



**Client Reference Guide for  
Microsoft DMS Outlook  
WinNT and Win2000 Clients  
DMS Release 3.0**

**Table of Contents**

**PURPOSE OF THIS DOCUMENT**.....3  
DMS OVERVIEW .....3  
WHAT’S NEW IN DMS RELEASE 3.0 .....3  
CONVENTIONS OF THIS REFERENCE .....4  
**GETTING STARTED**.....4  
VERIFYING THE SOFTWARE VERSION .....4  
    *Checking the Software Version Using the DMS  
    Splash Screen* .....4  
    *Checking the Software Version Using DMSVER*...4  
LOGGING ON THE SYSTEM .....4  
DMS ICONS.....4  
SETTING MENU CONFIGURATION .....5  
FORTEZZA CARD OPERATIONS .....5  
    *Software FORTEZZA Logon* .....5  
    *Automatic FORTEZZA logon* .....5  
    *Manual FORTEZZA Logon* .....5  
    *Selecting a FORTEZZA Role*.....6  
VIEWING MILITARY PROPERTIES.....6  
DISTINGUISHED NAME (DN) NAMING CONVENTION..6  
MESSAGING GUIDELINES BETWEEN MSP 3.0 AND  
ACP 120 .....6  
SERVER BASED DMS USER MAILBOX (A DMS  
REQUIREMENT) .....7  
**SENDING MESSAGES** .....7  
FROM FIELD POPULATION .....7  
    *Displaying the FROM Field on a Per DMS  
    Message Basis* .....7  
    *Displaying the FROM Field for all DMS  
    Messages* .....7  
    *Manually Using the FROM Field*.....7  
    *Auto-poulate FROM Field*.....7  
USING THE CONVERT BUTTON .....8  
COMPOSING A SMTP MESSAGE .....8  
SIGNING AND ENCRYPTING MGS MAIL .....8

COMPOSING A DMS MESSAGE .....9  
SIGNING AND ENCRYPTING DMS MAIL .....10  
DMS RECIPIENT AUTHORIZATION CHECKER (RAC)10  
MESSAGE SECURITY LABEL .....11  
    *Security Classification in MSP 3.0 Messages*.....11  
    *Security Labels in ACP 120 Messages* .....12  
    *Saving Security Labels* .....12  
    *Using Pre-Defined Security Labels* .....12  
REQUESTING A DELIVERY REPORT AND/OR MESSAGE  
RECEIPT .....12  
    *Requesting Delivery Reports and Read Receipts  
    for All DMS Messages* .....13  
    *Requesting Delivery Reports and Read Receipts on  
    a Per Message Basis*.....13  
SETTING MESSAGE PRECEDENCE .....13  
SETTING MESSAGE TYPES .....13  
INCLUDING AN ATTACHMENT IN A MESSAGE .....13  
FORWARDING A MESSAGE .....14  
    *Forwarding Multiple Message* .....14  
    *To forward a message without preserving the  
    Signature and/or Encryption* .....14  
    *To forward a message while preserving its  
    Signature and/or Encryption* .....14  
SAVING A DRAFT OF A MESSAGE.....14  
SETTING THE E-MAIL EDITOR .....14  
**RECEIVING MESSAGES** .....14  
OPENING A RECEIVED DMS MESSAGE.....15  
MESSAGES RECEIVED FROM THE PROFILING USER  
AGENT (PUA) .....15  
VERIFYING SIGNATURE UPON RECEIPT OF MESSAGE15  
IDENTIFYING MILITARY MESSAGE ID’S .....16  
    *Military Message Identifier (MMID)*.....16  
    *Message Transfer System Identifier (MTSID)*.....16  
RECEIVING AND VERIFYING MGS MAIL .....16  
CONFIGURING THE PRIMARY MAILBOX SENT ITEMS  
FOLDER IN A MULTI-MAILBOX CONFIGURATION .....16  
CORRELATING SIGNED RECEIPT NOTIFICATIONS.....17  
    *Method 1—Manual Correlation*.....17  
    *Method 2—Automated Correlation*.....17  
CORRELATING READ RECEIPTS FOR A SECONDARY  
MAILBOX .....18  
CORRELATING DELIVERY AND NON-DELIVERY  
NOTIFICATIONS FOR A SECONDARY MAILBOX .....18  
SAVING ATTACHMENTS SENT WITH A MESSAGE .....18  
SAVING A MESSAGE TO A FILE .....18  
ACCESSING A SAVED MESSAGE .....19  
PRINTING A MESSAGE .....19  
    *DMS Printing* .....19  
    *Standard Outlook Printing* .....19  
**DMS DIRECTORY--ACCESSING AND  
SEARCHING**.....20  
DIRECTORY OVERVIEW .....20  
DISTINGUISHING BETWEEN THE TWO DIRECTORY  
BROWSERS .....20

Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients

Lockheed Martin

Version 3.0.2M.0

USING MASTERKEYPLUS .....	20	SENDING MESSAGES FROM THE HIGH SIDE DOMAIN TO THE LOW SIDE DOMAIN .....	35
<i>The MasterKeyPlus Instances/configurations</i> .....	21	SENDING MESSAGES FROM THE LOW SIDE DOMAIN TO THE HIGH SIDE DOMAIN .....	35
<i>Finder Tools (Search tools)</i> .....	22	SENDING A MESSAGE WITH A GUARD TOKEN .....	35
<i>Search Screens</i> .....	23	<b>REFERENCE MATERIAL</b> .....	<b>36</b>
<i>Displaying additional recipient information</i> .....	23	ADDITIONAL REFERENCE MATERIAL .....	36
<i>For Normal Browser Use, Turn Off the Details</i> ..	24	<b>ORGANIZATIONAL MESSAGING</b>	
<i>Recipient Properties Displayed in the Detailed</i>		<b>ELEMENTS OF SERVICE</b> .....	<b>37</b>
<i>Browser View</i> .....	24	REQUIRED ELEMENTS OF SERVICE .....	37
<i>Attributes</i> .....	24	OPTIONAL ELEMENTS OF SERVICE .....	38
<i>Searching The DMS Directory From Within A</i>		<b>TROUBLESHOOTING GUIDE</b> .....	<b>39</b>
<i>DMS Message</i> .....	24	WARNINGS .....	39
<i>Searching the DMS Directory From Within the</i>		MGS/HGS COEXISTENCE PROBLEMS AND WORKAROUNDS .....	40
<i>Address Book Using the DMS Directory Browser</i>	24	TROUBLESHOOTING GUIDE .....	42
<b>ADVANCED FUNCTIONS</b> .....	<b>25</b>	NON-DELIVERY NOTICES (NDN) AND CORRECTIVE ACTION .....	53
ADDRESSING .....	25	HOW DO I KNOW MY DMS MESSAGE WAS DELIVERED? .....	58
<i>Determine where you are storing address</i>		SUPPORTED AND UNSUPPORTED ASCII CHARACTERS CHARTS .....	63
<i>Information (PAB or Contacts)</i> .....	25	<b>APPENDIX A: USING THE OLD 2.2 DMS</b>	
<i>Using the Personal Address Book (PAB) to</i>		<b>DIRECTORY BROWSER</b> .....	<b>69</b>
<i>Address Rich Text (RTF) Message</i> .....	25	SETTING THE SEARCH PATHS .....	69
<i>Adding an Address from a Message to the address</i>		<i>Adding an entry to the Search Paths List</i> .....	69
<i>book</i> .....	25	<i>Removing an entry from the Search Paths List</i> ...	69
<i>Changing the Display Name in Contacts</i> .....	25	<i>Editing an entry in the Search Paths List</i> .....	69
CONFIGURING USER FRIENDLY NAMES .....	25	ACCESSING THE DMS DIRECTORY USING THE DIRECTORY BROWSER.....	69
CONVERTING YOUR PERSONAL ADDRESS BOOK TO CONTACTS.....	26	MANUALLY SEARCHING THE DMS DIRECTORY .....	69
PAB/CONTACTS X.500 SYNCHRONIZATION TOOL ..	26		
<i>Updating Address Book Entries</i> .....	26		
DATE/TIME/GROUP (DTG).....	27		
<i>Displaying DTG In Inbox Viewer</i> .....	27		
<i>Changing Time and Date Format To Display Sent</i>			
<i>Time And Date In DTG Format</i> .....	27		
DMS ASCII TEXT CHECKER UTILITY .....	27		
AUTO FORWARDING A DMS MESSAGE.....	28		
RECIPIENT SPECIFIED ALTERNATE RECIPIENT (RSAR)	29		
ORIGINATOR REQUESTED ALTERNATE RECIPIENT (ORAR) .....	29		
DRAFT/REVIEW/RELEASE (DRR) PROCESS.....	29		
USING PROXY PUA TEMPLATE .....	30		
AUTODIN MESSAGING.....	31		
<i>Addressing/Sending a message to AUTODIN</i> .....	31		
<i>DMS Office Code Editor</i> .....	31		
<i>Sending a Message to an AUTODIN User</i> .....	32		
<i>Replying to an AUTODIN user</i> .....	32		
OFFLINE ACCESS .....	32		
<i>Enabling Offline Access</i> .....	32		
<i>Secure Offline Access</i> .....	32		
REMOTE ACCESS (DIAL-IN) FOR USER'S WITH SLOW MODEMS .....	33		
CONFIGURING A HIGH PRECEDENCE ALERT FOR A SECONDARY MAILBOX .....	34		
TURNING OFF AUTOSAVE .....	34		
<b>INTER-SECURITY DOMAIN MESSAGING</b> ...	<b>35</b>		
USING DMS ACROSS SECURITY DOMAINS .....	35		

## Purpose of this Document

This Client Reference Guide (CRG) provides a description of the technical capabilities of the Microsoft DMS client and a **general overview** of some DMS policies. For specific guidance on when and how to use the technical capabilities described here, refer to your own service or agency's specific policy guidelines.

## DMS OVERVIEW

The Defense Message System (DMS) version of Microsoft Outlook adds specific features to the commercial Outlook product to comply with the specifications set forth by the US Department of Defense and offers robust messaging and GroupWare capabilities in an integrated, easy to administer solution, which supports universal connectivity.

The Program's primary goal is to provide a message system that satisfies writer-to-reader requirements while reducing cost and staffing levels. Microsoft Outlook DMS provides a powerful functionality of traditional communication and collaboration systems, including a universal in-box, rich personal and group information management, and group scheduling as well as a foundation for powerful GroupWare applications such as workflow, document management, accounting, and office automation.

Microsoft Outlook DMS clients are available on Windows NT 4.0 and Windows 2000 platforms. The following instructions are generic and do not apply to a specific platform.

## WHAT'S NEW IN DMS RELEASE 3.0

The following paragraphs briefly provide an overview of some of the new features in the Release 3.0 client compared to the existing 2.2 client.

- **Contacts support.** The Microsoft DMS client has been enhanced to add Contacts support for high grade messaging. See page **25** for more detailed information.
- **Office Code Editor.** The DMS client now has an integrated Office Code Editor that supports adding office codes to both PAB and Contacts entries for AUTODIN recipients. See page **31** for more detailed information.
- **MasterKeyPlus.** A new and enhanced directory browser, MasterKeyPlus is now installed with the R3.0 DMS Client. MasterKeyPlus offers support for high grade messaging and Contacts. See page **20** for more detailed information.
- **Save security label functionality.** The sending of an ACP 120 message includes prompting the user, via the **Security Label** screen, to define the Security Label (i.e. classification and, if applicable, categories) for the message. The security label construction process can be complicated; as such DMS R3.0 client has implemented the ability to Save ACP 120 security labels. See page **12** for more detailed information.
- **DMS Recipient Authorization Checker (RAC).** DMS R3.0 introduces X.509 v3 certificates with ACP 120 access controls. Constructing a security label for ACP 120 message can be complex. The RAC allows classified messaging users to check the certificate of recipients to ensure they have appropriate certificates. See page **10** for more detailed information.
- **Configurable user-friendly names.** X.400 messages that are received from external sites (i.e. across the backbone) normally display the entire ORName (X.400 address+X.500 address) of the originator in the inbox viewer. DMS R3.0 has implemented configurable Friendly Names allowing you to configure the number of relative distinguished names (RDNs) you would like to display in their inbox viewer. See page **25** for more detailed information.
- **Auto-populate FROM field.** The Microsoft Client now has the capability to toggle the auto **FROM ...** field population to on or off. This enables the client to default the display of the **FROM ...** field to the current FORTEZZA role when a message is created. See page **7** for more detailed information.
- **PAB/Contacts Synchronization tool.** When an organizational entry is added to the PAB or

Contacts the associated security credentials are also copied to the PAB or Contacts. The PAB/Contacts Synchronization Tool provides an automated method of updating the DMS entries in the PAB or Contacts. See page 26 for more detailed information.

- **DTG ZULU display in inbox viewer.** AUTODIN uses the Date Time Group (DTG) to uniquely identify a message. The DMS R3.0 now has the capability to display DTG in ZULU time in the inbox view. See page 27 for more detailed information.
- **Delete DMS security cache from within Outlook.** The R3.0 DMS client now offers the capability to delete the DMS security cache from within Outlook. See page 26 PAB/Contacts Synchronization section for more detailed information
- **DMS Print enable/disable feature from within Outlook.** Signed and Encrypted DMS messages include a security label, which should be printed on each page. If DMS printing is enabled, it will support the printing of the security label on each printed page. DMS R3.0 now offers the capability to enable/disable this functionality from within Outlook. See page 19 for more detailed information.

## CONVENTIONS OF THIS REFERENCE

A **Bold** text indicates actual icon, button, tab, action, referenced step/section/table, typed entries, folders, tabs, or text that matches the prompts or window titles. All notes are also **Bold**.

## Getting Started

### VERIFYING THE SOFTWARE VERSION

#### CHECKING THE SOFTWARE VERSION USING THE DMS SPLASH SCREEN

When starting Outlook a warning that this is an U.S. Government System is displayed. The title bar of this window displays “**Defense Message System – Version x.x**”, where x.x is the software version number.

#### CHECKING THE SOFTWARE VERSION USING DMSVER

1. From Windows, go to **Start→Run**
2. In the **Open:** dialogue box type the following:  
**dmsver.**



You can also open a command prompt and type the command **dmsver**.

### LOGGING ON THE SYSTEM

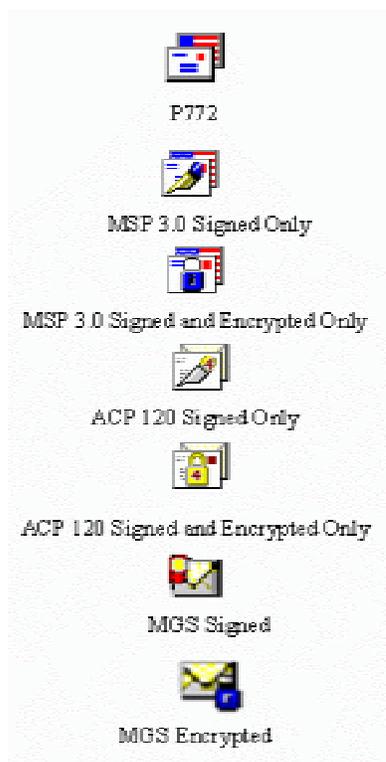
1. Double-click the **Microsoft Outlook** desktop icon to begin or click on **Start→Programs** and select **Microsoft Outlook**.
2. If the **Choose Profile** window is displayed, select your ID from the **Profile Name:** field.
3. Click **OK**.
4. The next window to appear will be the primary Outlook screen, known as the splash screen window, titled, **DMS Message System – Version X.X**. Click **Agree**, to complete the login to Outlook.



If you are prompted to identify a Guard, the Guard setup may have been incorrectly configured on the server. You may wish to cancel logging in and contact your administrator to report this.

### DMS ICONS

The icons displayed for messages in the **INBOX** provide a quick way of differentiating between the many different message types--P772, MSP 3.0 Signed Only, MSP 3.0 Signed and Encrypted, ACP 120 Signed Only, and ACP 120 Signed and Encrypted, MGS Signed, and MGS Encrypted.



### SETTING MENU CONFIGURATION

By default, commercial Outlook 2000 displays abbreviated menus. These show most recently used menu choices but not the entire menu.

To view the entire menu:

- Click the **double-arrowhead** at bottom of the menu.

To make full menus the default:

1. Select **Customize...** from the **Tools** menu.
2. Click the **Options** tab.
3. Uncheck the **Menus show recently used commands first** check box.
4. Click the **Close** button.

### FORTEZZA CARD OPERATIONS



Do **NOT** remove FORTEZZA cards from the FORTEZZA card reader while the activity light is on.

### SOFTWARE FORTEZZA LOGON

If you are a Software FORTEZZA user, you must eject any Hardware FORTEZZA cards that may be inserted into the FORTEZZA card reader prior to logging onto Software FORTEZZA. If you wish to

switch back to Hardware FORTEZZA, log off FORTEZZA and re-insert your FORTEZZA card.

