organizational Certificate file. The DN used does not have to exist in the DSA.

1. On the NATO CP-EXP Configuration Utility window under the System tab, select Postmaster.
2. Select Local.
3. If the DN being used exists in the DSA, select Load from X.500 and browse to the DIT entry in the DSA associated with the AMHS Postmaster account. Expand the "+" and select Copy Address to Record. The OR and DN fields will be populated.
4. Close DIT access window and skip the next step. Please refer to the AMHS System Administration Guide for instructions to configure a Postmaster DN and mailbox.
5. If the DN being used does not exist in the DSA use the Postmaster OR Name: and Postmaster DN Name: buttons to manually enter the required ORAddress and DN information.
6. Select OK to exit the Postmaster configuration window.
7. Log on to the AMHS Administration Web Utility.
8. Create an AMHS user and associate it with the DMS DIT entry account.
9. Select Site Settings and select the DMSErrorReport_Destination attribute.
10. Enter the name of the AMHS Postmaster account and save.
11. Log out of the AMHS Web Utility.

8.2.8 Select the SECURITY Tab

1. Click the drop-down arrow to configure the highest classification per the detail design.

8.2.9 Select the CHANNEL Tab

- *X.400 Channel 1*

1. Use the UP arrow key to select 1 on Channel.
2. Verify the Alternate Channel is set to –1.
3. Click the drop-down arrow under Security Type and set as per the detail design.
4. Accept the defaults for the remaining fields.

- *XML Input Channel 2*

1. Use the arrow keys to select 2 on Channel.
2. Verify the Alternate Channel is set to –1.
3. Set the Security Type as per the detail design.

- *XML Output Channel 3*

1. Use the arrow keys to select 3 on Channel.
2. Verify the Alternate Channel is set to –1.
3. Set the Security Type as per the detail design.

8.2.10 Save Configuration Settings

To save the configuration settings and exit the NATO CP-EXP Configuration Utility perform the steps listed below.

1. Select File→Install
2. Select File→Exit

8.3 Configure the NATO CP-EXP Certificate Files

The NATO CP-EXP can support up to 2000 individual certificate files. Each must be configured and, if password protected, the password must also be configured.

Perform the following steps to complete the certifcate configuration:

1. Logon to the system as a domain user that has local system administrator rights.
2. Select Start→CommPower XML Portal→Tools→Certificate Control and the Certificate File Configuration utility is displayed.
3. Select Browse and browse to and double click a certificate file. The filename will appear in the next available row with a green check in the associated Enable box.
4. Click in the associated Password box and use the keyboard to enter the password. “Enter” (<CR>) on the keyboard must be selected after entering the password. Each character entered will be displayed as an “*” and the Verified status will be listed as No.
5. Select Logon and the Verified status will be listed as Yes.
6. Repeat the steps above to configure each additional certificate file that will be used.
7. Select Save.
8. Select Exit.

9. Co-Hosted, Standalone, and Mid-Range/Enterprise System Specific Configuration

Type specific NATO CP-EXP configuration is accomplished in the following sections. Perform only the applicable section based on the type of NATO CP-EXP being installed.

- Section 9.1 Co-Hosted System
- Section 9.2 Standalone System with AMHS
- Section 9.3 Mid-Range/Enterprise System

9.1 Co-Hosted System

Note: The AMHS software must be installed prior to performing the procedures in the following section.

1. Logon to the system as a user with domain administrator privileges.
2. Select Start→ CommPower XML Portal→Configure CP-XP.

9.1.1 Select the SYSTEM Tab→ XML Server Settings button

1. If running in Multi-Domain Mode set Enable Multi-Domain Messaging to Yes. Otherwise select No.
2. For Co-hosted DN and Roles File Directory, browse to <install drive>:\Telos\Data\DnRoles.
3. Select OK. Select OK.

9.1.2 Select the SYSTEM Tab→ Enterprise Settings button

1. In the Enterprise Settings window, select the CP-EXP Settings tab.
2. Set the CP-EXP Node Name to the hostname of the NATO CP-EXP, for example: KYHFTZ11. Set the Top Level Node Specific NATO CP-EXP NAS Directory by browsing to or entering <install drive>: \Telos\Data.

Note: All message pool directories will be created under this point. If any of the pool directories does not exist, the Configuration Utility will create them automatically. Select OK if prompted to create the directories.

3. Verify or set the Inactive CP-EXP grace period and DN and Role Check/Update Cycle to 5 minutes.
4. Select the Common Pool Settings tab. These are the default Pool directory names in the Enterprise System. If prompted to create new directories select OK.
5. Select OK.

9.1.3 Save Configuration Settings

To save the configuration settings and exit the NATO CP-EXP Configuration Utility perform the steps listed below.

1. File→Install.
2. File→Exit.

9.2 Standalone System

Note: It is assumed the remote AMHS share folders are configured before the following steps are preformed.

1. Logon to the system as a user with domain administrator privileges.
2. Select Start→CommPower XML Portal→Configure CP-XP.

9.2.1 Select the SYSTEM Tab→ XML Server Settings button

1. If running in Multi-Domain Mode set Enable Multi-Domain Messaging to Yes. Otherwise select No.
2. Configure the DN and Roles File Directory, Browse to or enter the Universal Naming Convention (UNC) and folder as follows: \\AMHS_Server\Data\DnRoles, where "AMHS_Server" is the hostname of the AMHS.
3. Select OK.

9.2.2 Select the SYSTEM Tab→ Enterprise Settings button

1. Under the System tab, select Enterprise Settings.
2. In the Enterprise Settings window, select the CP-EXP Settings tab.
3. Set the CP-EXP Node Name to the hostname of the NATO CP-EXP, for example: KYHFTZ11 Set the Top Level Node Specific CP-EXP NAS Directory by browsing to or entering \\AMHS_Server\Data, where "AMHS_Server" is the hostname of the AMHS.

Note: All message pool directories will be created under this point. If any of the pool directories does not exist, the Configuration Utility will create them automatically. Select OK if prompted to create the directories.

4. Verify or set the Inactive CP-EXP grace period and DN and Role Check/Update Cycle to 5 minutes.
5. Select the Common Pool Settings tab. These are the default Pool directory names in the Enterprise System. If prompted to create new directories select OK.
6. Select OK

9.2.3 Save Configuration Settings

To save the configuration settings and exit the NATO CP-EXP Configuration Utility perform the steps listed below.

1. File→Install.
2. File→Exit.

9.3 Mid-Range/Enterprise System

Note: It is assumed the Enterprise AMHS System is installed and configured with a NASCluster.

1. Logon to the system as a user with domain administrator privileges.
2. Select Start→Programs→CommPower XML Portal→Configure CP-XP.

9.3.1 Select the SYSTEM Tab→ XML Server Settings button

1. Under the System tab, select XML Server Settings.

2. If running in Multi-Domain Mode set Enable Multi-Domain Messaging to Yes. Otherwise select No.
3. For DN and Roles File Directory, Browse to or enter the Universal Naming Convention (UNC) of the shared folder \\AMHScluster\AMHSData\Telos\Data\DnRoles. Where NAScluster is the virtual cluster name of the NAS.
4. Select OK.

9.3.2 Select the SYSTEM Tab→ Enterprise Settings button

1. Select Enterprise Settings.
2. In the Enterprise Settings window, select the CP-EXP Settings tab.
3. Set the CP-EXP Node Name to the hostname of the NATO CP-EXP, for example: KYHFTZ11 Set the Top Level Node Specific CP-EXP NAS Directory by browsing to or entering the UNC of \\AMHScluster\AMHSDATA\Telos\Data.