1. Using the SPEX/2 utility, make sure the Software FORTEZZA stack is listed first in the Current Socket Map section.
2. If the Software FORTEZZA stack is listed in the Available Interfaces section, highlight it and use the left arrow to move the stack to the Current Socket Map section.
3. If you wish to switch back to Hardware FORTEZZA, log off of the Software FORTEZZA and re-insert your FORTEZZA card. Then using the SPEX/2 utility move the Software FORTEZZA stack down to the bottom of the list.

### AUTOMATIC FORTEZZA LOGON

FORTEZZA Security user Logon is invoked automatically when a User attempts to open or send a Signed and/or Encrypted message.

### MANUAL FORTEZZA LOGON

1. Click the **FORTEZZA Security Logon** button on the toolbar to display the FORTEZZA Security Logon window.
2. You can also log onto FORTEZZA while composing a Military message. From Compose mode, simply click the "lock and key".

**Hint** The **FORTEZZA Security Log On/Off** button looks like a **lock and key** icon on the toolbar and is also located on the compose window of a new DMS message.

The FORTEZZA Security Log On/Off buttons look like a lock and key on the toolbar. The icon with the open lock is Log off and the one with a locked lock is Log on. A Log On button is also located on the compose window of a new DMS message"



Whether logon is manual or automatic, the user is required to enter a PIN in the **Security Password** field.

2. Enter the **FORTEZZA** PIN in the **Security Password** field.
3. Clicking the **OK** button will open the window for selecting the appropriate FORTEZZA role.

**SELECTING A FORTEZZA ROLE**



The role selected is directly related to the type of messages that will be processed. When selecting a FORTEZZA role, you are effectively determining whether to process MSP 3.0 or ACP 120 messages.

1. Click the **FORTEZZA Security Logon** button to display the **'FORTEZZA Security Logon'** window.
2. When prompted enter the FORTEZZA PIN.
3. From the **Select Role** dialog box, select the desired role from the **Available:** drop-down list by clicking the drop-down arrow.
4. Click the **OK** button.



- The FORTEZZA Role selected is now predominantly displayed in the FORTEZZA Role Box on each message during message compose.
- If a FORTEZZA card is NOT available, the client will only be able to read P772 and MSP/ACP 120 signed only messages

**VIEWING MILITARY PROPERTIES**

This CRG refers to **Military Properties**, which can be found via clicking on the various Military tabs present when composing or reading a military message. These tabs are the enhanced graphic user interface (GUI) for R3.0 and consist of the following:

- Message Tab
- Military Tab
- Recipient Tab (only present in compose mode)
- Advanced Tab
- AUTODIN Tab
- Other Tab

For more detailed information on Organizational Elements of Service on a per tab basis, see **Organizational Messaging Elements of Service** Section on page 37.

**DISTINGUISHED NAME (DN) NAMING CONVENTION**

The Distinguished Name (DN) by which a user can be located in the Directory is dependent on the type of certificate the user has been issued. The address of that user is found in the Directory under the DN. When a single user has both V1 and V3 certificates, a

separate DN is required for each certificate. Considering "User" as an example the following nomenclature is used:

- User(n) denotes an Unclassified or SBU V1 certificate.
- User(s) denotes a Secret and below V1 certificate
- User(t) denotes a Top Secret and below V1 certificate
- User(uc) denotes an Unclassified V3 certificate.
- User(mc) denotes Multiple Certificates--Unclassified V3 Secret and below V3 certificate.
- User(sc) denotes Secret and below V3 certificates.
- User(tc) denotes Top Secret and below V3 certificate.

If a DN has a one-character suffix [i.e. (n), (s), or (t)], then it is only capable of supporting MSP 3.0 (V1) messages. If a DN has a two-character suffix [i.e. (uc), (sc), (mc), or (tc)], it is only capable of supporting ACP 120 (V3) messages. Guard and PLA DNs have no suffix and contain both MSP 3.0 (V1) and ACP 120 (V3) certificates and support both MSP 3.0 and ACP 120 messaging.

**MESSAGING GUIDELINES BETWEEN MSP 3.0 AND ACP 120**

The Microsoft Client supports sending messages either as a military message type (with no security services applied (i.e. P772) or with signature and/or encryption applied (i.e. MSP/ACP120) or as a commercial message type. The table below defines the guidelines to be used when originating DMS messages.

Message Type	From	To
P772	MSP 3.0 or ACP 120	MSP 3.0 & ACP 120
P42 Signed Only	MSP 3.0	MSP 3.0 & ACP 120
P42 Signed and Encrypted	MSP 3.0	MSP 3.0
ACP 120 Signed Only	ACP 120	MSP 3.0 & ACP 120
ACP 120 Signed and Encrypted	ACP 120	ACP 120

## SERVER BASED DMS USER MAILBOX (A DMS REQUIREMENT)



Setting mail to be delivered to personal folders can make encrypted messages in the **Sent Items** folder appear unencrypted.

To verify the DMS User Mailbox is Server based:

1. From the main Outlook window menu bar, select **Services...** option from the **Tools** menu.
2. Under the **Delivery** tab, verify (and change if necessary by clicking the drop-down arrow) that the field **Deliver new mail to the following location:** displays **Mailbox-<Username>**.
3. Click the **OK** button.

**DO NOT SET MAIL TO BE DELIVERED TO PERSONAL FOLDERS!**

## Sending Messages



A message may not reach its destination for various reasons. If you receive an “undeliverable” or “delivery failure” notice, refer to the NDN guide on page 53. You may be required to re-send the message or contact your local control center for assistance. Save the notice to assist in troubleshooting.

### FROM FIELD POPULATION

Population of the **From...** field is only necessary if the user has a profile with two or more mailboxes. If you are going to be sending a message from your Primary Exchange account, you do not have to define the From Field. Your Primary Account is indicated by the words **Outlook Today** next to its mailbox in the folder list.

By default all of the messages sent from the DMS Client will come from the primary mailbox. The FROM Field will only need to be selected if you are sending a new message, replying, or forwarding from your secondary Exchange Account.

When using sibling certificates, it is important that the FROM field selected is that of the First Born user so that recipients will not be confused. For example, a first born DN of `c=us/.../ou=OrgA(sc)` might have a sibling of `c=us/.../ou=OrgA(sc)/cn=Smith`

John(sc). When using the Smith John(sc) certificate to send a message on the behalf of OrgA, the user should select OrgA(sc) as the From name. Remember to always define the FROM field from the GAL.



When in doubt of your FORTEZZA role, click the FORTEZZA **Security Logon** button on the toolbar or from within the military message and select the appropriate role.

### DISPLAYING THE FROM FIELD ON A PER DMS MESSAGE BASIS

The FROM Field can be entered on a per message basis by using the **FROM** button which is present on your tool bar when composing a new message.

### DISPLAYING THE FROM FIELD FOR ALL DMS MESSAGES

1. From the main Outlook window menu bar, select **Options...** under the **Tools** menu.
2. Under the **DMS** tab, select the **View FROM Field** checkbox.
3. Click **Apply** then click **OK**.



The **FROM ...** field button will be displayed on new messages by default.

### MANUALLY USING THE FROM FIELD



If the FROM field is not selected from the GAL, the following error message will be displayed **You do not have the permission to send the message on behalf of the specified user.**

1. Click on the **FROM ...** button.
2. Select the **user's name** you would like the message to be sent from using the **'Choose Sender'** window. The message originator **MUST BE** selected from the Global Address List (GAL).

### AUTO-POULATE FROM FIELD



If you are using sibling certificates for organizational messaging Auto-population of the FROM field is not supported. The FROM field must be manually populated.

1. The Microsoft Client now has the capability to toggle the auto **FROM ...** field population to on or off. This enables the client to default the

display of the **FROM ...** field to the current FORTEZZA role when a message is created.

2. Select **Options...** from the **Tools** menu.
3. Under the **DMS** tab, select the checkbox next to **Populate FROM field with currently selected FORTEZZA Role.**
4. Click the **OK** button.



Auto population of the FROM field will not function if there is no access to the directory (e.g. if you are off-line or the Directory is not accessible). It is recommended that this capability be turned off during off-line use and the manually populating the FROM field method be used.

### USING THE CONVERT BUTTON

The client supports sending either commercial or military message. The system administrator can configure the Microsoft Client to default the compose screen to military or commercial. The convert button allows the user to toggle between the two. DMS buttons are active in military messages and commercial buttons are active in commercial messages.

### COMPOSING A SMTP MESSAGE

Click the **New** button and if necessary use the **Convert** button so that the military GUI is not visible (i.e. commercial mode). You may simply type the SMTP address into the TO, CC, or BCC field. You may also choose the SMTP address from your Personal Address Book (PAB) or Contacts. If you would like to enter the SMTP address into your Personal Address Book or Contacts, follow the steps below:

1. Select the **Address book** icon from the tool bar and click **New**.
2. In the **Select the Entry Type** box select **Internet Address** and Click **OK**.
3. Enter data in the **Display Name** (e.g., John) and **Email Address** fields (e.g., John@xyz.com).
4. Click **OK**.



You may check the **Always send to this recipient in rich-text-format** box if the recipient is another Outlook client.

### SIGNING AND ENCRYPTING MGS MAIL

The DMS system provides High Grade Service (HGS) via FORTEZZA secure message processing. Message security is a major benefit of the HGS provided by DMS, however in some cases it is more than is necessary. There is a class of messages that do not require HGS. For these messages, DMS provides Medium Grade Service (MGS).

MGS is based on the commercial Microsoft security features. Rather than using a hardware token, such as a FORTEZZA card, MGS uses a soft token in the form of a disk file created by the DoD PKI Certificate Authority. This soft token is stored on the hard drive of the user's workstation. This token provides the user with the ability to send and receive signed and encrypted messages.

DISA has created instructions that cover all the procedures necessary to configure and implement MGS including:

- Installing PKI Class 3 Certificates
- Sending Encrypted and Digitally Signed Medium Grade E-mail
- Viewing DoD PKI Certificate Details

This documentation (along with other helpful information about MGS features and operations) can be found on the World Wide Web at <http://falcon3.ncr.disa.mil>.

The document you are reading contains some very basic send/receive guidance as well as specific guidance UNIQUE to operating in coexistence mode (i.e. with BOTH HGS and MGS enabled). It is important to pay attention to the limitations listed in the **MGS/HGS Coexistence Problems and Workarounds** section to avoid pitfalls - both commercial limitations as well as those unique to coexistence.

By default MGS sign and encrypt icons are not available on the toolbar. To add these icons so they are always available during compose mode of a message do the following:



- Make sure that this is a new commercial message. If your client default composition type is commercial, then your message will already be commercial and you can continue. If your client default composition type is military, use the Convert button to convert to commercial and then

continue.

- If you would like to change your default composition type (e.g. military or commercial), contact your administrator.

1. Pull down the **Tools** menu from the new message compose window.
2. Click **Customize**.
3. Click the **Commands** tab.
4. In the **Categories** box, click **Standard**.
5. Scroll down the **Commands** box until you see

the MGS sign  and encrypt  icons.

6. One at a time, click and drag these icons up and drop them on the toolbar.



If the Sign and Encrypt icons are not available to be added to the toolbar, MGS has not been enabled. Please contact your Administrator if you desire this functionality.

Use the following steps to sign and/or encrypt an MGS message:

1. In the viewer window, click the **New Mail Message** button from the toolbar (or pull down **File→New→Mail Message** from the menu bar).
2. Make sure that this is a new commercial message. If your client default composition type is commercial, then your message will already be commercial and you can continue. If your client default composition type is military, use the Convert button to convert to commercial and then continue. Your administrator can configure this for you if it is not already configured.
3. Click the **To...** button. Choose either Contacts or the Global Address List from the **Show Names from the:** box provided.
4. Highlight a name from the Address Book selected, click **To**, **Cc**, or **Bcc** (repeat for other recipients), and then click **OK**. You can also type names directly into the **To**, **Cc**, and **Bcc** fields if you wish.
5. In the **Subject:** box, type the message subject.
6. In the message body, type message text.
7. To digitally sign the message, click the sign



button on the toolbar

8. To digitally encrypt the message, click the



encrypt button on the toolbar.

9. Click the **Send** button on the toolbar (or select **File→Send** from the menu bar).
10. When the Private Key Container dialog box appears, enter your password in the **Password** box (this is not the same as the FORTEZZA pin), do **not** check the **Remember password** checkbox (for security reasons), and click **OK**.

## COMPOSING A DMS MESSAGE



V3 Signed only messages should not be sent to 2.2 DMS clients. The message will be received but the body of the message will not be displayed. It is recommended to use the recipient's suffix [i.e. (n) or (s)] as an indicator of what type of message the recipient will be able to receive. For example, a suffix of (n) would indicate the recipient would only be able to receive V1 message types.

1. Click the **New** button (and if necessary use the Convert button so that the Military properties tabs are visible—military mode) from the toolbar (or from the **Actions** menu, select **New Mail Message** (Inbox, Outbox, Sent Items, Deleted Items, etc.); or, from the **File** menu, select **New** and then **Mail Message**).
2. Click the **TO** button.
3. Select the **Personal Address book** (PAB), **Contacts**, or the **GAL** from the **Show Names from the:** field.
4. Type a name in the **Type Name or Select from List:** field; or highlight a **name** from the displayed list beneath the field.
5. Click **TO→**, **CC→**, or **BCC→**, (repeat for other recipients).
6. Click the **OK** button.
7. In the **Subject:** field, type the message subject. (A subject is mandatory on all DMS messages).
8. Optional: If you are sending a signed or signed and encrypted message, you can also enter a **Content Description**, which is located on the **Military** tab. If you don't manually enter this information, the subject of your message will be automatically copied into the Content Description field. This field is carried in the clear on your DMS message, and therefore will be displayed in the Inbox viewer as the subject PRIOR to the message being decrypted and

opened. Once the message is decrypted and opened the internal subject will be shown in the inbox viewer.



If you do not enter a Content Description, by default, the Subject becomes the **Content Description**.

9. In the message body, type the message text.

10. If desired, insert attachments.



You cannot forward an encrypted message as an attachment through the Guard unless the Guard has a token to open the attachment.

11. Click the appropriate tab to view the screen that allows you to set other elements of service (Example: precedence and message type are within the **Message** tab, delivery report is within the **Recipients** tab, etc.).

12. Verify that the **FROM ...** field displays the desired role.



To change FORTEZZA roles at this time, see the section on **FORTEZZA Card Operations** on page 5.

When ready to send the message:

13. Click the **Send** button or select **Send** from the **File** menu.



- Messages may sometimes be held in your outbox waiting to be delivered (i.e. if you are off-line or if the server is unavailable).
- If you open a message in your Outbox folder that is awaiting delivery, you must click the **Send** button.

## SIGNING AND ENCRYPTING DMS MAIL



The **Encrypt** button automatically digitally signs messages, as well as encrypts the message.

1. Under the **Military** tab, select the checkbox(s) **Digitally sign message** and/or **Digitally encrypt message content and attachments**. (Or use the toolbar **Sign** and **Encrypt** buttons).

2. Click the **Send** button.



- A MSP 3.0 encrypted message requires a classification label. The **'Select Classification Details'** screen will come up AFTER clicking **Send**
- An ACP 120 encrypted message requires a security label. The **'Security**

**Label'** screen will come up AFTER clicking **Send**.

## DMS RECIPIENT AUTHORIZATION CHECKER (RAC)



The RAC tool is intended to help classified domain users. Most Unclassified domain users will not have any security categories. 'No valid categories for this messaging domain' may be displayed if the RAC is used to check recipient(s) with Unclassified certificates.

DMS 3.0 introduces X.509 v3 certificates with ACP 120 access controls and dynamic security policies. If you are originating a message using DMS 3.0, you need to make sure you pick the right DNs for your recipients and make sure they have appropriate certificates, and you also need to make sure that the complex security categories will work with all recipients.

- There is a visual naming convention to assist originators in selecting the right recipient type for the domain they are messaging to. Users with a **(uc)** suffix have certificates for the Unclassified domain only. Users with a **(sc)** suffix have certificates for the Secret domain only. Users with a **(tc)** suffix have certificates for the Top Secret domain only. Users with a **(mc)** suffix have certificates for both the Unclassified domain and the Secret domain.

The naming convention is important, but an originator still needs to determine the recipient's ability to receive a message because they may not be authorized for a classification or category. To find out what messaging domains, security classifications and categories recipient's are authorized for, use the Recipient Authorization Checker (RAC)—which is an integrated part of the DMS client.. The originator selects a list of recipients for a message in the message compose window and runs RAC. It shows the certificate type(s) and authorized classifications and categories (contained in the recipient's certificate) for each recipient.

To use the RAC do the following:

1. Begin a new message.
2. Select the message recipients you wish to check. You may put them on the To:, Cc: or Bcc: lines.
3. Select the **RAC** icon from the toolbar of the message being



composed.

4. The **DMS Recipient Authorization Checker** window will be displayed. On the left is the **Security Info** section. In the middle is a box labeled **Check Recipients** containing all the recipients with check boxes (checked) in front of their names. If you do not wish to check a recipient, uncheck the box in front of the name. On the right is a box labeled **Remove From Message** with all the recipients listed again, but the check boxes are unselected. The bottom of the screen is the output display area.
5. Under the **Security Info** section, select the appropriate Messaging Domain from the drop-down menu (i.e. Secret, etc.). This corresponds to the suffix on the DN you intend to use for the message, e.g. if your DN ends with (**sc**), you should select Secret for the messaging domain, even if you only intend to send an Unclassified message. If your DN suffix is (**mc**), then you would select Secret if you intend to send a classified message or Unclassified if you intend to send an Unclassified message that also needs to go to users on the NIPRNet.
6. Under **Security Policy**, select the appropriate Security Policy. For the majority this will be **GENSER Security Policy**.
7. Select the **Check Recipients** button to get a report of the authorizations of each of the selected recipients.

The output report has two parts:

- A matrix showing the message classifications each recipient is authorized for in the selected messaging domain,
- This matrix is followed by a list of each recipient giving a textual description of what security categories they can receive.

At the bottom of the report are two buttons allowing you to print the report or save it to a file. If the list includes recipients you will be sending to often, saving the report will allow you to check their authorizations before trying to send to them.

One thing to note is that you may get a message reading ‘No valid categories for this messaging domain’ for one or more recipients. This does not matter if the only categories you plan to use in your security label are Tag Type 7 informational categories. These do not require access control like the other types. Therefore, they are not included in

users’ certificates. ‘No valid categories for this messaging domain’ may also be displayed if the RAC is used to check recipient(s) with Unclassified certificates since most Unclassified domain users will not have any security categories.

The **RAC** is a useful troubleshooting tool. If you have problems sending to certain recipients and don’t understand why, the tool will tell you exactly what they are authorized to receive, so you can determine which category (or classification) caused the problem (there may be multiple mismatches for a given recipient). It is suggested that you run the RAC if you get an error message that some recipients are not authorized to receive the message (an Access control failure) and you don’t understand why. The RAC will allow you to determine whether you can remove certain parts of the message to allow you to use a label the recipient(s) can receive or whether you will just have to remove them from the message. If you decide to remove them from the message, you may check the boxes in front of their names in the **Remove From Message** list and **Exit** from the RAC. You will be prompted to confirm that you want to remove these recipients. If you select **Yes**, they will be removed from the message. If you select **No**, you are returned to the screen where you can uncheck their boxes.



The RAC checks the authorization of the message originator. However, if you are using a shared message store configuration, the RAC originator will always be the primary message store account. Microsoft is currently working on resolving this issue. Until the issue is resolved, if you would like to check the authorization of a message originator that is not the primary message store account, add the secondary message store recipient to the To: line and then choose to remove the recipient from the mail message once the authorizations have been verified.

## MESSAGE SECURITY LABEL

### SECURITY CLASSIFICATION IN MSP 3.0 MESSAGES

The sending of a MSP 3.0 message process includes prompting the user, via the **Select Classification Details** screen, to define the classification for the message. The MSP 3.0 Security classification is now automatically inserted into the first line of text of encrypted messages.

## SECURITY LABELS IN ACP 120 MESSAGES

The sending of an ACP 120 message includes prompting the user, via the **Security Label** screen, to define the Security Label (i.e. classification and, if applicable, categories) for the message.

-  • Unclassified messages do not require selection of security categories although the user can optionally select them. Classified ACP 120 messages require certain categories.
- The Security Policy defines the dependencies between an ACP 120 message's classification and category. See your Site Security Office or the ACP 120 QRG for guidance on the proper selections.
- If you have made an invalid security label tag set/category selection, selecting the **Clear All** icon on the Security Label window can clear this.

First, the classification must be selected in the **Classification** pull-down.

To add a security category:

1. In the **Tag Sets** window, click the desired tag set.
2. Click the **Add** button to move the selected tag set to the **Selected Tag Sets** list.
3. From the **Selected Tag Sets** list, click the desired Tag Set.
4. Click the **Edit** button to select the categories within the selected tag set.
5. Select the tab (**Permitted**, **Restricted**, **Enumerated**, or **TagType 7**) that contains the desired category.
6. Select the desired category in the left-hand pane and click **Add** to add it to the right-hand pane. When all the desired categories in this set have been selected, click **OK**.

 TagType 7 are categories that do not require access control, i.e. will not be included in user certificates.

7. Repeat for each Tag Set. Click **OK** on the **Security Label** screen when finished.

 For more details on constructing Security labels see your Site Security Office or the ACP 120 QRG.

The **Security Label Details** window will then come up with a summary of the security label. If the label is correct, click **OK** to send the message. Otherwise, click **Cancel**.

## SAVING SECURITY LABELS

1. Compose a new ACP 120 signed and encrypted DMS message.
2. Select desired recipients
3. Click **Send**
4. On the **Security Label** interface, select your favorite security label Tag Sets, Categories, and Classification.
5. Once all of the selections have been completed, under **Security Label Details** Section → **Security Labels** enter a descriptive security label name
6. Click the **Save** button.
7. Click **OK** to the message **The Security Label has been successfully saved to disk**.
8. Repeat above process to define each security label you would like to save.

 If you want to change classification level it may be necessary to cancel out of the security label interface and select a different ACP 120 FORTEZZA personality.

## USING PRE-DEFINED SECURITY LABELS

 A set of saved security labels has been pre-defined and included with the DMS Client CD-ROM. These should have been added during the DMS Client installation.

1. Compose a new ACP 120 signed and encrypted DMS message.
2. Click **Send**
3. From the Security Label interface, under **Security Label Details** Section → **Security Labels** click on the drop-down and select the desired pre-defined security label

 You can edit a pre-defined security label and add or delete additional tag sets/categories.

## REQUESTING A DELIVERY REPORT AND/OR MESSAGE RECEIPT

A **Delivery Report** is a system notification sent to the originator's mailbox when the message has been

delivered. A **Delivery Report** does not indicate that the message has been read.

A Read Receipt is a system notification sent to the originator when an addressee opens the message. Signed or signed/encrypted messages produce signed read receipts.

#### REQUESTING DELIVERY REPORTS AND READ RECEIPTS FOR ALL DMS MESSAGES

Delivery Reports and/or Read Receipts can be requested for all DMS messages sent. Follow the following procedure to enable this option:

1. From the main toolbar, go to **Tools**→**Options**→**DMS** tab→**Delivery Options**
2. To enable Delivery Reports for all DMS messages, select “Request a Delivery Report for all messages I send”
3. To enable Read Receipts for all DMS messages, select “Request Read Receipts for all DMS messages I send”

#### REQUESTING DELIVERY REPORTS AND READ RECEIPTS ON A PER MESSAGE BASIS

Requesting **Delivery Reports** and **Read Receipts** for messages require a recipient to be listed in the **TO...**, **CC...** or **BCC...** field. The following steps define how to request a **Delivery Report** and/or **Read Receipt** when preparing a new message.

1. Create a new message (select **New** from the toolbar or select **Actions** from the menu bar and then click **New Mail Message**).
2. Click **To...**, **CC...**, or **Bcc...**, to add the message recipients. See the **Composing a DMS Message** section on page 9 for instructions on adding recipients.
3. Click on the **Recipients** tab of the message.
4. To select a delivery report, click on the pull-down arrow and highlight the appropriate option.
5. To select a **Read Receipt**, click on the pull-down arrow and highlight the appropriate option.

#### SETTING MESSAGE PRECEDENCE

The message precedence conveys the military precedence of the message. To send a message of higher than Routine precedence, a user must be logged onto a FORTEZZA card and have the proper authorizations as part of their certificate. It is also possible to draft messages and set the military precedence without a FORTEZZA card if the SPA

settings for your inbox are appropriately configured at the Server (contact your administrator if you desire Fortezza less drafting). At least one recipient must be listed in the **TO...** (primary), **CC...** (copy), or **BCC...** (blind copy) fields to activate precedence setting capability.

1. In the **Message** tab, click the **Primary Precedence:** drop-down arrow to select the desired precedence for the **TO...** recipients.
2. If there are any **CC...** or **BCC...** recipients in the message, then in the **Message** tab, click the **Copy Precedence:** drop-down arrow to select the desired precedence for the **CC...** or **BCC...** recipients.



Precedence options available are **Routine**, **Priority**, **Immediate**, **Flash**, **ECP**, and **Critic**.

#### SETTING MESSAGE TYPES

The message type conveys the military message type of the message. Depending on SPA settings, the default Message Type will be “Individual (Working Record)” or “Other Organizational”. Contact your administrator if your client is not configured as desired.



- **Message Type:** options available are **Drill**, **Exercise**, **Individual (Working Record)**, **Operation**, **Other-Organizational** and **Project**.
- The default for an Individual User is “Individual (Working Record)”. If you are an individual user without Organizational Release capability, you must use Individual (Working Record).
- Organizational users can select other types. “Other-Organizational” is the recommended Message Type for organizational users. If you are a user with Organizational release capabilities, then you can use any other message type.

1. When composing a message, under the **Message** tab, select the desired message type from the **Message Type:** field. For example, if **Exercise** is selected for **Message Type**, you might enter **Able Archer** in the **Type ID** field.
2. Enter the optional MessageTypeID, if desired.

#### INCLUDING AN ATTACHMENT IN A MESSAGE

1. In the message being created, click the cursor in the area where the file attachment is to appear.
2. From the **Insert** menu, select **File** to display the '**Insert File**' screen.
3. Browse to the desired file. (Or type the path and file name directly in the **File name:** field.)
4. Click the **Insert** button.

## FORWARDING A MESSAGE

### FORWARDING MULTIPLE MESSAGE

With commercial Microsoft Outlook, it is possible to forward multiple messages. If you want to forward multiple messages in DMS Outlook, use the following method:

1. From the main Outlook Inbox view, select several messages using **Ctrl-Click** (non-contiguous) or **Shift-Click** (contiguous).
2. Once the multiple messages are chosen, click the **Forward** button in the toolbar to create a message that contains all of the chosen messages as attachments.
3. Address the message, add body text and click **Send**.

### TO FORWARD A MESSAGE WITHOUT PRESERVING THE SIGNATURE AND/OR ENCRYPTION

1. From within a received message click the **Forward** button (or select **Forward** from the **Actions** menu.).
2. In the **TO...** field, specify the recipients.
3. In the **FROM ...** field, specify the originator if not already specified.
4. In the message body move the cursor to the point where text is to be placed and type any comments required.
5. Click the **Send** button to send the message.

### TO FORWARD A MESSAGE WHILE PRESERVING ITS SIGNATURE AND/OR ENCRYPTION



If you are forwarding an encrypted message and preserving the original encryption, remember that the recipient must have the FORTEZZA key of one of the original recipients of the message to open it.

1. Select **New** from the toolbar to create a new mail message.

2. Select **Item...** from the **Insert** menu to display the '**Insert Item**' screen.
3. Select the **Inbox** folder (or whichever folder the message is stored in) from the '**Insert Item**' screen.
4. Double-click the message that you want to forward.
5. Address the new message.
6. Add a subject and body text to the new message.
7. Click the **Send** button.
8. If prompted with a '**Modify Security**' dialog box appears, click the **Continue** button.

## SAVING A DRAFT OF A MESSAGE

When composing or editing a message, a draft can be saved and completed later.

1. During creation of the message, Select **Close** from the **File** menu; or, click the **X** (Close) button at the right of the message title bar.
2. Select **Yes** to the **Do you want to save changes?** prompt to have the message saved in the **Drafts** folder.

To continue processing the message:

1. Open the **Drafts** folder.
2. Double-click the **Saved Message**. Use the Subject to identify it.
3. Continue editing until ready to save again or send the message.

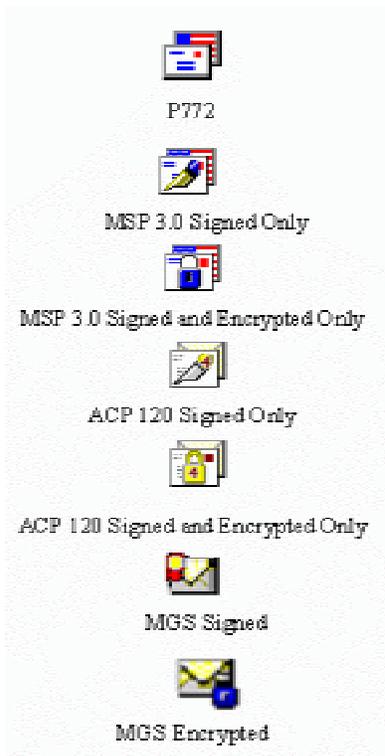
## SETTING THE E-MAIL EDITOR

Your client does NOT support the use of Microsoft WORD as an editor. Do NOT use this feature. The native outlook editor provides many of the same features (text formatting, spell checking, etc.). The DMS client is designed to send military messages from an Outlook message composition. Many of the Office Suites include a "File Send To" Mail Recipient function to invoke messaging from within that application. This feature is not supported for DMS clients.

## Receiving Messages

Your DMS client will receive a variety of military, commercial and MGS messages. Intuitive icons provide visual separation between commercial e-mail and organizational e-mail. Additional icons separate

organizational mail into clear text messages, signed-only message, and signed-encrypted messages. Other icons separate MGS messages into signed-only and signed-encrypted messages. Release 3.0 introduces additional icons to visually separate ACP 120 and MSP 3.0 protected messages.



## OPENING A RECEIVED DMS MESSAGE

 Please note, marking a DMS message as “read” is not the same as opening a DMS message. If you mark a DMS message as “read” and a signed receipt is requested...it will not be generated.

To open a message received from another user:

1. From the **Inbox** folder, double-click the message to be opened.
2. If the message is:
  - P772, the message will be opened and displayed.
  - MSP3.0/ACP 120 signed or signed and encrypted, and your previous FORTEZZA logon was inactive too long, you will be prompted to logon to FORTEZZA.
3. If FORTEZZA logon is required, enter your FORTEZZA PIN and click **OK**.

4. If the message is
  - MSP 3.0 the message will be displayed.
  - ACP120, the “**Security Label Details**” window will be displayed unless you have configured the DMS Client not to display this. Click **OK** to open and display the message.

## MESSAGES RECEIVED FROM THE PROFILING USER AGENT (PUA)

Messages from the Profiling User Agent (PUA) will arrive as a message containing both extracted content and an attachment (forwarded message).

- The information in the body of the message from the PUA contains a copy of the profiled message
- The attachment is a signed/only copy of the original message and can be used to validate the originator’s signature.

## VERIFYING SIGNATURE UPON RECEIPT OF MESSAGE

 It is critical to signed receipt verification that the appropriate FORTEZZA role be selected prior to opening the message otherwise the Signed Receipt may be generated from the wrong FORTEZZA role. If the correct FORTEZZA role is not selected the digital signature may not be verified (e.g. a V3 role must be selected to verify a V3 signature). If this occurs, close the message and select the correct FORTEZZA role and reopen the message.

To verify a message, click on **Verify** from the message toolbar and the **Verify Digital Signature** window appears. A message is displayed in the **Security Level** field stating **The message has been digitally signed and encrypted** or **This Message has been digitally signed**. The message **The digital signature was verified** will also be displayed.

1. Prior to opening the message, logon to the appropriate FORTEZZA role (again, thought this was no longer required).
2. After opening the message, select the **Verify** button.
3. Verify the accuracy of the Distinguished Name (DN) of message signer in the **Message Content Signature Signer:** area.

## IDENTIFYING MILITARY MESSAGE ID'S

Two different message ID's are available in the DMS system and can be located by opening a message and examining the Military tab.

### MILITARY MESSAGE IDENTIFIER (MMID)

This ID is typically used to correlate a 'Sent' message with a signed receipt and to reference a message from another message.

### MESSAGE TRANSFER SYSTEM IDENTIFIER (MTSID)

This ID is generated by the MTA at the time of message origination and remains unchanged from origination to final destination. This ID is typically used for message tracing.

## RECEIVING AND VERIFYING MGS MAIL

MGS messages will appear in the inbox with distinct icons.



MGS signed messages appear as an envelope with a red seal on top.



MGS encrypted or signed and encrypted messages appear as an envelope with a blue lock on bottom right of the envelope.

To open an MGS signed message and check the signature, do the following:

1. Double click the message in the inbox.
2. When the message opens, there will be a red seal icon in the lower right hand side of the header area, click this icon to verify the signature.
3. A digital signature dialog box will appear. This dialog box will display the identity of the signer and tell if the signature is valid.
4. To view the signer's certificate, click the **View Certificate** button.