Caution! All NATO CP-EXPs in the Enterprise System must have the same Top Level Node directory designation.

Note: All messaging pool directories will be created under this point. If the directory does not exist the Configuration Utility will prompt the user to create it, select OK.

4. Verify or set the Inactive CP-EXP grace period and DN and Role Check/Update Cycle to 5 minutes.
5. Select the Common Pool Settings tab. These are the default Pool directory names in the Enterprise System.
6. Select OK. If prompted to create new directories select OK.

9.3.3 Save Configuration Settings

To save the configuration settings and exit the NATO CP-EXP Configuration Utility perform the steps listed below.

1. File→Install.
2. File→Exit.

10. Configuring the Security Label Server

10.1 Co-Hosted

For Co-hosted configurations, the Security Label Server will be automatically configured when the NATO CP-EXP is configured if all of the steps above were followed that apply to Co-Hosted operation. The steps listed below are here to make the installer/operator aware of the Security Label Server Configuration Utility.

1. Log on to the server as a domain user that has local system administrator rights.
2. Open Windows Explorer, browse to **<install drive>:\cpe\csci\mfg\bin** and double-click SL_ServerConfig.exe.
3. Select Parameters. Confirm that Cache Expiration is set to 1 day. Select OK.
4. Select X500. Confirm that the Primary and Secondary DSA IP addresses are correct. Confirm that the DIT Top DN is correct. Confirm that the LDAP radio button is selected.
5. Select the Alternate Certificate tab and confirm that the proper attribute is set.
6. Select OK.
7. Select MMHS Settings. Confirm that all required SPIFs are configured.
8. Select OK.
9. Select the XML Server Settings and confirm that the value is set to **<install drive>:\Telos\Data\DnRoles** folder, select OK.
10. Select File→Install, then File→Exit.
11. Continue installation and configuration at Section 11.

Note: If any of the parameters checked above are not set to the listed values the Co-Hosted installation may have been performed incorrectly. If simple typo-graphical errors were noted, correct the errors with this configuration utility. Otherwise, the problem may require that the Security Label Server, MTA, ADUA and NATO CP-EXP be un-installed and re-installed. See Appendix B for instructions on un-installing the software.

10.2 Standalone

1. Log on to the Security Label Server system as a domain user that has local system administrator rights.
2. Open Windows Explorer, browse to **<install drive>:\cpe\csci\mfg\bin** and double-click SL_ServerConfig.exe.
3. Select Parameters and change the Cache Expiration of -1 to 1 day. Select OK on the Edit System Parameters window.
4. Select X500 and enter the IP address of the Primary DSA and Secondary DSA (optional).
5. Select LDAP for Connection Type.
6. Select DIT Top DN
7. Set the Country, Organization, and Organization Unit (OU) parameters as required.
8. Reorder the DN entries utilizing the Move Up and Move Down buttons so that the DIT top is in LDAP, reverse ORAddress order.

9. Select OK
10. Select Alternate Certificate tab.
11. Click the drop-down arrow in User Certs frame to select mmhsSecurityDomainName-2.16.124.101.1.259.5.4.1.8.
12. Select OK.
13. Select XML Server Settings and browse to **AMHS_Server\Telos\Data\DnRoles** folder, select OK.
14. Select MMHS Settings.
10. Select Load From X.500 in top row of the SPIF Locations frame.
11. Browse the DSA to the location of the first English SPIF that will be used and highlight the entry. Choose Select and then Close. If no English SPIF will be used do not perform this step or the next two steps.
12. Browse the DSA to the location of the second English SPIF that will be used and highlight the entry. Choose Select and then Close. If only one English SPIF will be used do not perform this step.
13. Browse the DSA to the location of the third English SPIF that will be used and highlight the entry. Choose Select and then Close. If only two English SPIFs will be used do not perform this step.
14. Browse the DSA to the location of the first non-English SPIF that will be used and highlight the entry. Choose Select. If no non-English SPIF will be used do not perform this step or the next two steps.
15. Browse the DSA to the location of the second non-English SPIF that will be used and highlight the entry. Choose Select and then Close. only one non-English SPIF will be used do not perform this step.
16. Browse the DSA to the location of the third non-English SPIF that will be used and highlight the entry. Choose Select and then Close. If only two non-English SPIFs will be used do not perform this step.
17. Select Close.
15. Select OK to return to NATO CP-EXP Configuration Utility.
16. Choose Close.
17. Select OK to return to NATO CP-EXP Configuration Utility
18. Select File→Install, then File→Exit.

10.3 Mid-Range/Enterprise

1. Log on to the server as a domain user that has local system administrator rights.
2. Log on to the Security Label Server system as a domain user that has local system administrator rights.
3. Open Windows Explorer, browse to **<install drive>:\cpe\csci\mfg\bin** and double-click SL_ServerConfig.exe.
4. Select Parameters and change the Cache Expiration of -1 to 1 day. Select OK on the Edit System Parameters window.
5. Select X500 and enter the IP address of the Primary DSA and Secondary DSA (optional).
6. Select LDAP for Connection Type.
7. Select DIT Top DN
8. Set the Country, Organization, and Organization Unit (OU) parameters as required.

9. Reorder the DN entries utilizing the Move Up and Move Down buttons so that the DIT top is in LDAP, reverse ORAddress order.
10. Select OK
11. Select Alternate Certificate tab.
12. Click the drop-down arrow in User Certs frame to select mmhsSecurityDomainName-2.16.124.101.1.259.5.4.1.8.
13. Select OK.
14. Select XML Server Settings and browse to **\\AMHSCluser\AMHSDATA\TELOS\DATA\DNROLES** folder, select OK.
19. Select MMHS Settings.
18. Select Load From X.500 in top row of the SPIF Locations frame.
19. Browse the DSA to the locatioin of the first English SPIF that will be used and highlight the entry. Choose Select and then Close. If no English SPIF will be used do not perform this step or the next two steps.
20. Browse the DSA to the locatioin of the second English SPIF that will be used and highlight the entry. Choose Select and then Close. If only one English SPIF will be used do not perform this step.
21. Browse the DSA to the locatioin of the third English SPIF that will be used and highlight the entry. Choose Select and then Close. If only two English SPIFs will be used do not perform this step.
22. Browse the DSA to the locatioin of the first non-English SPIF that will be used and highlight the entry. Choose Select. If no non-English SPIF will be used do not perform this step or the next two steps.
23. Browse the DSA to the locatioin of the second non-English SPIF that will be used and highlight the entry. Choose Select and then Close. only one non-English SPIF will be used do not perform this step.
24. Browse the DSA to the locatioin of the third non-English SPIF that will be used and highlight the entry. Choose Select and then Close. If only two non-English SPIFs will be used do not perform this step.
25. Select Close.
20. Select OK to return to NATO CP-EXP Configuration Utility.
21. Choose Close.
22. Select OK to return to NATO CP-EXP Configuration Utility
23. Select File→Install, then File→Exit.

11. On-Line NATO CP-EXP Configuration

To complete the configuration of the NATO CP-EXP, the NATO CP-EXP must be started. The NATO CP-EXP Start Monitor displays each process as it starts. When a green light is displayed, the process has started. If a light stays red or yellow, please see Debugging the NATO CP-EXP Startup in Appendix C.

11.1 Start NATO CP-EXP User Interface

1. Select Start→Commower XML Portal→Start CP-XP.
2. Select the User Interface button after all processes turn green.
3. Select Close at the Startup Summary window.

Note: If running with an Enterprise license for the first time, pop-up window(s) may be displayed indicating the Inbound and Outbound router services are not configured correctly. Select OK to close the windows. Configuration of an Enterprise System will be completed in the following section.

11.2 Set Disk Threshold, Command Waiting, and Purge Archive

1. Select System→Preferences→Disk Threshold…
2. Set the Low Disk Threshold at 90. Select OK. Select OK on the Information window.
3. Select System→Preferences→Command Waiting…
4. Set the Minutes at 2 and Seconds at 0. Select OK.
5. Select System→Archive Operations→Set Purge Age…
6. Using the scroll bar, set Archive Purge Age to 10 Days. Select OK. Select OK on the Information window.

11.3 NATO CP-EXP X.400 Channel Configuration

1. From the XML Portal window, select Channels, or select System→Channel Operations.
2. Enter 1 in the Channel Number field.
3. Select Setup.
4. At the Channel 1 Setup window, select the Email tab.
5. If not already selected, set the Configuration field to Input/Output.
6. Set the Precedence field to the maximum “precedence” allowed to be received per the detailed design.
7. Leave the Closed Alternate field blank.
8. In the Type section, select X400.
9. Select OK on the Channel 1 Setup window.
10. A Response window appears, it allows channel settings to be reviewed.
11. Select Close to return to the Channel Operations window.
12. Select Open Channel.

13. Select Close on the Response window.

11.4 NATO CP-EXP XML Input Channel Configuration

1. Enter 2 in the Channel Number field.
2. Select Setup.
3. At the Channel 2 Setup window, select the XML tab.
4. Set the Configuration field to Input Only Input Only.
5. Set the Precedence field to the maximum "precedence" allowed to be received per the detailed design.
6. Select OK to close the Channel 2 Setup window.
7. A Response window is displayed.
8. Select Close to return to the Channel Operations window.
9. Select Open Channel.
10. Select Close on the Response window.

11.5 NATO CP-EXP XML Output Channel Configuration

11. Enter 3 in the Channel Number field.
12. Select Setup.
13. At the Channel 3 Setup window, select the XML tab.
14. Set the Configuration field to Output Only.
15. Set the Precedence field to the maximum "precedence" allowed to be received per the detailed design.
16. Enter the Channel Description to AMHS (a maximum of nine characters is permitted).
17. Accept the default settings for XML Attachment Reference, XML Server Comeback Copy, Generate Unique MTS ID fields.
18. Select the XML Output Folders tab. Browse or enter the UNC of the folder location to set the Message, Attachment, and Error folders as follows based on the type of NATO CP-EXP being installed

    - Co-Hosted

      <install_drive:>\Telos\Data\XMLinput\message

      <install_drive:>\Telos\Data\XMLinput\attachment

      <install_drive:>\Telos\Data\XMLinput\error

    - Standalone

      \\<AMHS_Server>\Data\XMLInput\message

      \\<AMHS_Server>\Data\XMLInput\attachment

      \\<AMHS_Server>\Data\XMLInput\error

    - Mid-Range/Enterprise

      \\<AMHSCluster>\AMHSdata\Telos\Data\XMLinput\message

\\<AMHSCluster>\AMHSdata\Telos\Data\XMLinput\attachment

\\<AMHSCluster>\AMHSdata\Telos\Data\XMLinput\error

19. Accept the default setting for Backside Org. DN and Role File Location.
20. Select OK to close the Channel 3 Setup window. If prompted, select Yes to the next subsequent windows to allow the system to create new directories.
21. A Response window is displayed.
22. Select Close to return to the Channel Operations window.
23. Select Open Channel.
24. Select Close on the Response window.
25. Select Close on the Channel Operations window.

11.6 Configure Default Routing

1. Select on Routing from the Menu bar. Select Default Routing.
2. Enter 1 for the X400 field.
3. Enter 3 for the XML field.
4. Select OK.

11.7 DN Channel Association

The DN for each organization that the NATO CP-EXP is protecting for must be associated with an output channel. This is a new configuration requirement for this version of the NATO CP-EXP. This provides the capability to direct input X.400 messages translated to XML to be directed to different XML Backside Servers. Perform the steps listed below.

1. Select Start→CommPower XML PORTAL→Relay Editor.
2. Select the Organization Configuration tab.
3. Highlight all listed Organization DNs.
4. Select the Output Channel down-arrow to select the designation as Channel 3 and then select Yes on the Modify Multiple Records Request window.
5. Select Exit on the Relay Editor.

12. Start the Security Label Server

The SLS runs as a Service and will automatically start if properly configured whenever the system is started. However, after installation it is not properly configured and does not start after the post-install re-boot.

If the configuration steps have been performed as described above the Security Label Server (SLS) can to be manually started. Perform the steps listed below to start the SLS.

1. Select Start→Programs→Administrative Tools→Services.
2. Double-click CommPower Security Server.
3. Select Start.
4. Select Close after the Service starts.

13. Configure Relay Addressing

The NATO CP-EXP provides a consolidated Relay Editor to be used to define and configure both System Relay recipients and Client Relay recipients. The System Relay recipients are defined for the NATO CP-EXP component; however, each organization may be configured to enable or disable System Relay recipients for messages addressed to that organization. Client Relay recipients are defined for each organization, and all configurations for the Client Relay recipients are defined per Organization. The NATO CP-EXP is installed with no System Relay recipients and Client Relay recipients configured.

By default, all DNs supported by the NATO CP-EXP will be automatically populated in the Organization Configuration Table of the Relay Editor when the NATO CP-EXP is started or after a Hot Swap operation is performed. All organizations will be set to pass all message types through to the XML backside system. The System Relay will be enabled and the NATO CP-EXP Delivery End Point will be set to No.

14. Configure the NATO CP-EXP MTA With the DC Config Utility

Perform the following steps to add components to the installed DCL MTA domain and to create the routing rules that will allow the installed MTA to pass X.400 messages to/from an adjacent MTA.

Note: The MTA must be running to perform any configuration steps. The NATO CP-EXP starts the MTA as part of its startup. To start/stop the MTA manually refer to Appendix D.

14.1 Starting DC Config

1. If not already running, start the NATO CP-EXP application.
2. Select Start→Programs→DC Config→DC Config.
3. The Log on to Directory window appears. Enter the following information and then select OK to connect.
   - For Directory Server enter the hostname or IP Address of the NATO CP-EXP (as per the detail design).
   - For Username enter `/c=us/cn=mtaadmin` (as per the detail design).
   - For Password enter the DC Directory password (as per the detail design).
4. The name of the local DC IMS MTA will appear in the Select MTA window. Select the name and then select OK to continue.

Note: If another copy of the tool is started, a 'Login Conflict' warning box will appear. Select Read Only to simply examine the configuration. Select Override to log in and make changes. This warning may also occur if the DIB was shutdown incorrectly and then restarted without restarting the Windows 2003 Server. In this case shutdown and restart the Windows 2003 Server to correct the problem.

14.2 Default Association and Timing Changes

Changes to NIST timeouts and Association parameters are needed to meet grade-of-delivery requirements. This procedure sets the default settings that all MTAs defined on this NATO CP-EXP will inherit by default.

1. Select Window→Message Transfer Agents to make it the active window.
2. Locate and double-click the entry for the Home MTA.
3. The Basic Parameters tab appears. Set the NIST Timeout values to those listed in Table 14.2 -1 - NIST Timeouts.