To open and verify an MGS signed and encrypted message, do the following:

1. Double click the message in the inbox.
2. Enter your password in response to the prompt.
3. When the message opens, there will be a blue lock icon in the lower right hand side of the

header area, click this icon to examine encryption information.

4. An encrypted message dialog box will appear. This dialog box will display the algorithm used to encrypt the message.
5. To view the encryption certificate, click the **Encryption Certificate** button.
6. If the message is also signed, the signature can be validated as stated earlier in this section.

When you receive an MGS message, you can add the sender's address and MGS certificate to your Contacts so that you can send MGS mail to that person in the future. The Personal Address Book (PAB) does not store MGS certificates, so you should use Contacts for MGS entries. To add the sender's addresses and MGS certificate to your Contacts do the following:

1. Open the MGS message.
2. Right click on the sender's address in the header of the message.
3. From the pop-up menu that appears, select **Add to Contacts**.

## CONFIGURING THE PRIMARY MAILBOX SENT ITEMS FOLDER IN A MULTI-MAILBOX CONFIGURATION

When you send a message from your secondary mailbox address in a multi-mailbox configuration, the sent message goes into the primary mailbox's **Sent Items** folder instead of the secondary mailbox's **Sent Items** folder. This makes correlating receipts back to the secondary mailbox difficult and confusing. This can be manually corrected by moving the messages sent by the secondary user from the primary's **Sent\_Items** folder to the secondary user's **Sent Items** folder. The following steps explain how to do this.

1. In the primary mailbox, click the **Sent Items** folder to highlight it.
2. From the **View** menu, select **Current View**.
3. From the **Current View** menu, select **Customize Current View**.
4. Click the **Fields** button.
5. In the **Available Fields** list, click **From** to highlight it.
6. Click the **Add** button.
7. Highlight 'From' in the **Show these fields in the order** field.

8. Use the **Move up** and **Move down** buttons to move the field to the desired position in the list.
9. Click the **OK** button twice.
10. Sort the messages in the **Sent Item** folder, by the **From...** field, by clicking the From column heading at the top of the list.
11. Select all of the messages sent from the secondary user.



You can select a group of messages by first clicking the first message to highlight it, then, while holding down the <Shift> key, scroll down and click the last message in the list.

12. Drag selected messages to the **Sent Items** folder of the secondary mailbox and drop them there.

### CORRELATING SIGNED RECEIPT NOTIFICATIONS

There are two methods to correlate signed read receipts. Both methods assume a copy of the original message remains in a Server folder such as Sent Items.

#### METHOD 1—MANUAL CORRELATION

The signed receipt in the **Subject** column (**Inbox**) will include a subject with “Signed Receipt” in it. Open the receipt and it will automatically correlate to the sent message and the subject field will now contain the subject of the original message. If the original message is not in the **Sent Items**, the receipt subject will indicate this. To manually, correlate signed receipts:

1. Record the ‘original subject text’ from the message header bar at the top of the message window (Signed Receipt: <original subject text> Properties).
2. Close the receipt.
3. Open **Sent Items** and search on the ‘original subject text’ in the subject column. If the subject is not unique enough then refer to Method 2 to obtain the Military Message ID (MMID) that can be found on the Military tab of the Military Properties dialog box for the message.

#### METHOD 2—AUTOMATED CORRELATION

To use Method 2, a one-time setup to add the MMID to the Field Chooser.



It is not recommended to add the MMID to the Inbox box view. If you do so anyway, the MMID will not be displayed on messages that are received from external sites (sent native x.400). The MMID will ONLY be displayed on messages sent within the same site.

1. Select **View→Current View→Customize Current View→Fields** from the toolbar.
2. Click on **New Field** icon
3. Under Name enter the following exactly as shown: **MMID[#7017001e]** and leave other setting as default.
4. Click on **OK** three times.
5. Now you can correlate signed receipts to a sent item. You will use the MMID from the signed receipt as the value to search for (using the Advanced Find capability of Outlook) in the sent-items.

To use the **Advanced Find** tool to correlate messages to message receipts using the MMID, perform the following:

1. Open the signed receipt you would like to correlate.
2. Highlight and copy (use **ctrl+c**) the **MMID** of the MSP Receipt from the body of the message to the Clipboard or from the Military tab of the signed receipt.
3. Once you have copied the MMID of the signed receipt, close the signed receipt and change to the main Outlook viewer window.
4. Select **Tools→Advanced Find...** Then click on the **Advanced** tab.
5. Click the **Field** drop-down box from the **Define more criteria:** section. Select **User-defined fields** in folder→**MMID**.
6. Set the **Condition;** drop-down to **is (exactly)**.
7. In the **Value** field, paste (use **Ctrl-V**) the **MMID**.
8. Click **Add to list**.
9. Click **Browse** and select the folder to be browsed (make sure **Only the Sent Items** checkbox is selected). Click **OK**.
10. Click **Find Now**. If found, the message will be displayed in the lower section of the screen. This is the sent items (original message) for

which the signed receipt was generated. To verify, examine the MMID of the original message to match that, which was in the signed receipt.

11. Click **File→Close to Exit** to exit the **Advanced Find** tool.

### CORRELATING READ RECEIPTS FOR A SECONDARY MAILBOX

1. Ensure you have followed the directions in the section on **Configuring the Primary Mailbox Sent Items Folder in a multi-mailbox configuration** on page 16. That is...you have sorted and dragged the sent items for the secondary mailbox from the primary mailbox Sent Items to the **Sent Items** folder for the secondary mailbox.
2. Now follow directions in the section on **Correlating Signed Receipt Notifications** on page 17.

### CORRELATING DELIVERY AND NON-DELIVERY NOTIFICATIONS FOR A SECONDARY MAILBOX

When you send a message from a secondary mailbox using the **FROM** button, the sent message is saved in your primary **Sent Items** folder. However, Delivery Report (DR) and Non-delivery Notifications (NDN) for the message are returned to the *secondary Inbox*. Because of this, Outlook cannot automatically correlate the DRs and NDNs for the secondary mailbox. One way to fix this is to send from your secondary personality and then immediately (before a DR or NDN is returned) move the message from your primary **Sent Items** folder to your secondary **Sent Items** folder. Then when the DR or NDN does come back, it will be automatically correlated. If you do not move the **Sent Items** before the DR or NDN is retrieved, you can use information in the Notifications to manually correlate as follows.

For DRs:

- Open the DR. It will contain the X.400 address of the recipient that got the message and the date and time that the message was received.
- Follow the instructions in the **Correlating Read Receipts for a Secondary Mailbox** section on page 18 to move the messages sent from your secondary personality from the primary **Sent Items** folder to the secondary **Sent Items** folder.
- Examine the secondary **Sent Items** folder. Sort it by the **To...** field and use the date and time

information to find the sent message that corresponds to the DR.

For NDNs

- Open the NDN. It has the X.400 address of the recipient that got the message, the date and time the message was received, and, finally, it will have the MTS-ID of original message.
- Follow the instructions in the **Correlating Read Receipts for a Secondary Mailbox** section on page 18 to move the messages sent from your secondary personality from the primary **Sent Items** folder to the secondary **Sent Items** folder.
- Examine the secondary **Sent Items** folder. Sort it by the **Sent...** field and use the date and time information to find the sent message that corresponds to the NDN. Open the message in the **Sent Items** folder and look on the **General** tab of its properties to verify the MTS-ID.

### SAVING ATTACHMENTS SENT WITH A MESSAGE

1. Double-click to open the message with attachments or select the item in the inbox.
2. From the **File** menu, select **Save Attachments**.
3. For multiple attachments in a message, select the attachments to be saved in the **Save All Attachments** window and click the **OK** button.
4. Browse to the location where the attachments are to be saved using the **Save in:** and **File name:** fields.
5. Click the **OK** button.

### SAVING A MESSAGE TO A FILE



As long as encrypted messages are in Outlook mail folders (Inbox, Sent Items, Personal Folders, etc.) they remain encrypted. Saving them to a file will remove the encryption.

1. Open the message you want to save.
2. Select **Save As** from the **File** menu to display the 'Save As' dialog box.
3. Specify the location and name of the file to be saved in the **Save in:** and **File name:** fields.
4. Select one of the following from the **Save as Type** field.
  - a. Text Only (\*.text.)
  - b. Outlook Template (\*.oft)
  - c. Message Format (\*.MSG)
5. Click the **Save** button.



A DMS Security Extension message is displayed “Caution! Save of secure message in clear form requested”.

### ACCESSING A SAVED MESSAGE

To access a previously saved message:

1. Access Windows Explorer.
2. Access the directory where the saved message is located.
3. Double-click the saved message to display.

### PRINTING A MESSAGE

#### DMS PRINTING

Encrypted DMS messages include a security label, which should be printed on each page. If DMS printing is enabled, it will support the printing of signed only or signed and encrypted messages. Please note signed and encrypted messages will automatically be printed with classification banners on the top and bottom of each page. However, they will be printed without any rich text formatting (proportional fonts, bold, underlining, italics, etc.). If DMS printing is not enabled, signed only and signed and encrypted messages will be printed without banners, but with the rich text formatting. Enabling the DMS printing option does not affect messages that are not encrypted. Signed and encrypted V3 messages print with security markings as specified in the Security Policy Information File (SPIF).

To Enable this feature, do the following:

1. From the inbox viewer, go to **Tools** → **Options** and click on the **DMS** tab.
2. Under the **Printing** section, **enable Use DMS Printing** (check the box)
3. Click **Apply** and then **OK**.

#### STANDARD OUTLOOK PRINTING

There is a method, using Print Styles, of getting a classification to print on the header and footer of any messages and keep the rich text formatting. This method requires a user to manually choose the classification banner each time you print a message. To do this, perform the one time setup described in the following section “Preparing Print Styles”. When you want to print using these styles, follow the instructions in the “Printing an Open Message Using a Print Style” or “Printing a Message Directly from

the Message List (without opening it) Using a Print Style” sections.

#### Preparing Print Styles

1. In the menu bar in the main Outlook window, Select **Page Setup** from the **File** menu.
2. Select **Define Print Styles** from the **Page Setup** menu.
3. In the ‘**Define Print Styles**’ dialog box, highlight the **Memo** Style and click the **Copy** button.
4. In the **Style Name** field, change the name to an appropriate name for the form (e.g., if this form will be used to print unclassified messages, then name it ‘**Unclassified**’).
5. Click the **Header/Footer** tab.
6. Under the **Header:** heading in the middle box, type the appropriate header text (e.g., if this form will be used to print unclassified messages, then type in “**Unclassified**”).
7. Under the **Footer:** heading in the middle box, type the appropriate footer text (e.g., if this form will be used to print unclassified messages, then type in “**Unclassified**”). Leave the page number there if you wish.
8. Click the **OK** button.
9. Click the **Close** button.
10. Repeat this process to create styles for other classifications.

#### Printing an Open Message Using a Print Style

1. From the message menu bar, select **Print Preview** from the **File** menu.
2. Click the **Print** button.
3. In the **Print Style** field of the **Print** dialog, highlight the appropriate style.
4. Click the **OK** button.

#### Printing a Message directly from the Message List (without opening it) using a Print Style

1. Highlight the message in the list.
2. From the menu bar of the main **Outlook** window, select **Print Preview** from the **File** menu.
3. Click the **Print** button.
4. In the **Print Style** field of the **Print** dialog, highlight the appropriate style.
5. Click the **OK** button.

## DMS Directory--Accessing and Searching

### DIRECTORY OVERVIEW

The DMS Directory contains addressing and security information required to send DMS messages to individuals and organizations. For Release 3.0, the recommended method to browse and search the DMS Directory is by using MasterKeyPlus.

The preferred method of finding entities in the DMS Directory is to conduct searches. Set your search paths to areas most frequently used as this will save significant amounts of time. Directions are included in this portion of the CRG. It is also recommended that rather than expanding (browsing) large subtrees (such as the AUTODIN PLA sub-tree) that a user conduct a search.

### DISTINGUISHING BETWEEN THE TWO DIRECTORY BROWSERS

MasterKeyPlus is new in Release 3.0, but the client also retains the old DMS Directory Browser. We do NOT recommend the use of the old DMS Directory Browser in R3.0 – since it cannot be used to populate Contacts.

From the Inbox viewer toolbar:

- The **MasterKeyPlus** icon looks like this: 
- The **MasterKeyPlus** icon is also present in compose mode of a new DMS message.
- The old **DMS Directory Browser** looks like this: 

### USING MASTERKEYPLUS

MasterKeyPlus is an enhanced directory browser that contains many new features and significant improvements over the old directory browser including enhanced searching capabilities. The superior search functions are discussed in detail in the Finder Tools (Search tools) (page 22) and Search Screens (page 23) sections.

When attempting to locate an entry in the DMS directory, it is recommended that a search is conducted instead of browsing the directory for the entry. Many of the subtrees in the DMS directory contain large numbers of entries which take an extremely long time to expand and cause directory

performance issues. One example is the AUTODIN PLA subtree.

The following are general comments on MasterKeyPlus behavior:

1. MasterKeyPlus displays the contents of the directory in a similar manner as windows Explorer.
2. The left-hand pane will display all entries (subtree and leaf) that are present or you have expanded in the directory.
3. The right-hand pane displays all entries immediately subordinate (under) to the highlighted entry in the left-hand pane.
4. Clicking an entry in the left-hand pane paints or displays the subordinate subtree and leaf entries in the right-hand pane.
5. Double-clicking on an entry on the left-hand pane expands the directory entry and displays all subordinate entries (subtree and leaf). This also displays subordinate entries (subtree and leaf) in the right-hand pane.
6. Clicking on the plus (+) sign on the left-hand pane expands the entry but does NOT display the subordinate entries (subtree and leaf) in the right-hand pane.
7. Displaying entries in the right-hand pane is the same as expanding the entries in the left-hand pane. Therefore, it is important to search large branches of the directory rather than “clicking on”, selecting, or expanding the subtree.
8. When executing a search, it is important to note that the search will start from the last entry selected in the left-hand pane of the MasterKeyPlus directory browser window. Searches will not be started from a selection made in the right-hand pane even though the entry is selected. Be sure to select the appropriate starting place from the left-hand pane before conducting a search.

When attempting to locate an entry in the AUTODIN PLA subtree of the directory it is important to note the following information:

1. NEVER expand the AUTODIN PLA subtree.
2. ALWAYS use one of the search methods [see section Finder Tools (Search tools) (page 22) and Search Screens (page 23) for details] to locate an entry in the AUTODIN PLA subtree.
3. Clicking on a subtree of the AUTODIN PLA branch will display all the entries subordinate to

the subtree. Do NOT do this. Conduct a search from the main AUTODIN PLA branch.



For more detailed information concerning MasterKeyPlus installation, configuration, and operational use, see the **DMS Technical Notes for MasterKeyPlus** located in <local\_drive>:\program files\boldon james\messaging and directory\masterkey\dms technical notes.doc

**THE MASTERKEYPLUS INSTANCES/CONFIGURATIONS**

If the client has been installed per the instructions, the user will have three different MasterKeyPlus instances/configurations. For most effective search and browsing of the directory, select the configuration, which is most likely to contain the information you are looking for. The Basic configuration will search the smallest amount of data and is most likely to find the information on the local DSA and may avoid the process of chaining to other DSA locations to retrieve information. The DoD configuration searches a large percentage of the current directory and Total configuration allows searching and browsing of the entire DSA structure.

MasterKeyPlus Instance	Search level and browser starting level
X500 MasterKeyPlus DMS Basic	ou=Your lowest level,ou=DoD,o=U.S. Government,c=us
X500 MasterKeyPlus DMS DoD	ou=DoD,o=U.S. Government,c=us
X500 MasterKeyPlus DMS Total	c=us

**ACCESSING MASTERKEYPLUS**

MasterKeyPlus has several methods of locating recipients. Three of the primary methods are:

- Outlook Client Message Compose Window
- Address Book
- MasterKeyPlus Standalone Browser.

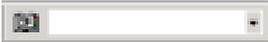
**Client Message Compose Window Method (From message screen)**

1. The MasterKeyPlus search functions may be used to add recipients from the Microsoft Outlook message compose window, (this

window could be a new note, an opened note or reply/forward note). In a new note, it is a good practice to enter the subject line before adding addresses.