Grade-Of-Delivery	NIST Timeout (hours)
Urgent	1
Normal	4
Non-Urgent	96

Table 14.2 -1 - NIST Timeouts

4. Select the Association Parameters tab. This tab sets the default association parameters that this MTA will use when connecting to other X400 MTAs.

5. Select the check boxes for Use separate associations for High priority messages? and for Use separate associations for Low priority messages? This will allow new values to be entered.
6. Set the values for Lifetime, Retry Interval, Number of retries and Association Threshold to the values shown in Table 14.2 -2 - Default MTA Associations.

Association	Lifetime (seconds)	Retry Interval (seconds)	Number of Retries	Association Threshold
Default association parameters	300	180	4	37
Parameters for High priority associations	300	10	3	37
Parameters for Low priority associations	300	1800	9	37

Table 14.2 -2 - Default MTA Associations

7. Select the Network Parameters tab. If the CPXP has multiple network connection, verify that IP address is set to the external NIC. When complete press OK.
8. Select Directory→Commit to save all changes.
9. Select Directory→Routing Status to determine whether your changes have been committed. Repeat this step until the message reads Successfully Loaded Routing Table at time/date local time.

14.3 Working with MTA Gateways

The NATO CP-EXP interfaces with adjacent or external X.400 DMS MTAs such as, BMTAs to send or receive messages. Reference the DMS *Detail Design* for the MTA definition you are creating.

14.3.1 Adding MTA Connections

14.3.1.1 First MTA Entry:

1. Select the Home MTA and from the MTA Menu, select Add MTA.
2. Enter the Basic MTA information.
   - Select the Basic tab and enter the following information (per the detail design):
   - Enter a unique Directory Name: (e.g., /C=US/CN=DCIMS/CN=DKBMTAQLV002 for the external MTA entry). It is recommended that this entry be the same as for the Bind Name. The entry has no affect on routing.
   - Enter the 12 character Bind Name: (e.g., DKBMTAQLV002). The bind name is the same as the Directory Name. This is case sensitive.
   - Enter the Bind Credentials: (e.g., DKBMTAQLV002). The bind credentials are the same as the Bind Name. This is case sensitive.
3. Enter information for the Adjacent Global Domain Identifier:
   - Enter the 2-digit Country Code (e.g., US for the United States).
   - Enter DMS for Administration Domain Name: (ADMD).
   - Enter a value for Private Domain Name: Leave blank if a PRMD is not used (as per the detail design).

4. For Connection Type, always leave the default: X.400 Messages (1988).

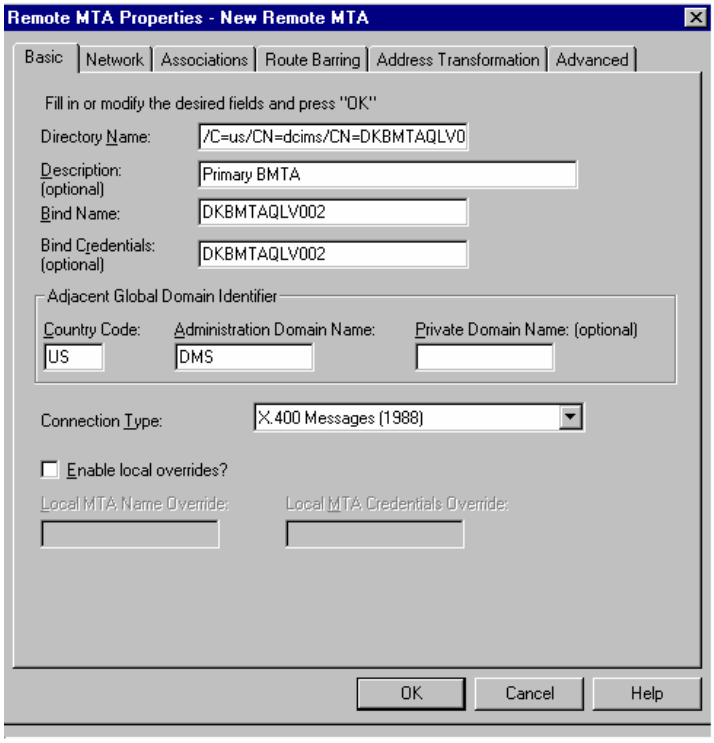

Figure 14.3.1.1 -1 New Remote MTA – Basic Tab

5. Enter the Network information.
   - Select the Network tab.
   - Enter the value for Remote TSAP. Enter `X400-88`
6. Enter `102` for Port Number.

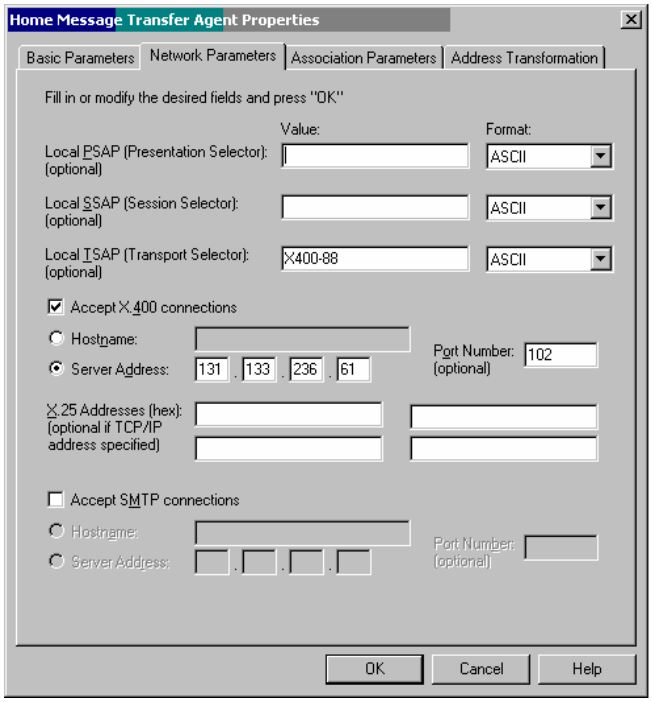

Figure 14.3.1.1 -2 New Remote MTA – Network Tab

7. For Remote Network Addresses enter the Hostname of the server; or, if DNS is not configured, select Server Address and enter the IP address of the server.
8. Select OK to continue.

Note: The first time an MTA is created the Routing Entry window displays as follows:

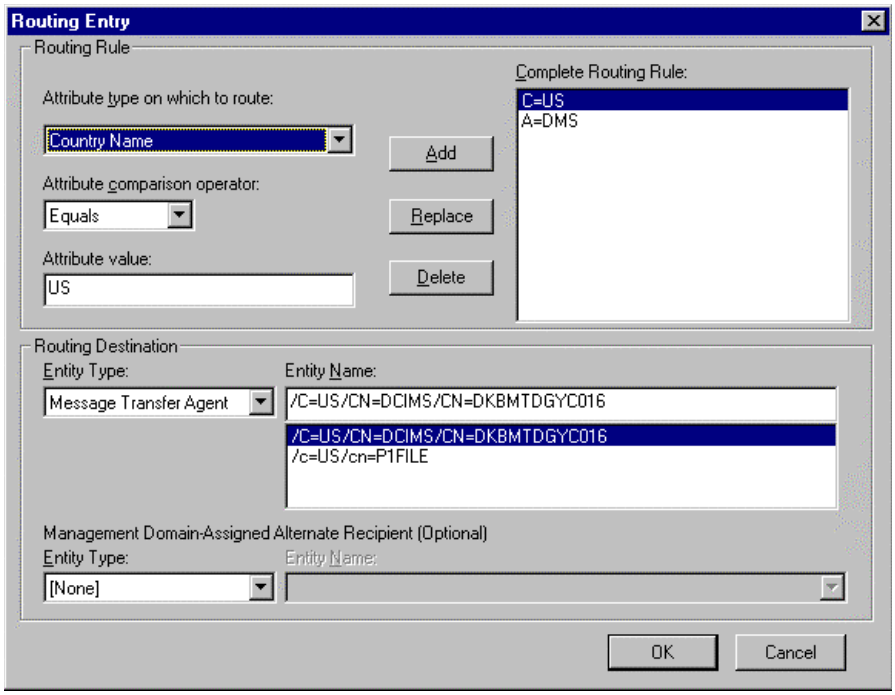

Figure 14.3.1.1 -3 Routing Entry – Default

9. Select OK.

14.3.1.2 Subsequent MTA (not a backup or tertiary MTA) Entry Creation:

1. Repeat Steps 1 – 8 of Section 14.3.1.1 to add subsequent MTA Connections.
2. Resolve the **Routing Rule Conflict** Message that appears:

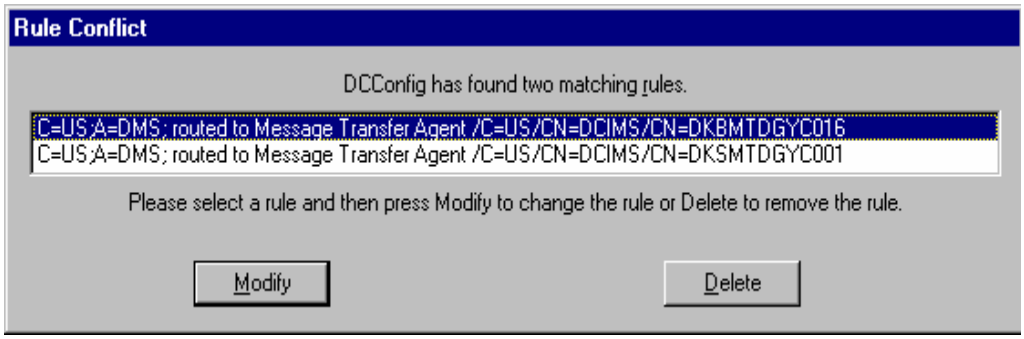

Figure 14.3.1.2 -1 Rule Conflict

3. Highlight the Subsequent MTA Entry.
4. Select Modify. The **Routing Entry** window appears:

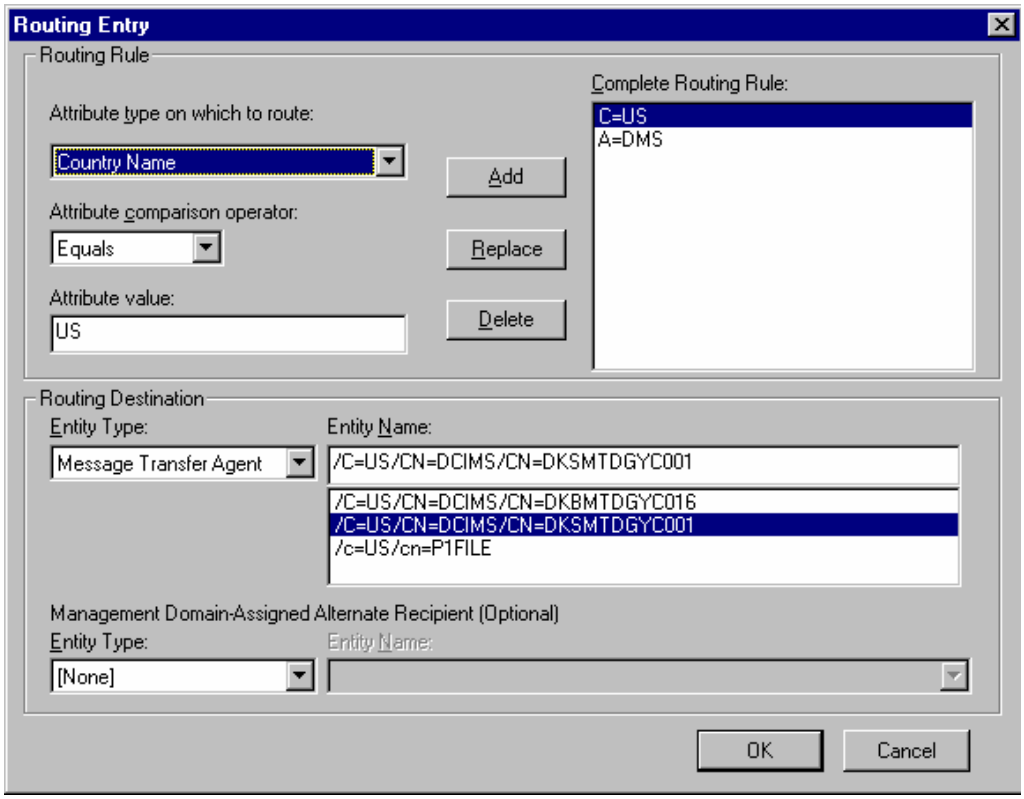

Figure 14.3.1.2 -2 Routing Entry – Configuration

5. Highlight the Entity Name MTA to which you are entering a new route. Select the Attribute type on which to route. Type in the Attribute Value. Select Add. Repeat until all attribute type entries are completed.
6. Select OK.

14.3.1.3 Secondary and Tertiary (Backup MTAs) MTA Creation:

Backup MTAs may be created in the following way:

1. Highlight the Primary MTA in the Message Transfer Agents Window.
2. Select MTAs from the window menu and then select Copy MTA.
3. Under the Basic tab, replace the last CN value in the Directory Name with the backup MTA's name.
4. Replace Description field with new MTA type.
5. Replace Bind Name with the new last CN value.
6. Replace Bind Credentials with the new last CN value.
7. Under the Network tab, replace the Remote Network Addresses with either the Hostname (if using DNS) or Server Address IP Address.
8. Select OK.
9. When the Rule Conflict Error Message Appears:
    a. Highlight the new MTA.

b. Select Delete.

c. Select OK to confirm deletion.

10. Repeat steps 1-9 for the Tertiary MTA.

14.3.1.4 Configure Alternate MTAs to the primary MTA

When completed with the above creation of subsequent MTAs, configure them as alternate MTAs to the primary MTA as follows:

1. In the Message Transfer Agent window, double-click on the Primary MTA entry.
2. Go to the Advanced tab.
3. Select the drop down arrow in the Reroute to field.
4. Select the Secondary MTA.
5. Select Add.
6. Select the Tertiary MTA.
7. Select Add.
8. Select OK.

The next section will add the default address for the NATO CP-EXP.

14.3.2 Adding P1file Connections

Select the Home MTA and from the MTAs Menu, select Add MTA.