2. From an open message compose window, Click one of the **To: Cc: or Bcc:** buttons.
3. From the **Select Names** window, go to the **Show names from the:** drop down menu, and **select / highlight** one of the MasterKeyPlus instances. Choose the one most likely to contain the recipient you wish to locate (example, X500 MasterKeyPlus DMS Basic).
4. Select the **Find...** button, near bottom right hand corner of screen.
5. The **Find** window will be presented. Enter the name of the recipient or organization you wish to find in the Simple or Person Finder tabs provided and select **OK**. (More details describing the use of the Finders, in later sections).
6. If your search was successful the desired recipient will be displayed in the **Select Names** window.
7. From the **Select Names** window, **highlight** the desired recipient and click one of the **To-> Cc-> or Bcc->** buttons to add their name to the note. At this time you could also right click the recipient and add them to your Outlook Contacts (or Personal Address Book).
8. Click **OK** to close the **Select Names** window and the selected names will be added to the note in progress

**Address Book Method (from primary Outlook window)**

1. From the primary Microsoft Outlook e-mail window, to find a recipient, select the **Tools** button, followed by the **Address Book...** item. (You may also select the "book" icon  if available, from the toolbar menu bar selection.).
2. From the **Address Book** window, go to the **Show names from the:** drop down menu, and **select / highlight** one of the MasterKeyPlus instances. Choose the one most likely to contain the recipient you wish to locate, (example, X500 MasterKeyPlus DMS Basic).
3. Select the **Find items** icon,  near top left hand corner of screen. (From the menu bar,

selecting **Tools > Find** will open the same window).

4. The **Find** window will be presented. Enter the name of the recipient or organization you wish to find in the Simple or Person Finder boxes provided and select **OK**. (More details describing the use of the Finders, in later sections).
5. The results of your find will be displayed in the **Address Book** window.
6. If your search was successful, at this point you would select the appropriate recipient for further action. You may wish to add the recipient to your address book. Right-click, and select Add to Personal Address Book. This will be written to either Outlook Contacts or the PAB. Your Outlook profile determines which address book is used.
7. When complete, close the **Address Book** window.
8. See **Attachment A - Using the Address Book Method** for annotated screen captures of the address book method.



Once a search has been completed, do not select the New Message icon from within the address book. You will not be able to set message precedence and you can not ask for any recipients—read or delivery. Instead add the entry to your address book, click on the new message, and add the addressee from the address book.

### **Standalone Browser**

Opening the standalone MasterKeyPlus browser is another method to access the DMS Directory. The standalone browser displays a graphical representation of the Directory hierarchy and allows the user to explore the directory structure looking for possible mail recipients.

1. To open the MasterKeyPlus browser, select the **MasterKeyPlus browser** icon from the toolbar  in the main Outlook window.
2. A new browser window will be opened. The window title will be in the format "Name of the configuration selected" - MasterKeyPlus Browser. Example title, *X500 MasterKeyPlus DMS Basic - MasterKeyPlus Browser*.
3. At this point you may find recipients by walking the directory tree, or using the **Find** icon .

4. The standalone browser may also be opened from the Client Message Compose Window by clicking the MasterKeyPlus icon available in the open message window.

### **FINDER TOOLS (SEARCH TOOLS)**



- When attempting to locate an entry in the directory browser, it is recommended that the user search for the entry instead of browsing (expanding) the directory subtrees. Searching the directory will return faster results as some subtrees of the directory contain large number of entries (e.g. AUTODIN PLA subtree). Performance and directory browser response will greatly improve by using the search method.
- When executing a search, it is important to note that the search will start from the last entry selected in the left-hand pane of MasterKeyPlus directory browser window. Searches will not be started from a selection made in the right-hand pane even though the entry is selected. Be sure to select the appropriate starting place from the left-hand pane before conducting a search.

Using either the address book or browser method, two search or “finder” tools are available: the **Simple Finder**, and the **Person Finder**. As their names suggest, they offer a degree of flexibility to the search capability. The finder tools are enabled by

selecting the Find icon “binoculars ” in the MasterKeyPlus toolbar in the browser. Using the Address Book method, select a Find button or Find Items icon “book with magnifying glass ”. Once selected, the **MasterKeyPlus Browser Search** window will open. Select the appropriate tool from the tabs provided.

### **Simple Finder**

The Simple Finder provides the most basic of the MasterKeyPlus search algorithms. The Simple Finder has a single **Name: field**. Type the name, or part of the name, of the organization, or person you are looking for into this field. Click on **OK**. MasterKeyPlus will then build a list of directory entries “starting with” the letters specified in the search field.

**Person Finder**

The Person Finder allows the user to request information using any of four fields. The default configuration provides a primary field - **Organization**: as well as three description fields. The user can also change these entries on the fly by selecting other criteria from the pull down options. Common usage would be to enter criteria in the organization field to locate an organizational recipient (or change organization to Name to locate an individual). (It may be possible to enter additional criteria to narrow down the number of possible search results, or hits.) Enter the relevant information into the fields and click on **OK**. MasterKeyPlus will build a list of directory entries that “contains” the letters specified in the search field(s).

**SEARCH SCREENS**

**Search Examples**

Some examples of recipients found if the search string "Jo" has been entered:

Type Search	Example
<b>Simple</b> Search finds organizations and individuals (Remember this is a "starts with search")	<b>Joint</b> Staff Ops, <b>Johnson, Jones</b>
<b>Person</b> Search (organization)	CDR <b>Joint</b> Command, 320/321 SQN DET AB
Person Search (name)	<b>Johnson, Jones, Laforge</b> <b>Jordi, Houltz Joanna</b>
(These are "contains" searches)	Monti <b>JO</b>

**Using a Wild Card with Simple Finder Search**

Normally the Simple Finder search uses a "starts with" search technique. This can be changed to a "contains" search by using the wildcard character "\*". If you know the recipient for which you are looking for does not start with **Jo**, but contains the string **Jo**, enter **\*Jo** in the simple finder search window. The search will return all recipients that contain **Jo**. Enter the wildcard entry \* before your search string.

The Simple Finder can be used for most searches by using the wildcard character. If you know the starting letters of the recipient for which you are searching, type them into the search area (example, MCAS Cherry Point). If you only know some of the

letters within the recipient for which you are searching, use the wildcard (example, \*Cherry Point).

If you use a “wildcard” in the Simple Finder, it works best if you have browsed to a low level in the directory structure or are using the MasterKeyPlus instance, which starts at your lowest directory level. In summary, the wildcard search can return many matches and executing the search from a low level in the directory helps to minimize the entries returned and will aid you in quickly identifying your match.

**Multiple Searches**

When doing multiple searches, in the **MasterKeyPlus Browser** Search window, the names from previous searches may be removed by checking the **Clear old results from: x500 MasterKeyPlus DMS xxx** box. If the box is unchecked, then search results will be added to any names already displayed from previous searches. Once the box is checked, for each Finder method, it will stay checked for the remainder of the session.

**Searching in the Browser**

The browser will open with the last used instance of MasterKeyPlus as the default. When the browser is opened, you may start searching to lower levels in the directory structure by highlighting lower levels in the tree view. When the browser is open, any of the installed MasterKeyPlus instances may be selected. These are available in the **Select Service** box in the upper left portion of the Browser toolbar.

**Important point:** the Simple and Person Finder Search methods are sensitive to the location of the node highlighted by the cursor. The search methods will display entries matching the criteria starting at the highlighted node and all branches below it. This allows the user to minimize the data searched by starting closer to the location of the data requested. The number of entries found and base search name is displayed in the status bar.

**DISPLAYING ADDITIONAL RECIPIENT INFORMATION**

Additional information is available when recipients are returned from searches or while browsing recipient entries in the standalone browser.

1. If you wish to view more data associated with the recipient, right-click on the recipient, and select Properties. MasterKeyPlus will display a set of tabbed property sheets for the recipient.

2. An advanced user may also wish to right-click on the recipient and then select LDAP Attributes. This will produce a screen displaying the raw LDAP attributes of the recipient.

#### **FOR NORMAL BROWSER USE, TURN OFF THE DETAILS**

There are four controls that determine how recipient properties are displayed in the right hand pane of the browser window. The control icons are located in the toolbar. The user should make a habit of using one of the first three controls available (large icon, small icon or List). Only select the Details option when you need to get additional recipient properties. Selecting the Details feature results in much slower browser response time because the details take a lot of extra time to retrieve and display. After looking at details, click one of the other options before exiting.

To change the browser display properties, from the toolbar go to **View** and select **Large Icons**, **Small Icons**, **List**, or **Details**. Under normal browser usage, use **Large Icons**, **Small Icons**, or **List**. **Details** should only be selected to view detailed properties for a specific directory entry and should be immediately changed back to one of the other setting.

#### **RECIPIENT PROPERTIES DISPLAYED IN THE DETAILED BROWSER VIEW**

In the browser, the following recipient properties will be displayed if the Details button is selected from the browser display:

- **Name:** Name of User or Organization
- **Organization:** Displayed if the item found is an Organization
- **Preferred Delivery:** Preferred delivery MHS, AUTODIN or blank.
- **mhsORAddress:** This is the recipient OR address. If this does not exist, it indicates that the recipient does not have a valid email address and will be likely to fail if entry is used to send mail.
- **V1 Cert:** A value is shown if the recipient has a V1 certification in the DSA. Not meant to be readable, just an indication that signed/encrypted messages can be sent to the user.
- **seeAlso:** seeAlso information if available
- **associatedPla:** The associated Plain Language Address (PLA) if available.
- **Description Field 1:** Descriptive information field associated with the recipient.
- **V3 Cert:** A value is shown if the recipient has a V3 certificate in the DSA. Not meant to be readable, just an indication that signed/encrypted messages can be sent to the user.

#### **ATTRIBUTES**

MasterKeyPlus can be configured to display additional directory attributes. For example, you may want to display the "phone number" attribute. This can be configured from Outlook by selecting **Tools → Services → "X500 MasterKeyPlus xxx" → Properties** button. Then **Properties Tab → Mappings... → Display Properties** → double click on the properties to be (de)selected. A flag in front of an item indicates it will be displayed. Select **OK** to exit from these dialog boxes. The added items will now be shown when recipient's details are displayed.

#### **SEARCHING THE DMS DIRECTORY FROM WITHIN A DMS MESSAGE**

1. Open new DMS message
2. Type the name of the person or organization you would like the message to be sent to
3. Press **CTRL+K**
4. **X.500 Check Names** will be displayed if the recipient is not in the PAB, Contacts or GAL.
5. Once the search has been completed, the appropriate name from the list of names display and click on **OK**.

#### **SEARCHING THE DMS DIRECTORY FROM WITHIN THE ADDRESS BOOK USING THE DMS DIRECTORY BROWSER**



These instructions can be used for either directory browser .

1. From within a new DMS message, click on the **TO:** icon.
2. Under **Selected Names** → **Show Names From the: section**, select **X.500 Directory** from the drop down window
3. Click on **Find**

4. Under **Find names containing:**, Type the name of the person or organization you would like the message to be sent to
5. Click on **OK**
6. **X.500 Check Names** will be displayed.
7. Once the search has been completed, the appropriate name from the list of names display and click on **OK** twice.



Once a search has been completed, do not select the New Message icon from within the address book. You will not be able to set message precedence and you can not ask for any recipients—read or delivery. Instead add the entry to your address book, click on the new message, and add the addressee from the address book.

RTF enabled and others without RTF enabled, the message will be sent as plain text.

If you using a PAB and would like to originate messages that contains rich text formatting (i.e. Bold, underline, picture, color, etc.), you must enable this options in the personal address book (PAB) for each recipient. To enable RTF in the PAB do the following:

1. Go to the PAB. You can do this by click on the address book icon in the main Outlook window.
2. In the **Address Book** window, select **Personal Address Book** in the **Show Names from the:** drop-down.
3. Double-click on a PAB entry.
4. Enable the **Always send to this recipient in Microsoft Outlook rich-text format** checkbox.
5. Click **Apply** and then **OK**.
6. Repeat for each recipient, you would like to enable this option on.

## Advanced Functions

### ADDRESSING

DMS R3.0 supports DMS messaging when the message is addressed from either the PAB or Contacts. Please note: MasterKeyPlus must be used to populate Contacts entries from the DMS Directory.

#### DETERMINE WHERE YOU ARE STORING ADDRESS INFORMATION (PAB OR CONTACTS)

1. From the main Outlook window, go to **Tools**→**Services** and click on the **Addressing** tab
2. Under the **Keep Personal Address In:** section click on the drop-down to choose where you would like to store address (i.e. PAB or Contacts). Contacts is the recommended address book since at some point in the future PAB support will be eliminated.

#### USING THE PERSONAL ADDRESS BOOK (PAB) TO ADDRESS RICH TEXT (RTF) MESSAGE



- You should not enable this option for AUTODIN recipients. The MFI does not accept RTF formatting and may reject the message.
- Once this option is enabled and you send to multiple recipients some with

#### ADDING AN ADDRESS FROM A MESSAGE TO THE ADDRESS BOOK

You may add an address from a message that you have received into your PAB or Contacts by doing the following:

1. Double-click the message to open.
2. Right-click any of the addresses in the **TO...** **From...** or **CC...** fields to display the selected fields popup menu.
3. Select **Add to Personal Address Book** from the displayed menu.

#### CHANGING THE DISPLAY NAME IN CONTACTS

1. Browse to the Contacts folder.
2. Double-click on the Contact entry that you would like to change the display name for.
3. On the **General** tab, edit the **Full Name...** to the desired display.
4. On the **General Tab**, edit the **File As:** name to be the desired display name.



The **Full Name...** and **File As:** name must be identical. If they are not identical, the display name may not be updated properly.

5. Click **Save and Close**.

#### CONFIGURING USER FRIENDLY NAMES

X.400 messages that are received from external sites (i.e. across the backbone) normally display the entire ORName (X.400 address+X.500 address) of the originator in the inbox viewer. The ORName can be lengthy and cause difficulties sorting/figuring out who the message originator is. DMS R3.0 has implemented configurable Friendly Names. This allows the message recipient to configure the relative distinguished names (RDNs) they would like to display in their inbox viewer. To configure Friendly Names, do the following:

1. From the inbox viewer, go to **Tools→Options→DMS** tab.
2. Under **Preferences** Section, **enable Use Friendly Names** (check the box).
3. Select the number of desired RDNs by clicking on the drop-box next to **Number of RDNs to use**. You can make a selection of 1 through 10. The default setting is 2 RDNs.

### CONVERTING YOUR PERSONAL ADDRESS BOOK TO CONTACTS

1. Prior to converting your Personal Address Book (PAB) to Contacts, it is recommended to make a copy or backup your PAB.
2. From the Inbox viewer, go to the **File→Import and Export**.
3. In the **Choose an action to perform list**, click **Import from another program or file**, and then click **Next**.
4. In the **Select file type to import from list**, click **Personal Address Book**, and then click **Next**.
5. In the **Select destination folder list**, click **Contacts**, and then click **Next**.
6. On the **Import File** window, click **Finish**.

 It may take several minutes for the import to complete.

### PAB/CONTACTS X.500 SYNCHRONIZATION TOOL

This tool synchronizes data between the DMS X.500 Directory and the Outlook Personal Address Book (PAB) or Contacts. When an organizational entry is added to the PAB or Contacts using the Microsoft DIT Browser, MasterKeyPlus, or IDUA, the Distinguished Name, E-Mail address and associated security credentials are copied from the DMS X.500 Global Directory into the PAB or Contacts. From this point on, the PAB or Contacts entry represents a local copy of the organizational entry and

maintenance is the responsibility of the user (i.e. the owner of the PAB or Contacts). This tool provides an automated method of synchronizing the DMS entries in the PAB or Contacts with the mastered information in the DMS X.500 Directory.

### UPDATING ADDRESS BOOK ENTRIES

 The PAB/Contacts Sync tools will not synchronize invalid entries (wrong certificate posted in directory into contacts. However, the PAB/Contacts Sync tool will detect expired certificates.

1. To update PAB or Contact entries go to **Tools→Synchronization→address book**

 The PAB/Contacts Sync tools will be automatically started by selecting the above.

2. At the **X.500 PAB/Contacts Synchronization Tool** window, select the appropriate address book you would like to synchronize (i.e. PAB or Contacts)
3. Once the PAB/Contacts Synchronization has completed, a summary window will be displayed indicating what was or was not updated by the tool.
4. To save the results, click on **Save Screen Status** button.
5. To exit the PAB Sync tool click on the **Close** button.
6. For more detailed information, please refer to the **PabSync.doc** located at the following: **<local\_drive>:\dms\docs\PabSync**.
7. Clear the DMS client cache (smcache.bin and X.500 cache)

- From the Inbox viewer, click on **Tools** and select **Delete DMS Security Cache** from the drop-down menu.
- Click **Yes**, to the message box **“You are about to delete the DMS security cache. This process is irreversible and you will be logged off your Fortezza card. Do you want to continue?”**.

 If you have difficulties opening or sending signed and encrypted messages, it may be necessary to delete the DMS cache file (smcache.bin) and X.500 cache. smcache.bin and X.500 cache stores certificate information locally. If the certificates have changed or are invalid, deleting this file and attempting the

operation again may resolve the issue. To delete smcache.bin from within Outlook do the following:

From the Inbox viewer, click on **Tools** and select **Delete DMS Security Cache** from the drop-down menu.

Click **Yes**, to the message box **“You are about to delete the DMS security cache. This process is irreversible and you will be logged off your Fortezza card. Do you want to continue?”**.