1. Enter the Basic MTA information.
    a. Select the Basic tab and enter the following information (per the detail design):
        i. Enter a unique Directory Name: `/C=US/CN=p1file` for the server entry. The entry has no affect on routing.
        ii. Leave the Bind Name: blank.
        iii. Leave the Bind Credentials: blank.
2. Enter information for the Adjacent Global Domain Identifier:
    a. Enter the 2-digit Country Code (e.g., US for the United States).
    b. Enter DMS for ADMD.
    c. Enter a value for PRMD. Leave blank if a PRMD is not used (as per the detail design).
3. For Connection Type select: X.400 Gateway.
4. Select OK to continue.
5. If the rules Conflict Error Message appears. Make sure the P1file entry is selected.
    a. Select Modify.
    b. Set the Complete Routing Rule to the partial OR address of the NATO CP-EXP.

c. Select OK.

14.4 Routing Rules

All work for routing rules is done with the Routing Rules window active.

If additional routing rules are required, they can be added by selecting the Routing Rules window and selecting Rules→Add Rule.

14.4.1 Changing Routing Rule

1. Enter the appropriate routing information at the 'Routing Entry' window for the newly created MTA.

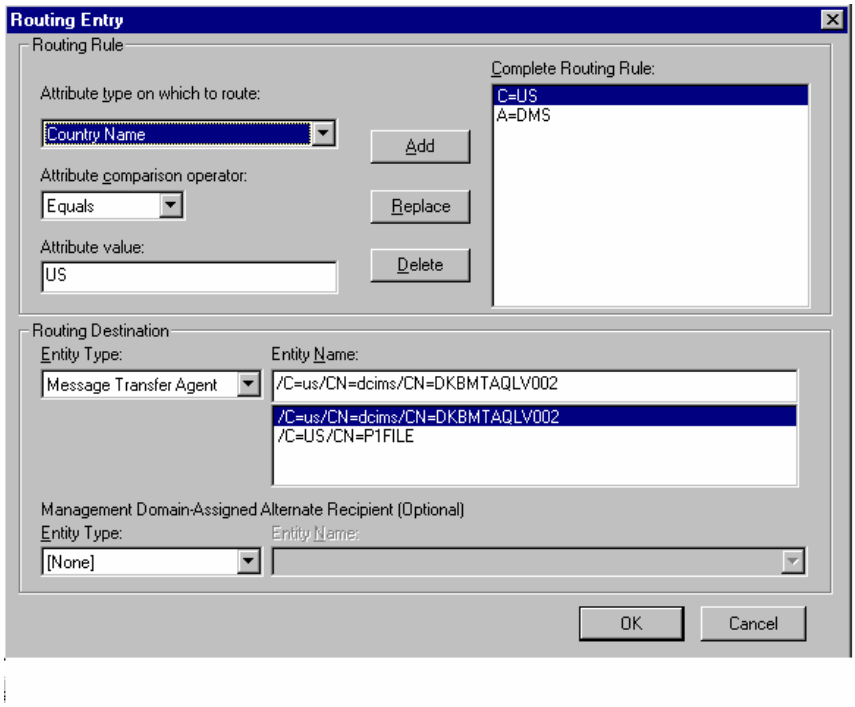

Figure 14.4.1 -1 Routing Entry – Change

2. Change default route to point the NATO CP-EXP X.400 address to the P1File. Select Default, and modify the entries in the Routing Entry window.