## DATE/TIME/GROUP (DTG)

### DISPLAYING DTG IN INBOX VIEWER

AUTODIN uses the Date Time Group (DTG) to uniquely identify a message. Because of this, if you receive many AUTODIN messages, it may be useful to you to see the DTG in the inbox view. DTG will be displayed in ZULU time. The following procedure tells how to configure the DMS Client to display the DTG in the Inbox view.

1. Open Outlook as any user.
2. From the toolbar select **View→Current View→Customize Current View→Fields** button in the View Summary dialog box.
3. Click on **New Field** icon
4. Under Name enter the following exactly as shown: **DTG[#0x7CEC001E]** and leave other setting as default.
5. Click on **OK**
6. **DTG** should now appear in the show these fields in this order list. Click and drag the **DTG** entry to the desired location on the inbox header bar and drop it there.
7. Click on **OK**.



DTG will not be displayed until the message has been opened once and then closed.

### CHANGING TIME AND DATE FORMAT TO DISPLAY SENT TIME AND DATE IN DTG FORMAT



Changing the Time and Date format will affect system time display and may also affect the format of time and date displayed in other applications.

1. Log in with administrative privileges.

2. Go to **Start→Settings→Control Panel** and select **Regional Options** for Windows 2000 and **Regional Settings** for Windows NT.
3. For Windows 2000:
  - In the **Time Format** section manually type in the following: HH:mm:ss
  - In the **Date, Short date** section manually type in the following: yyyy/mm/dd
  - In the **Date, long date** section manually type in the following: yyyy/mm/dd
4. For Windows NT:
  - From the **Time** tab, in the **Time Style** section type in the following: HH:mm:ss
  - From the **Date** tab, in the **Short Date Style** section type in the following: yyyy/mm/dd
  - From the **Date** tab, in the **Long Date Style** section type in the following: yyyy/mm/dd
5. Select **OK** and close Control Panel.

## DMS ASCII TEXT CHECKER UTILITY



The DMSASCIITextChecker executable is a utility to assist DMS to AUTODIN message drafters/releasers in avoiding inadvertent release of a message that will result in a non-delivery notification (NDN from the MFI due to invalid characters in the message). This utility can be loaded and used with any version of the DMS client. The use of this utility is provided as-is, with no warranty or software maintenance implied.

DMS to AUTODIN messaging is supported via the MFI, which provides translation of an e-mail from a DMS client into AUTODIN. The MFI translates basic ASCII characters (text) into the text based AUTODIN system. If a word processor such as Microsoft Word is used to draft a message, extended ASCII characters may be inadvertently created as part of the draft message. If this message is then released to the MFI it will result in NDN. Examples of non-supported characters include the "á" in Bogotá, the "é" in Attaché, the use of the "..." when Word makes this a single character, or in some cases the apostrophe or quotes that Word may insert can be extended ASCII characters. Unfortunately, the Microsoft product suite (Word, NotePad, Outlook) do not maintain a consistent definition of what plain text is (e.g. Outlook plain-text compose, Word save as \*.txt, Notepad saving as \*.txt). These extended ASCII characters, depending on the version of the DMS client, result in a sent item, where the entire

message is sent as an att.dat (in which case the MFI rejects the message because there is no security line) or message that includes the extended characters and is therefore rejected by the MFI.

A handy stand-alone application that will detect and identify characters that will NOT traverse the MFI (i.e. like the examples above). Simply cut and paste your text into the application and run the checker. The application will allow you to fix the characters and then either save the text to a file or cut and paste it back into your message.



If Outlook spell check is run after this utility, words containing extended character sets could be added to the message and the message will be non-delivered by the MFI. Again, the Microsoft product suite (Word, Outlook, etc.) does not maintain a consistent dictionary and spelling suggestions can vary dependent upon the application being used. Therefore, it is recommended that this utility be run after spell check and that the Outlook client be configured to not verify spelling on message submission. Spell check should be invoked manually and prior to using this utility.

1. You can run the DMS ASCII Text Checker utility on any NT or W2K desktop. There is no dependency on DMS or Outlook. It is recommended that it be used in conjunction with a DMS client releaser to ensure the final message content is checked and scrubbed for unsupported characters prior to sending the message to AUTODIN.
2. Browse to <local\_drive>:\dms (i.e. c:\dms) and find the DMSASCIITextChecker executable or select the desktop shortcut.
3. Double-click DMSASCIITextChecker.exe or the shortcut icon to execute.
4. The main DMS IA5 US ASCII Text Checker window will be displayed. Where <Paste text to be checked for IA5 content in here and then press "Check Text"> is displayed, copy the message body or text from another document (e.g. Word) and press the Check Text button.
5. If extended ASCII characters are found, the Correct Invalid ASCII Characters window will be displayed. This window will display the invalid character and the context in which the invalid character was found. You must enter a replacement character. Once a New Value

(replacement character) has been entered, click Change or Change All. Continue this process until all invalid characters have been corrected. When complete, click OK to the IA5 text checking complete message box.

6. If no invalid characters are found, click OK to the IA5 text checking complete, no invalid characters found message box.
7. Now, either select all the text in the checker, copy and then paste into new DMS mail message or you can save the text to a text file for later use by clicking the Save As button.
8. It is important to be cautious when running a spell checker. Spell check can suggest words containing extended character sets (e.g. Attaché).
9. For reference purposes, charts of both supported and unsupported ASCII Character Sets is provided in the troubleshooting section (Supported and Unsupported ASCII Character Charts) of this document.

#### AUTO FORWARDING A DMS MESSAGE

Auto Forwarding allows a user to instruct the DMS GroupWare Server (GWS) to forward the received messages to another user.



- The auto-forward recipient requires the intended recipient's FORTEZZA information and permissions to decrypt the message.
- Please read the "Warnings and Trouble Shooting" section later in this guide, as pertaining to Rules Wizard.

1. Select **Rules Wizard** from the **Tools** menu.
2. Click the **New** button.
3. Select the **Check messages when they arrive** from the displayed list.
4. Click the **Next** button.
5. Select the desired checkbox(s) for **Where my name is in TO:** and **Where my name is in CC:.**
6. Click the **Next** button.
7. Check the **forward it to people or distribution list** check box in the **What do you want to do with the message?** field.
8. Click the underlined **people or distribution list** in the **Rule description** box.

9. Scroll through the list of entries and select the target recipient. Highlight the name(s) and click the **TO** button.
10. Click the **OK** button.
11. Click the **Next** button twice.
12. Enter a name for the rule in the **Please specify a name for this rule** field.
13. Click the **Finish** button.
14. Click the **OK** button to close the 'Rules Wizard' screen.



Rules can be made 'active' or 'inactive'. An example would be to activate forwarding rules while traveling, but to deactivate them when at work.

The steps for activating and deactivating a rule are:

1. Select **Rules Wizard** from the **Tools** menu.
2. Scroll through the list of rules and find the rule in question. If the check box to the left of the rule is checked, the rule is active. If the box is unchecked, the rule is inactive.
3. Click the check box to change the rule status.
4. Click the **OK** button to exit.



- If your profile is configured with two mailboxes, you can set auto forwarding (or any Rules Wizard function) for the **PRIMARY MAILBOX ONLY**.
- In order to auto forward from your secondary mailbox (say it's called "Mailbox B"), you must have the administrator configure an additional profile that has the Mailbox M mailbox as the **PRIMARY** mailbox. Then log into Outlook using that profile and follow the steps above to configure auto forwarding for that mailbox.

### RECIPIENT SPECIFIED ALTERNATE RECIPIENT (RSAR)

The RSAR capability addresses the need for short-term redirection of incoming messages by modifying the related user registration information in the DMS GWS.



- The RSAR recipient requires the intended recipient's FORTEZZA information and permissions to decrypt the message.

- Consult your DMS administrator to configure this service.

### ORIGINATOR REQUESTED ALTERNATE RECIPIENT (ORAR)

A message originator can select the ORAR service, which includes an alternate recipient when the message is created.



The ORAR recipient **does not** require the intended recipient's FORTEZZA information and permissions to decrypt the message.

When the originator activates the service (see steps below) the client will automatically include in your message the required information for both the recipient (i.e., someone in the TO/CC) as well as his alternate. This service is activated on a per recipient basis using the following instructions:

1. Go to the DMS Directory and look up the intended recipient (e.g., Smith, John).
  2. Highlight the user and examine the user's attributes. The 'alternateRecipient' attribute is the recipient's Alternate to be used for ORAR. The attribute value is a Distinguished Name and will be used to look up the Alternate Recipient's entry in the DMS Directory.
- 
- If an 'alternateRecipient' does not exist on the DMS Directory, then the originator may select any other recipient from the PAB or Contacts to be the Alternate Recipient.
3. Select all intended recipients in **TO...** or **CC...** field(s) in your mail message.
  4. Under the **Recipient** tab, highlight the name of the recipient that will have ORAR activated in the **Recipients:** field.
  5. Under the **Alternate Recipient** field, click the **Set** button to display a list of recipients to select from.
  6. Highlight the **Alternate Recipient** from the Personal Address Book or Contacts and click the **OK** button.
  7. Repeat the two previous steps for any additional names.

### DRAFT/REVIEW/RELEASE (DRR) PROCESS

The Draft/Review/Release (DRR) cycle is a coordinated procedure that is created by a routing

script keyed to a public folder on the server. Typically, a new message is drafted and coordinated before being submitted to a “release authority” for final approval and transmission.

For further details, see the System Administrator, and refer to the section “Organizational Messaging” in the Getting Started Guide (file Dmscli.rtf) on Microsoft Outlook Client Software and Documentation CD, (Part #Z2S0303).



- The Drafter, Reviewers, and Releaser must all be in the same Exchange site for the Draft/Review/Release processes to work.
- All Reviewers and the Releaser must be included in the Draft/Review/Release (either Serial or Parallel) military message as CC: or BCC: recipients if the message starts the cycle as a signed and encrypted message or is going to be changed to a signed and encrypted message any time during the process. If you do not include the Reviewers and the Releaser, they will not be able to open the message or the message will open with a <blank> body and changes or comments cannot be made to the message. Also, when the Releaser releases the Draft/Review/Release message, it is recommended that the Releaser remove the Reviewers and the Releaser from the message unless they are also intended recipients of the message.
- The Releaser will only be able to release the Draft/Review/Release military message as a signed or signed and encrypted message.
- You can **automatically** have the Reviewers and Releaser removed from the Draft/Review/Release message by doing the following:
  1. Compose military message that will go through the Draft/Review/Release cycle.
  2. Once you have completed the message, click on the **Recipients** tab.

3. On the **Recipients** tab, a list of the message recipients will be displayed in a box on the right.
4. Select one recipient that you would like to have removed from the message when it is released by the Releaser and then check the box next to **Participant of Draft-Review Cycle** under the **Notification/Requests** section.
5. Repeat the above steps for each recipient you would like to have removed from the message when it is released by the Releaser.

### USING PROXY PUA TEMPLATE

1. Click the **Choose Form...** button on the toolbar (or select **Choose Form** from the **Forms** submenu under the **Tools** menu).
2. From the **Look In:** drop-down list, select **Organizational Forms Library**.
3. From the list of forms, select **Proxy PUA Request** and then click the **Open** button.
4. Compose the message with recipient address of the desired organizational proxy.
5. Click the **Send** button when the message is ready to be sent.
6. The **Proxy PUA Request** screen appears. You can view the current recipient addresses in this dialog (there will be no addresses until you add them). However, you cannot add or delete addresses from this dialog. It may seem like you should be able to delete addresses from this dialog, but you cannot. TO add or delete addresses, you must click the **TO...** or **CC...** buttons to get to the address list dialog (as in the next step).
7. On the **Proxy PUA Recipients:** template add all **Proxy** recipients by clicking on the **TO...** and **CC...** buttons.



You must specify at least one recipient in the **TO...** field. Make sure that the recipients selected here have an X.500 DN (e.g., NO SMTP addresses are allowed). Otherwise, an error message “Could not locate distinguish name (DN) entries for the following recipients: with recipients listed” will be displayed. The recipients listed in the error dialog box will be ignored when the message is finally sent.

8. Click the **OK** button if an error message is displayed, and re-select recipient as needed.
9. Select the **Primary Precedence** and the **Copy Precedence** in the Proxy PUA Form.
10. Select **Security Policy** type. Use the “DMS 1.0 Security Policy (MSP 3.0)” for all MSP messages.
11. For ACP 120 message only, select **Classification** type. User must select **Security Policy** type prior to selecting **Classification** type because the drop-down list for **Classification** is based upon the **Security Policy**.
12. Select **Message** type.
13. Specifying **Message Type Optional Text** is optional.
14. For ACP 120 messages only, Select **KEA Domain** type.
15. Set Security Labels.
16. Click the **OK** button to send the message.

## AUTODIN MESSAGING

### ADDRESSING/SENDING A MESSAGE TO AUTODIN



- When addressing messages to AUTODIN ensure the AUTODIN recipient is either a TO: or CC: recipient. Do not send a message to AUTODIN as a BCC: recipient.
- Always sent messages to AUTODIN in Plain Text. Do NOT send Rich Text messages. This can cause rejection notices.

Only Organizational Users can send to AUTODIN. Users that send to AUTODIN must have an associated PLA in their directory entry. If Individual users send a message to AUTODIN, the AUTODIN Gateway (the MFI) will reject it.

Be especially careful if you have a multi-mailbox configuration. If you default to your Individual account when sending, then you will have to specify your Organizational account in the From address of messages you send to AUTODIN. See the section titled “Specifying a From Address (Multi-Mailbox Configuration)”.

To Retrieve an AUTODIN address from the directory:

1. Browse the Directory down to and expand the ‘AUTODIN Pals’ subtree.
2. Locate the subtree most likely to contain the AUTODIN PLA entry and click the subtree name once, but DO NOT expand it.



If you accidentally expand the entry, it may take a considerable time to complete.

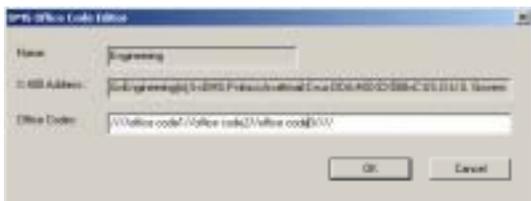
- AUTODIN PLAs are organized alphabetically within a number of subtrees. For example, to search for an entry that begins with the number 2 first browse down to the 0-5 subtree:  
  
C=US, o=U.S. Government, ou=DoD, OU=AUTODIN PLAs, OU=0-5
- Once you have highlighted the correct subtree, use the search feature in the DMS Directory Browser or MasterKeyPlus to search for the **AUTODIN** recipient.
- Once the entry is found, add it to the Personal Address Book or Contacts by highlighting it and clicking the **Add to Address Book** button in the toolbar; or, selecting **Add to Personal Address Book** or **Contacts** from the **Edit** menu.
- MasterKeyPlus can also be used to add an AUTODIN recipient to the PAB or Contacts. Note: only MasterKeyPlus supports high-grade encryption and the use of Contacts.

### DMS OFFICE CODE EDITOR

Once the appropriate AUTODIN entry has been added to the PAB or Contacts, an Office Code(s) can be added to the entry.

1. From the Inbox Viewer click on the **DMS Office Code Editor** button in the toolbar 
2. Once the **DMS Office Code Editor** window has opened, all entries containing PLANAMES (ACP-PLAD) will be displayed.
3. The Office Code Editor supports adding office codes to both PAB and Contacts entries and modifying the display name. To toggle between the PAB and Contacts, from the **Office Code Editor** window, click on the drop-down box in the **Update X.400 Address In:** section and select PAB or Contacts.
4. Select the entry, you would like to add an Office Code to and click the **Modify** button.

- The Name and the X.400 address will be displayed. Under the **Office Codes:** section enter in the desired Office Code ensuring there are 4 slashes (////) at the beginning and end and 2 slashes (//) between each office code as shown below.



- Once complete, click **OK**.



The PLA part of an AUTODIN address can be only 128 characters long. Outlook will allow you to enter more than 128 characters, but the PLA will be truncated and the extra characters will have no effect. This is something to watch if you are adding anything (i.e., office codes) to an AUTODIN address.

#### SENDING A MESSAGE TO AN AUTODIN USER



If you do send a message to an AUTODIN user with an attachment, the MFI will strip the attachment off, send the rest of the message on to the AUTODIN user, and send a commercial (P22) read receipt back to the originator. If you get a commercial read receipt that you did not expect, you probably sent a non-USMTF attachment to an AUTODIN user.

- In a new message, click **TO...** field and select the AUTODIN recipient from your Personal Address Book or Contacts.
- Click the **OK** button.



If you get a commercial read receipt that you did not expect, you probably sent an attachment to an AUTODIN user.

#### REPLYING TO AN AUTODIN USER

- Before sending a message double-click on the AUTODIN user address in the **TO...** field.
- Verify that the **Always send to this recipient in Microsoft Outlook rich-text-format** check box is unchecked and click the **OK** button.