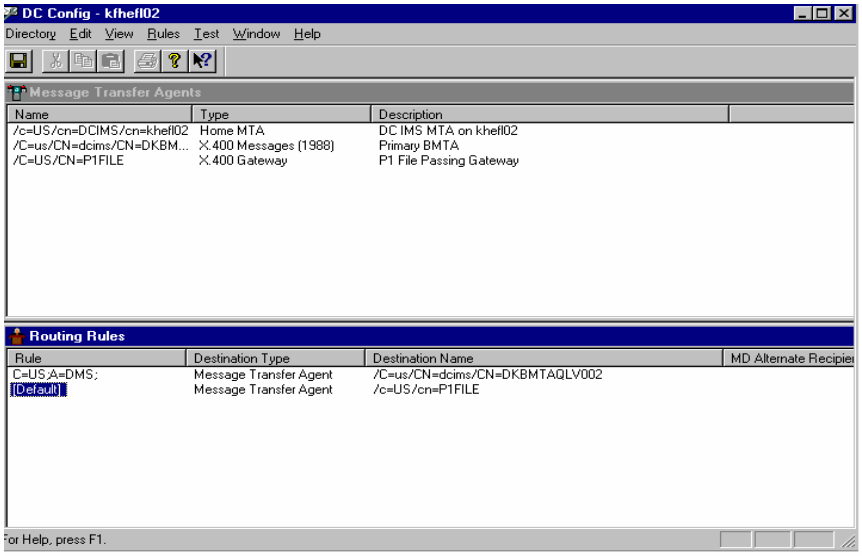

Figure 14.4.1 -2 DC Config Main Display

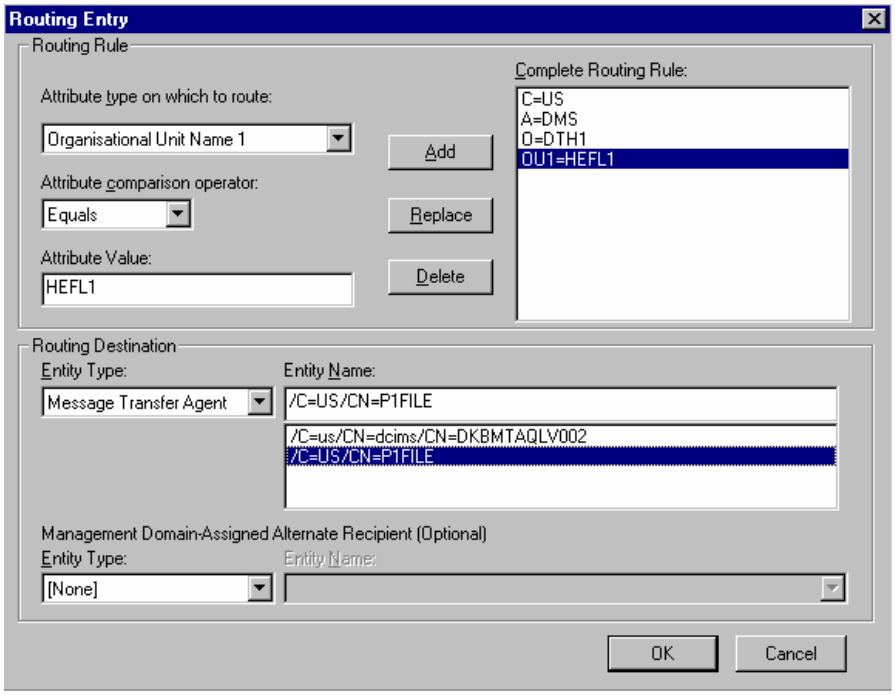

Figure 14.4.1 -3 Routing Display

14.4.2 Committing Changes

1. Once all MTAs and routing rules have been added, select Directory→Commit to save your changes.

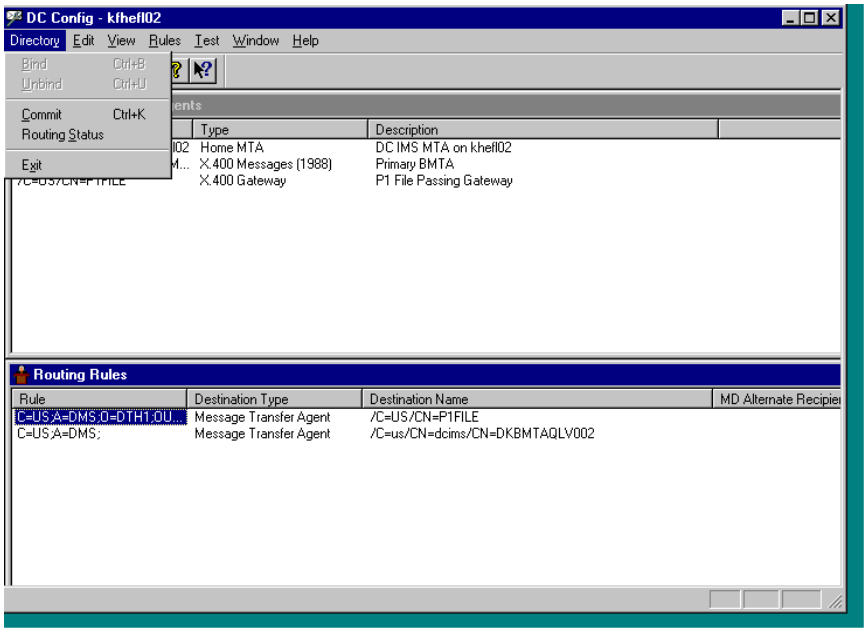

Figure 14.4.2 -1 DC Config Main Display –Commit

2. Select Directory→Routing Status. Ensure that the configuration changes have taken effect. A message will read Successfully Loaded Routing Table.

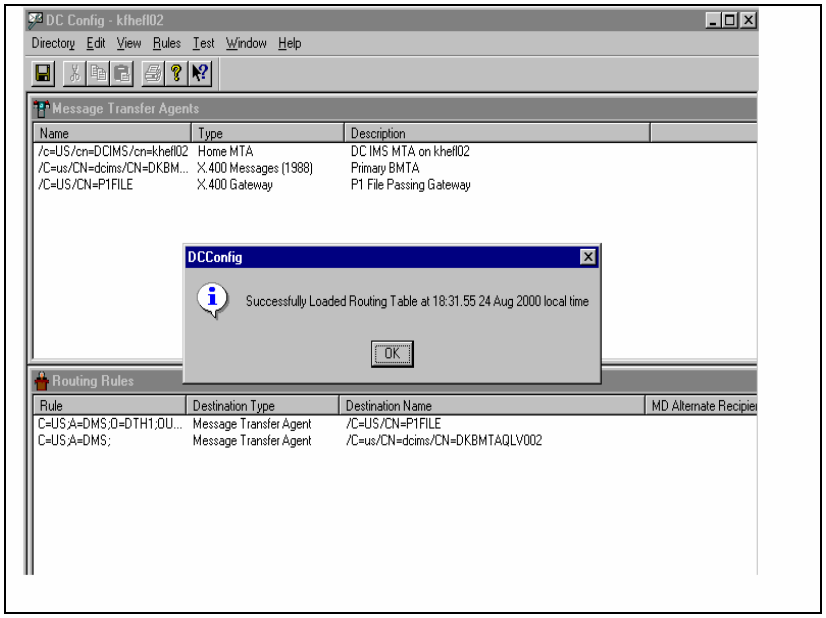

Figure 14.4.2 -2 Successful Commit

3. Select OK.
4. Directory→Exit.

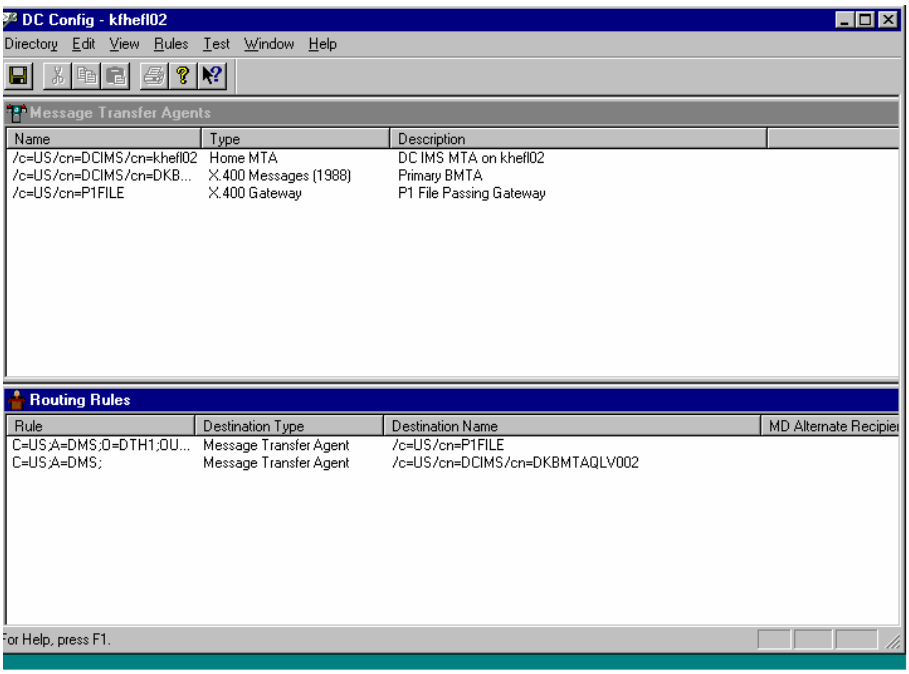

Figure 14.4.2 -3 DC Config – Configuration Complete

15. Installation of the Anti-Virus FEN, Security FEN, and IAVA FENs

15.1 Anti-Virus FEN

Perform anti-virus installation in accordance with applicable FEN(s).

15.2 Security FEN

Perform security installation in accordance with applicable FEN(s). The operator must download the applicable Security FEN for Windows 2003 Servers from DADS (3.1.2-SECURW2003-XXX where XXX is the latest version on DADS applicable to NATO CP-EXP.). This Security FEN or a later version of the FEN must be installed on NATO CP-EXP system.

Caution: Failure to follow the Post Security Script configuration completely will cause the NATO CP-EXP to become inoperable.

Appendix A: Initializing Software with Site Specific Data

As mentioned above, site specific data must be used when configuring the NATO CP-EXP. Use the detailed design documents for the site and fill in the table below.

Table A-1 - NATO CP-EXP Data Sheet

Attribute Name	Value
Physical Address (MAC ID) of the system	
NATO CP-EXP IP Address	
NATO CP-EXP Host Name	
NATO CP-EXP O/R Address	
Global Domain Identifier	
X.400 Postmaster ORAddress	
PINs for each .p12 Organizational Certificate file	Do not actually record this data
System administrators password for the NATO CP-EXP Windows 2003 Server	Do not actually record this data
NATO CP-EXP's MTA's Component Name (12 Characters)	
NATO CP-EXP's MTA's Credential (12 Characters)	
Primary DSA IP Address	
Secondary DSA IP Address (if applicable)	
Primary NTP Server hostname	
Primary NTP Server IP Address	
Secondary NTP Server hostname	
Secondary NTP Server IP Address	
Tertiary NTP Server hostname (if applicable)	
Tertiary NTP Server IP Address (if applicable)	
DNS Server IP Address	
Active Directory Domain Name	
Relay Editor data (Organizational DNs). One entry for each org the NATO CP-EXP protects for.	This data is recorded in the detail design. It is not recommended to re-record it here.
All adjacent MTAs connected to the NATO CP-EXP. Need the Component name and credentials PSAP/SSAP/TSAP values Route data.	This data is recorded in the detail design. It is not recommended to re-record it here.