## OFFLINE ACCESS

### ENABLING OFFLINE ACCESS



Please Note: This section only needs to be completed once to enable offline access.

You will be able to send signed and/or encrypted in offline mode **ONLY** if the necessary Certification Authorities have been copied to your PAB or Contacts. Check with the Administrator if you have any questions about which Certification Authorities need to be copied and where they should be copied from (GAL, x.500).

- Click **Services** from the **Tools** menu to display the Services screen.
- Highlight **Microsoft Exchange Server** from the list.
- Click the **Properties** button.
- Under the **Advanced** tab, select the **Offline Folder File Settings...** button.
- Enter the User's name in the **File** field or accept the default. Make sure that this file is created on a local drive **NOT** a network drive.
- Click the **OK** button to display a message box inquiring if you would like to create the file.
- Select the **Yes** button (if prompted) to create the file.
- Click the **OK** button.
- Select the **Enable offline Use** checkbox (left of the **Offline Folder File Settings...** button).
- Click the **OK** button twice.



If the user's dial-up connection is lost during the process of sending a message, the message will remain in the user's Outbox until the connection is restored.

### SECURE OFFLINE ACCESS

In order to perform secure (high-grade message encryption) in offline mode you must have all of the appropriate user certificates and certification authorities stored locally. Please do the following to ensure the necessary information is present prior to sending off-line:



When adding the appropriate entry to the PAB or Contacts using the correct directory is necessary.

- If you are using the PAB—entries can be added from either the Microsoft Directory Browser or MasterKeyPlus
  - If you are using Contacts—entries can only be added to Contacts from MasterKeyPlus. If entries are added from the Microsoft Directory Browser to Contacts, the certificate information will not be present in Contacts. The use of Contacts and high-grade encryption is only supported with MasterKeyPlus
  - If you want to use Contacts for secure DMS messaging, MasterKeyPlus must be installed and operational (MasterKeyPlus is available on the DMS client CD-ROM)
1. Complete the previous section—**Enabling Offline Access**.
  2. Add all Certification Authorities to either the PAB or Contacts for yourself, the message originator, and also the Certification Authorities for each potential recipient. The Certification Authorities include the following:
    - PAA
    - PCA
    - ICRLA (V3 only)
    - CA



Location of the Certification Authorities in the Directory are normally the following:

- PAA is located under US\U.S. National.
  - PCA is located under US\U.S. Government or service/agency name in the Directory.
  - ICRLA is located under US\U.S. Government. Note: This Certification Authority is used for V3 messaging only
  - CA(s) normally appear below the service/agency name in the Directory. They start with **CERTAUTH**.
3. If you are using Contacts and once you have added all the certificate authorities, you will need to remove extra spaces added after full stops (.) for all of the certificate authorities. If

this is not completed, you will not be able to log onto your FORTEZZA card.

4. Go to Contacts in the folder view and scan your contact entries for any certificate authorities that contains a full stop (.). The only known certificate authority with a full stop is the PAA.
5. Open the certificate authority that contains the full stop.
6. In the **File as:** section of the contact entry, remove any extra spaces that were automatically added to the contact entry by Outlook. If you are unsure if an extra space was automatically inserted, the **File As:** name should match the name that appears in the directory.
7. Once complete, click on the **Save and Close** button. Repeat these steps for each certificate authority present in Contacts.
8. Add all potential message recipients to either the PAB or Contacts including yourself, the message originator. The recipients must be added from the DMS directory browser or from MasterKeyPlus if you will be using Contacts for messaging.
9. It is recommended to periodically run the PAB/Contacts Synchronization Tool to ensure all the entries in your PAB or Contacts contain the most up-to-date certificate information available in the directory. Running the tool update certificates, CRLs, CKLs, and ICRLs. Please run this tool prior to any off-line use.

#### REMOTE ACCESS (DIAL-IN) FOR USER'S WITH SLOW MODEMS

Under normal circumstance, it is not necessary to perform these procedures for Remote Access or dial-in. However, if you are using an extremely slow modem (14.4 or below) the following is the recommended procedure for remote access:

1. Prior to going in a Remote Access or dial-in situation (i.e. when online) do the following: under the **Off-line Access** section of this CRG complete **Enabling Off-line Access**.
2. If you will be performing and secure off-line messaging (signed and encrypted) complete the **Secure Off-Line Access** section. If you are unsure what type of messaging you will be performing off-line, please complete both sections.
3. Go into off-line mode.
4. Send message, reply, forward, or perform desired e-mail activities

5. Connect remotely
6. Synchronize (send, receive mail, etc.)
7. Exit outlook
8. Go off-line again and repeat steps 3-6 as necessary until messaging needs are met.

### CONFIGURING A HIGH PRECEDENCE ALERT FOR A SECONDARY MAILBOX

By default the DMS Outlook Client software is configured to alert the user when a high precedence message arrives (this is part of the DMS installation procedures). However, if your profile includes a secondary mailbox, that mailbox will NOT have an alert for high precedence messages by default. This section explains how to configure a secondary mailbox to have a high precedence alert. This procedure will require some assistance from your administrator.

To configure this alert for the secondary mailbox, you must perform the following one time procedure:

1. Assume that your primary mailbox is "Mailbox A" and your secondary mailbox is "Mailbox B".
2. With the help of your administrator, create a profile that has Mailbox B (your secondary) as its primary (or more commonly its only) mailbox. We will call this profile B and your original (multi-mailbox) profile A.
3. Log into Outlook using profile B.
4. Select the **Rules Wizard** option from the **Tools** menu to display the **Rules Wizard** screen.
5. Click **New** to create the rule.
6. Click the **Next** button.
7. Check **marked as importance**, in the top window.
8. Click **importance** in the bottom window.
9. Click **High** from the pull down list and click the **OK** button.
10. Click the **Next** button.
11. Check **forward it to people or distribution list** in the top window.
12. Click **people or distribution list** in the bottom window.
13. In the address window that appears, select your primary mailbox (Mailbox A) from the PAB, Contacts, or GAL, by double-clicking it and click the **OK** button.
14. Click the **Finish** button.
15. Click the **OK** button.

16. Select **Exit and Log Off** from the **File** menu.
17. Start Outlook again, but this time logon with your original profile (Profile A).
18. Select **Rules Wizard** from the **Tools** menu.
19. Click **New**.
20. Click the **Next** button.
21. Select the check the box, **from people or distribution list**, in the top window.
22. Click **people or distribution list**, from the list in the bottom window.
23. From the address window that appears, select your secondary mailbox (Mailbox B) from the GAL by double-clicking it and click the **OK** button.
24. Scroll down the top window and select the **which has an attachment** checkbox.
25. Click the **Next** button.
26. Check **Notify me using a specific message** in the top window.
27. Click **a specific message** in the bottom window.
28. Type: **You have received an Urgent Grade of Delivery Message in your 'Mailbox B' mailbox**.
29. Click the **OK** button.
30. Check the **delete it** check box.
31. Click the **Finish** button to display a message informing you **This rule is a client only rule, and will only process while Outlook is running**. Select **OK** twice.

Now when a message marked with high importance arrives at your secondary mailbox, it will be forwarded to your primary mailbox.

An alert from the primary mailbox will be issued and the message will be deleted from the primary mailbox (which is OK because it is in your secondary mailbox).

### TURNING OFF AUTOSAVE

AutoSave is a commercial Outlook feature that saves messages that are in-work periodically. This allows recovery of the messages in case of a system or application hang. Although this is a desirable feature, **AutoSave cannot be used in conjunction with a DMS client**. If a DMS signed/encrypted message is AutoSaved by the client and is subsequently sent, the message will be blank when it arrives at the recipient's client. The DMS client installation procedures instruct the installer to disable AutoSave.

However, in case AutoSave is accidentally enabled, it can be disabled again with the following procedure:

1. From the main Outlook window, pull down **Tools**→**Options**.
2. Click the **E-mail Options** button.
3. If the **Automatically save unsent messages** checkbox is checked, uncheck it.
4. Click **OK** to close the **E-mail Options** dialog.
5. Click **OK** to close the **Options** dialog.

## Inter-Security Domain Messaging

### USING DMS ACROSS SECURITY DOMAINS

DMS is comprised of multiple security domains. For clarity, all references to security domains will be done using the terms, high side and low side (of the Guard). For example, in a domain model of SIPRNET and NIPRNET, the SIPRNET domain would be on the high side and the NIPRNET domain would be the low side

Users of a specific security domain can exchange messages among the other security domains, as well as within their own security domain. For example, users on a Secret security domain are able to send messages labeled Secret and below within their own security domain, and these users are also able to exchange unclassified messages with users on the unclassified security domain. Each user that needs to communicate across security domains will have a separate mailbox for each security domain.



You cannot forward an encrypted message as an attachment through the Guard unless the Guard has a token to open the attachment.

### SENDING MESSAGES FROM THE HIGH SIDE DOMAIN TO THE LOW SIDE DOMAIN



To send a message from the High side domain to the Low side domain, the message must be signed and encrypted and a Guard token must be included.

1. Verify that you are logged into the FORTEZZA card and have selected the appropriate role (MSP 3.0/ACP120) on the card (See the section “**Selecting a FORTEZZA Role**” page 6).
2. Open a new mail message.

3. Select the encryption service.
4. When accessing multiple mailboxes from the same Outlook profile and you want to send from a secondary mailbox, you will need to specify this in the **FROM** field. Click the **FROM** button and select the desired mail address from the list (See the section “**Manually Using the FROM Field**” page 7”).
5. The administrator can set up the server to have your client automatically add a Guard token to your message. Check with your Administrator if you have any questions on whether your server is configured to automatically add a Guard token.
6. Complete the message as normal.
7. Click the **Send** button.
8. Complete the message send process by setting the security label.

### SENDING MESSAGES FROM THE LOW SIDE DOMAIN TO THE HIGH SIDE DOMAIN



Low to High messaging is evolving on the DMS Program. Currently, most Guard implementations are using what is referred to as “sibling certificates” at the Guard for low to high messaging. What this means to YOU, a message originator is simply, if you are on the access control list for low to high messaging to the Guard, simply ensure that your message is properly addressed to the high side user, has the proper military properties constructed, select signed and encrypted and send your message.

### SENDING A MESSAGE WITH A GUARD TOKEN

This is a procedure to manually add a Guard Token to a message. If the server is configured to automatically add a Guard token, then it is NOT necessary to manually add one with this procedure for high to low messages. Check with your Administrator if you have any question whether the server is configured to automatically add a Guard token.



This procedure should only be used low to high and only if the recipient does not have a sibling certificate on the Guard.

When you are requesting signed receipts from recipients of a message, do not accidentally request a receipt from the Guard. This might happen if you are manually adding a Guard token to a message (see the section below “**Sending a Message with a Guard Token**”). There is no reason to request a receipt from the Guard, but if you do, the Guard will reject the message.

Messages that are sent through the Guard must include a token for the Guard.

1. Before sending a message, use the Directory Browser to find the Guard’s entry and copy this entry into the Personal Address Book (PAB) or Contacts. This only needs to be done once per PAB or Contacts.
2. Click the **CC...** button. Choose the PAB or Contacts from the **Show Names from the...** box provided.
3. Highlight the name of the Guard from the PAB or Contacts, and then click the **OK** button.

- 3.0-DTOOLS-Install-Agents-1100
- 3.0-DTOOLS-user-manual-xx.doc
- 3.0-DRIVERS-02X.doc
- 3.0-DRIVERS-03X.doc
- ACP120QRG.doc. ACP 120 Quick Reference Guide
- MSP\_ERRORS.doc. Decryption/Encryption Error Document.
- NDN-SUMM.doc. Non-Delivery Report Summary Document.
- NDN.doc. Non-Delivery Document.
- NTP.doc. Network Time Protocol Document
- Pabsync.doc. PAB Synchronization Document

<ws\_drive>:\program files\baldon james\messagaing and directory\masterkeyplus

- DMS Technical Notes.doc. MasterKeyPlus Document

## Reference Material

### ADDITIONAL REFERENCE MATERIAL

Your Local Help Desk should be the primary path to resolve your issue. They will have access to the extensive DMS hierarchical help structure including Lockheed Martin and the vendor.

A copy of the following DMS documentation is available on your hard drive in the <ws\_drive>:\DMS\Docs folder (<ws\_drive> is the drive where \DMS folder is installed typically, but not necessarily c:).

- INSTALL.doc. Installation Document
- CRG.doc. Client Reference Guide
- RELEASE.doc. Release Notes.
- DMS\_Client\_Guide.rtf Getting Started Guide
- DMS\_Client\_Guide.chm DMS Client Getting Started Guide
- DMS\_Administor\_Guide.rtf. Administrators Getting Started Guide
- DMS\_Administor\_Guide.chm. Administrators Getting Started Guide

Doc files are in Microsoft Word format. Release Notes and Installation Instructions documentation are available from the Local Control Center (LCC).  
DMS Support Web Site:  
<http://www.lmdms.com/dms>

## Organizational Messaging Elements of Service

### REQUIRED ELEMENTS OF SERVICE

The ACP 120 U.S. Supplement requires that each organizational DMS military message must contain an originator indicator, primary and copy recipient's indication, subject indication, primary precedence, message type and extended authorization. The following table indicates the location where each attribute can be entered on message origination, as well as the location the information can be found on received messages. Check your service or agencies specific policies for further guidance.

Elements of Service (EoS)	Location where entered on new messages	Location found on received messages
Originator Indication (From Line)	Click <b>Message</b> tab to access the FROM field button.	Click <b>Message</b> tab to view the FROM line.
Primary & Copy Recipients Indication (TO, CC, and BCC)	Click <b>Message</b> tab to access the TO, CC and BCC buttons.	Click <b>Message</b> tab to view the TO:, CC, and BCC recipients.
Subject Indication (subject)	Click <b>Message</b> tab to access the Subject field. Note: the subject is limited to a maximum of 128 character.	Click <b>Message</b> tab to access the field. Subject line.
Primary & Copy Precedence (TO, CC, and BCC)	Click <b>Message</b> tab to access the <b>Primary Precedence</b> and <b>Copy Precedence</b> fields.	Click <b>Message</b> tab to view the Primary Precedence or the Copy Precedence.
Message Type	Click <b>Message</b> tab to access the Message Type pull-down selection menu.	Click <b>Message</b> tab to view the Message Type.
Extended Authorizations <sup>1</sup> (Release Date/Time)	Click <b>Military</b> tab view the Release Date/Time field. Note: changes can be made to the Release Date/Time field by checking the box next to the field and then click on the pull-down window, which brings up a calendar.	Click <b>Message</b> tab (displayed in ZULU time) or <b>Military</b> tab Message Content section (displayed in UTC and Local time) to view the Release Date/Time field.

---

<sup>1</sup> The *extended authorization* attribute (EAI), in conjunction with the *originator indication*, provides a common message reference. The *extended authorization* attribute is used by the MFI to generate the Date Time Group in Format Line 5 of an AUTODIN message. The EAI will be automatically entered (using the client desktop time) if the message is an organizational message type, signed and encrypted, and the originator is an organizational message releaser.

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

**OPTIONAL ELEMENTS OF SERVICE**

Although not required by the ACP 123 U. S. Supplement, the use of message instructions, handling instructions, originator reference, and distribution codes is recommended and may be required by your service or agency. The following table indicates the location where each attribute can be entered on message origination, as well as the location the information may be found on received messages. Other Elements of Service are also available. Check your service or agencies specific policies for further guidance.

<b>Elements of Service (EoS)</b>	<b>Location where entered on new messages</b>	<b>Location found on received messages</b>
Message Instructions	Click <b>AUTODIN</b> tab to enter Message Instructions	Click <b>Advanced</b> tab to view Message Instructions.
Handling Instructions	Click <b>AUTODIN</b> tab to enter Handling Instructions.	Click <b>AUTODIN</b> tab to view Handling Instructions.
Originator Reference	Click <b>AUTODIN</b> tab to Originator Reference.	Click <b>Advanced</b> tab to view the Originator Reference.
Subject Indicator Codes or Subject Indicator	Click <b>AUTODIN</b> tab to enter Subject Indicator Code(s)	Click <b>Advanced</b> tab to view the Subject Indicator Code(s).

## TROUBLESHOOTING GUIDE

This troubleshooting section is divided into the following sections:

- **Warnings.** This section provides warning information for general messaging.
- **MGS/HGS Coexistence Problems and Workarounds.** This section provides information on coexistence problems with medium grade services (MGS) and high grade serves (HGS).
- **Troubleshooting Guide.** This section provides information on general messaging trouble shootings.
- **Non-Delivery Notices (NDN) and Corrective Action.** The section provides information on general Microsoft NDNs and possible corrective actions.
- **How Do I Know My DMS Message was Delivered?** This section provides information on tracing DMS messages.
- **Supported and Unsupported ASCII Character Charts.** This section provides charts of supported and unsupported ASCII characters sets.