Appendix B: Software Un-installation

Follow the steps listed below to remove or "un-install" the NATO CP-EXP, Security Label Server, and MTA:

1. Log onto the system as the user that installed the software.
2. Select **Start** -> **CommPower XML Portal** -> **Stop CP-EXP** to stop the NATO CP-EXP.
3. Stop the **CommPower Security Server** service.
4. Stop/Close the ADUA and DCConfig if either is running.
5. Select **Start** -> **Settings** -> **Control Panel**. Double-click on **Add or Remove Programs** to display the **Add or Remove Programs** window.
6. Highlight **CommPower NATO Security Label Server** and select **Remove**. Select **Yes** at the **Add or Remove Programs** window. If the Security Label Server was not installed on this system, skip to step 9
7. The software un-installation begins.
8. Note/Record the folders/files that were not removed.
9. Highlight **CommPower XML Portal** on the **Add or Remove Programs** window and select **Change/Remove**. Select **Remove CommPower XML Portal** option, then select **Finish**.
10. Select **Close** on the **Installation Complete** window.
11. Note/Record the folders/files that were not removed.
12. Highlight **DC Directroy Administrator** on the **Add or Remove Programs** window and select **Change/Remove**. **The Confirm File Deletion** window is displayed.
13. Select **Yes** on the **Confirm File Deletion** window. The software un-installation begins.
14. Select **Details…** on the **Remove Programs From Your Computer** window and the **Details** window is displayed.
15. Note/Record the folders/files that were not removed. Select **OK** and the **Remove Programs From Your Computer** window is displayed.
16. Select **OK** on the **Remove Programs From Your Computer** window and software removal is completed.
17. Highlight **DC Config** on the **Add or Remove Programs** window and select **Change/Remove**. The **Confirm File Deletion** window is displayed.
18. Select **Yes** on the **Confirm File Deletion** window and the window is closed and software un-installation begins.
19. Select **OK** on the **Remove Programs From Your Computer** window and software removal is completed.
20. Highlight **DC IMS** in the **Add or Remove Programs** window and select **Change/Remove**. The **Confirm File Deletio**n window is displayed.
21. Select **Yes** in the **Confirm File Deletion** window and the window is closed and software un-installation begins.
22. Select **Details…** on the **Remove Programs From Your Computer** window and the **Details** window is displayed.
23. Note/Record the folders/files that were not removed. Select **OK** and the **Remove Programs From Your Computer** window is displayed.
24. Select **OK** on the **Remove Programs From Your Computer** window and software removal is completed.
25. Select **Start** ->**Programs** ->**DC Directory Server**->**Uninstall DC Directory**. The **Uninstall DC Directory Server?** window is displayed.
26. Select **Yes** on the **Uninstall DC Directory Server?** window and software un-installation begins.
27. Select **Details…** on the **Remove Programs From Your Computer** window and the **Details** window is displayed.
28. Note/Record the folders/files that were not removed. Select **OK** and the **Remove Programs From Your Computer** window is displayed.
29. Select **OK** on **the Remove Programs From Your Computer** window.

30. Select **OK** in the untitled window recommending the system is restarted and an Information window is displayed.
31. Select **OK** in the **Information** window to complete the uninstall process.
32. Re-start the system.
33. Log onto the system as the user that uninstalled the software and manually delete the folders/files that were not removed by the un-install processes from above.

Appendix C: Notes

1. NATO CP-EXP Application Notes

a. Copy Monitor Tool and Create Shortcuts for Debugging Tools

1. Create a shortcut on your desktop for the cache utility. Name the icon **Cache Utility**. **(<install drive>:\cpe\csci\bin\mfg\bin\cache_utililty.exe**).
2. Create a shortcut on your desktop for NATO CP-EXP in debug mode. Name the icon **NATO CP-EXP debug**. (<**install drive>:\cpe\csci\bin\mfg\bin\ssr_sup.exe –debug** with the debug flag turned on "–debug").

b. Run the NATO CP-EXP debug

1. Double-click the **NATO CP-EXP debug** icon.

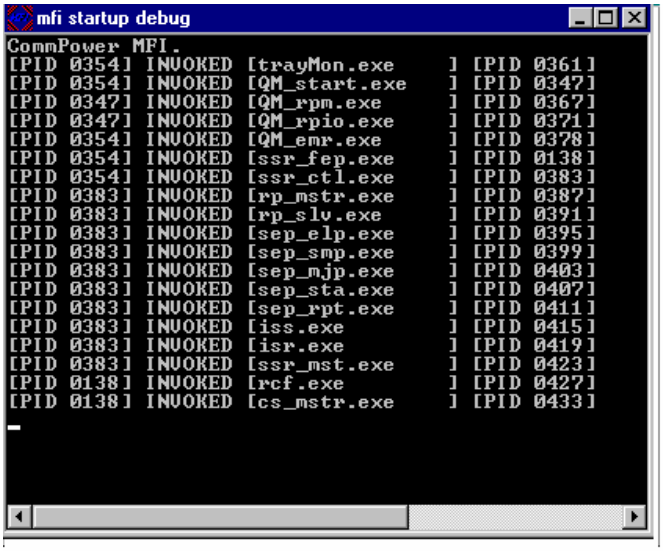

Figure C-1 – NATO CP-EXP Debug Command Prompt

a. Application Log Full Pop Up

If "The Application Log is full" window is displayed, follow the instructions on the screen to clear the Application Log.

b. User Interface Buttons

Note: If the User Interface buttons at the top of the screen are not viewable, select the maximize/minimize square in the upper right corner of the User Interface.

2. Important NATO CP-EXP/Security Label Server/MTA Log File Locations

NATO CP-EXP logs: **<install drive>:\cpe\csci\mfg\logs\ERR**

Files of note are:

- **ss.log** – System Startup/Shutdown log

- **libCS_trace.log, libCMS.log and cs.log** for cryptographic and certificate related errors
- **xd.log** - DSA requests

Security Label Server logs: **<install drive>:\cpe\cpxp\SL_Server\logs**

- **SecurityServer.log** – Security Label Server errors

DCL MTA Logs: **<install drive>:\dcims\run\dcims**

MTA Event and Activity logs:

- **EA**<date-stamp>.<time-stamp>
- **EV**<date-stamp>.<time-stamp>

For example: **EA20050507.1300**

Appendix D: DCL MTA Manual Startup/Shutdown

The DCL MTA will be started by the NATO CP-EXP application. It does not start at a system boot.

1. Manual Startup of DCL MTA

1. Manually start DC Directory Server.
   - Select **Start**→**Programs**→**Administrative Tools**→**Services**.
   - Select **DC Directory Server**→**Start**.
   - Verify that **DC Directory Server** started.
2. Manually start DC IMS Server.
   - Select **DC IMS Server**→**Start**.
   - Verify that **DC IMS Server** started.
3. DC IMS Server automatically starts DC IMS Routing Daemon.
   - Verify that **DC IMS Routing** Daemon started
4. Manually start DC IMS P1 File Gateway.
   - Select **DC IMS P1 File Gateway**→**Start**.
   - Verify that DC IMS P1 File Gateway started.
5. Manually start DC IMS Monitor Daemon.
   - Select **DC IMS Monitor Daemon**→**Start**.
   - Verify that DC IMS Monitor Daemon started.
   - Select **Close**.

2. Manual Stopping of DCL MTA

1. Manually stop DC Directory Server.
   - Select **Start**→**Programs**→**Administrative Tools**→**Services**.
   - Select **DC Directory Server**→**Stop**. (This will stop all the MTA processes)