### WARNINGS

- From within a Microsoft Word document, do not use the option under **File→Send To→Mail Recipient**, as this will cause DMS to stop functioning properly from within Outlook. Specifically, after this has been done no new messages will contain DMS military properties, FORTEZZA will not function, and any customization made to toolbars will reset.
- Do not attempt to send an ACP 120 (V3) signed only messages to non-R3.0 user as the message will open but the body of the message will not be displayed. When forwarding or replying to DMS messages, the icons are not updated with a symbol that indicates the messages has been replied to. Also when the message is open, it also does not indicate action has been taken on the message.
- Make sure the **AutoSave unsent every:** is deselected (**Tools→Options→E-mail Options**) and/or **Automatically save unsent message (Tools→Options→E-mail Options)**. This is very important because if a DMS signed/encrypted message is AutoSaved by the

client and then sent after the AutoSave, it will arrive at the recipient blank.

- If an Non-Delivery Notification (NDN) arrives in your mailbox, do not click on the **Send Again...** button. The button does not function and will invoke a series of error messages. To Re-send the message, go to the **Sent Items** folder, locate the original message, open, and go to **Actions→Resend This Message...**
- No DMS message can contain more than 150 total entries in the **TO...**, **CC...** and **BCC...** fields. This includes the combination of DMS, SMTP, AUTODIN, and Mail List addresses. This does not apply to size of a mail or address list, which is considered a single entry.
- As a result of a commercial limitation, the Microsoft product allows users to designate delegates and give these delegates certain privileges to the user's mailbox. Unfortunately, this does not work as expected. If you give a delegate read permissions, but no delete permissions, the delegate **will still be able to delete messages in the mailbox**. Be aware of this.
- You can not grant access to a secondary mailbox from the client using the delegate access feature in Microsoft Outlook. If a secondary mailbox is needed, access must be granted at the server by the administrator when they set up the secondary mailbox
- The Preferred Delivery attribute in the Directory cannot be displayed using the old DIT Browser. Please use the MasterKeyPlus DIT Browser. The current Microsoft DUA Browser incorrectly displays this as an asn.1 field. It is actually a text field with this form 0a01XX, where XX is 00 for SMTP address, 01 for AUTODIN address, and 02 for DMS address.
- Do not change or remove the Rules Wizard Rule for High Precedence messages. It is configured to provide an alert for an Urgent Grade of Delivery message including the High Precedence Alert filter.
- Do not configure the Rules Wizard with a rule that has criteria of Any Condition for a client that is expected to process MSP/ACP 120 messages as it could interfere with the high precedence alert.
- Do not step through the Directory Information Tree using the old DIT browser using the **arrow keys** since this will initiate a read request for

each entry and will cause unnecessary network traffic.

- Any message sent to a non-Microsoft DMS client from a Microsoft DMS client with a Rich-Text content will include a 'Winmail.dat' file. This is a commercial limitation based on how non-Rich-Text clients store the Rich-Text content.
- When an organizational message is re-released, the DTG entry must be cleared or edited if a new DTG is desired.
- Roaming capability must be used on the same operating system platform.
- There is no option to prevent the client from receiving Non Deliverable Notices (NDNs) or Delivered Notices (DNs).
- When multiple users are logged onto a single DMS mailbox simultaneously and a high priority message arrives at that mailbox, one and only one of the users will get the high priority message alert.
- Embedded SMTP Messages appear with DMS icons. The message will still be a commercial message but will display with the wrong icon.

### **MGS/HGS COEXISTENCE PROBLEMS AND WORKAROUNDS**

**Issue:** Unable to publish MGS certificate to GAL if MGS user is the secondary mailbox in a multi-view mailbox profile.

One of the recommended profile configurations suggests that the profile have the HGS (v3) organizational mailbox as primary, and the MGS individual, and HGS (v1) as secondary mailboxes. In this scenario the MGS user is unable to publish its MGS certificate to the GAL. The **Publish to GAL** of the certificate fails when trying to incorrectly post the MGS certificate information to the HGS (v3) organizational users' address.

**Recommendation:**

Publish the MGS certificate to the GAL by creating a new profile where the MGS user is the primary mailbox. Once the certificate is published to the GAL it is okay to go back to using the recommended profile configuration.

**Issue:** Voting Buttons do not function properly.

Commercial messaging including S/MIME messages allow the use of voting buttons. However, the voting button feature does not function properly on DMS Outlook Clients.

**Recommendation:**

Microsoft is investigating this behavior. It is recommended that you do not use voting button at this time.

**Issue:** Read Receipts are not received for messages sent external to your Exchange site.

When sending a MGS message that will be received external to your own Exchange site, read receipts will not be produced.

**Recommendation:**

This is a documented Microsoft commercial limitation. It is recommended that users not request a Read Recipient for MGS messages that will be sent external to your own Exchange site. If you want confirmation of delivery, ask for a delivery report. Note: this will only confirm delivery to the recipients' server and not actual delivery to the recipient.

**Issue:** All MGS Messages have Attachment Icon

Messages in Inbox have multiple attributes that provide information relevant to each message. One of these attributes is the paper clip icon indicating that the message has an attachment. It is expected that when a message (with any combination of security options selected) does not have an attachment, this icon would be absent for that message in the inbox.

When an MGS message with security (encryption and/or signature) is received and listed in the inbox, the paper clip icon is always present. This masks the true presence or absence of attachments within that message. This represents a potential usability issue.

**Recommendation:**

This is a commercial limitation. The MGS information that comes along with an MGS signed and/or encrypted message is interpreted by Outlook as an attachment. Therefore all MGS protected messages will have the paper clip icon. Microsoft states that this client behavior is as designed and they have no plans to change this. There is no workaround

identified for this issue. The recommendation is to document the behavior and educate the users. The users should know that when dealing with an MGS message (encrypted and/or signed), the paper clip icon is not a positive indication that there is an attachment present. The messages must be opened to validate the presence or absence of attachments.

**Issue:** PKI Password Cancellation

While opening a commercial message with security (Encryption and/or Signature) options selected by the originator, recipient may be required to enter the PKI password. If the user attempts to cancel the password entry action, the client goes into a looping mode requiring the user to cancel 4 times. This is a commercial client issue that gets amplified by DMS presence.

This causes a usability issue since the user has to click through 4 password prompts before the action is cancelled.

**Recommendation:**

Microsoft is investigating this behavior. It is recommended that users not use the cancel button, but enter the PKI password and, after the message opens, simply close the message. If the user inadvertently clicks cancel he/she must continue to click cancel as many times as necessary to get to the subsequent message: Can't open this item. Your Digital ID name can not be found by the underlying security system. At this time canceling of the PKI password entry process has been accomplished.

**Issue:** Security not retained during conversion of a message from HGS to MGS to HGS.

During message composition a user creates a military message with security (Encryption and/or Signature) options selected. The user then converts the message to a commercial message and then back to military message. As a result of the conversion the military message does not retain the security settings.

If the user inadvertently clicks on send he/she will have inadvertently sent this clear, P22 message instead of the military message with security settings enabled.

**Recommendation:**

It is recommended that users reapply/verify the security settings of military messages prior to releasing the message.

**Issue:** MGS read receipt generated before password is entered.

While opening a commercial message with security (Encryption and/or Signature) options selected by the originator, the recipient is required to enter a password. When this password prompt appears the read receipt is generated and sent to the originator.

If the user decides not to enter the password then the read receipt would be a false indication that the message has been read.

**Recommendation:**

Read receipt should not be generated until after the message has been successfully opened.

**Issue:** DMS Exchange servers will not support a pure SMTP address.

Microsoft Exchange 5.5 core commercial architecture requires all recipients to have an SMTP and X.400 address. Commercial users with only SMTP addresses on DMS Exchange servers can NOT route messages. The messages get stuck in the originator's Outbox and then an NDR is received. The NDR states that the recipient name is not recognized.

**Recommendation:**

It is recommended that every commercial user in a DMS Exchange site have a x400 address.

**TROUBLESHOOTING GUIDE**

This trouble shooting guide is provided as a means to assist the user with common errors. In the event your error (e.g. a specific error code) is NOT included in this guide—please notify your local help desk for assistance.

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
<b>General</b>		
Subject of a signed receipt is signed receipt: original message missing.	The original message used to correlate the signed receipt is missing. Note: this can occur at the recipient if attempting to open a signed receipt in the sent items or at the message originator if the original message is missing or deleted.	<ul style="list-style-type: none"> <li>• Attempt to go into the deleted items or personal folder and restore or “undelete” the original message to the inbox or sent items and then re-open the signed receipt.</li> <li>• If the original message can not be restored/undeleted, you will not be able to correlate the signed receipt and the subject will remain signed receipt: original message missing.</li> </ul>
When using Quick Find on the Outlook toolbar or Find a Contact on the Advanced toolbar to find a contact, Outlook abnormally terminates.	You may have a damaged QuickFindMRU registry key.	<ul style="list-style-type: none"> <li>• Close all open programs including Outlook.</li> <li>• On the <b>Start</b> menu, click <b>Run</b>, and type <b>regedit</b> in the <b>Open</b> box.</li> <li>• Navigate to the following registry key: <b>HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Contact\QuickFindMRU</b></li> <li>• Click to select the key, and on the <b>Edit</b> menu, click <b>Delete</b>.</li> <li>• When you receive the <b>Confirm Key Delete</b> prompt, click <b>Yes</b>.</li> <li>• Quit the Registry Editor, and restart Outlook.</li> <li>• Note: When you restart Outlook, the registry key is recreated. Your previous Quick Find list is removed and will be rebuild.</li> </ul>
Can not log onto the FORTEZZA card or decrypt secure messages.	You are using Contacts, and you are unable to logon onto your FORTEZZA card or decrypt secure messages.	<ul style="list-style-type: none"> <li>• You are using Contacts to store your personal address and have added a certificate authority to your Contacts that contains a full stop (.).</li> <li>• Outlook automatically inserts a space after a full stop thus cases name resolution failure.</li> <li>• See Secure Offline Access section in this CRG.doc for detailed instructions on how to correct the address in Contacts.</li> <li>• In summary, you need to manually remove the space automatically inserted into the Contact entries in the File As: section.</li> <li>• Note, the Contact entry should match the name in the directory.</li> </ul>
When re-opening an embedded message, operation failed error is received.	When re-opening an embedded message an operation failed error message is received.	<ul style="list-style-type: none"> <li>• Close the entire message.</li> <li>• Re-open the message.</li> <li>• Re-open the embedded message.</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Commercial message tracking does not function.	Microsoft Outlook message tracking feature does not function.	Microsoft is currently investigating this issue. At this time, commercial message tracking does not function.
Auto-signature is enabled, and the signature is added to the compose screen but there is no return before the signature block.	There is no return prior to the auto-signature block.	When setting up auto-signature, you must put an extra return prior to your signature block. To do this, do the following: <ol style="list-style-type: none"> <li>1. Go to <b>Tools&gt;Options&gt;Mail Format&gt;Signature Picker</b>.</li> <li>2. Click on <b>Signature</b>.</li> <li>3. If signature present, select <b>Edit</b>. If no signature, click <b>New</b>.</li> <li>4. Under <b>Signature Text</b>, add a return (press enter) to the first line of the signature block.</li> <li>5. Click <b>OK</b> until you exit options.</li> </ol>
Converting between a DMS message to commercial message and back to DMS message, requires that you re-select the signed and encrypted buttons (if previously selected).	If you select to signed and encrypted a DMS message→click on the convert button to convert to a commercial message→and then click the convert button again to convert back to a DMS message, you will need to re-select the signed and encrypted buttons on the DMS message.	Select the signed and encrypted button if the DMS message is going to be sent signed and encrypted.
Double-clicking on the information bar does not show message history.	Commercial message history function does not function.	Microsoft is currently investigating this issue. At this time, commercial message history does not function.
The following message is received when attempting to move/copy-to-folder: This functionality is not supported for DMS encrypted message or for commercial messages when selecting multiple messages from the inbox. Please cut and paste or drag and drop the message to the appropriate destination folder.	Move/Copy-to-folder is temporary not supported for all signed and encrypted messages. Also if you are attempting to move/copy-to-folder multiple messages from the Inbox viewer, this is also not supported—even if the message are non-signed and encrypted.	Please cut and paste or drag and drop the message to the appropriate destination folder
Non-Release 3.0 Clients receives R3.0 client military Form	Occasionally forms-definitions (R3.0 military Form) is sent with the original message.	This causes no issues to the recipient. However, they may receive a dialog box that indicates the message contains a macro. Clicking OK to this dialog and allowing access will allow the recipient to view the message.
Message sent to the PUA is not delivered to the recipient.	Message instructions field can not exceed 64 characters in length.	Ensure the message instructions field does not exceed 64 characters in length and re-send the message.

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
AutoForwarding does not function	DMS requires the use of server based auto-forwarding rules.	Ensure the client has a server based auto-forwarding rule. If a rule is being set up that is not a server-based rule, the rules wizard will indicate this. If this occurs, delete the rule and recreate ensuring it is a server-based rule.
Cannot work <b>off-line</b> due to following errors:  “Unable to expand the folder. The set of folders could not be opened. The information store could not be opened”.  “The command you specified could not be carried out. The information store could not be opened”.  ”Cannot create the e-mail message because a location to send and receive messages from could not be found. To add a location, click the <b>Tools</b> menu.... <b>Delivery</b> tab”.	The client has not been correctly set up for off-line use.	Follow the instructions listed in the CRG section titled “ <b>To Enable Offline Access</b> ”.
Certain attachment types (i.e., *.exe, *.vbs, etc...) don't work after installing the DMS Outlook client.	This version of the DMS Outlook client includes Microsoft Office SP2, which incorporates the security patch for the “I love you” virus, which prevents access to certain types of attachment types to protect the client.	For further information about this patch go to the Microsoft web site ( <a href="http://www.microsoft.com">http://www.microsoft.com</a> ) and search for knowledge base article number Q262631.
Get Recipient Name is not Recognized when trying to send a message.	This can happen if you saved a signed and/or encrypted message to the <b>Drafts</b> folder and then tried to open it and send it. Doing this will cause the error and the message won't be sent.	Open the message in the <b>Drafts</b> folder, then delete all of the recipients. Add all of the recipients back and then send the message. The message should send.
Message is blank at the recipient and in the originators Sent Items.	This happens when the message has been AutoSaved and is subsequently sent.	The AutoSave feature of Outlook cannot be used in conjunction with DMS. Turn off AutoSave using the instructions in the section titled: <b>Turning Off AutoSave</b> .

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Messages originated from Microsoft clients have Winmail.dat attachments	Microsoft clients send messages out with rich text. Foreign e-mail systems (non-Microsoft) often strip out the rich text formatting and attach as a Winmail.dat attachment.	No action required.
Receive <b>“Decode from P22/P772 failed”</b> message	This can be caused by a corrupt message. It can also be caused by a Lotus user sending a message with a multiple line subject, which the Microsoft client cannot resolve.	Contact the originator. If they are a Lotus user, determine if they sent the message with a subject consisting of more than one line. If so, have them send the message again with a subject that has only one line.
Receive <b>“Unable to connect to network”</b> message.	Connection to server failed. Possible cause – network or server error.	Contact the Local Control Center (LCC) and report inability to connect to network server. Log off and log back on when LCC staff resolves problem.
Receive an unexpected commercial read receipt that simply says the message was read.	The user sent a message to AUTODIN with an attachment and/or rich text formatting. This is not allowed.	See notes at the end of the section titled “To Address and Send an AUTODIN Message”.
Receive an unexpected commercial read receipt that simply says the message was read.	The <b>Always send to this recipient in rich text format</b> check box is checked on the AUTODIN address in the address book	Open the address book and double-click the AUTODIN user’s address. If the <b>Always send to this recipient in rich text format</b> checkbox is checked, uncheck it.
Receive the following error message, “The form required to view this message cannot be displayed. Contact administrator.”	This release of DMS uses custom forms. These forms are cached locally on the workstation. Dependent upon circumstances, occasionally the forms become corrupted.  If your workstation is used by more than one NT log-in (e.g. roaming users), changing between the accounts can cause this error.	If you receive this error message. Close Outlook. Perform a search for frmcache.dat. Delete all occurrences of this file. Restart Outlook. If the problem persists, contact your administrator. Ensure to enable “show all files” prior to searching.

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
<p>Receive the following error message when attempting to publish forms, a Microsoft Publish All DMS Forms – Discussion Message window will appear with the following text:</p> <p>“Publish All DMS Forms. This application enables you to publish the DMS forms to the organizational forms library on the Exchange Server. Cannot publish forms: You do not have macros enabled. In order to publish the forms you must close this message and re-open it with macros enabled.”</p>	<p>SP2 disables macros, which are needed to publish and/or access DMS Forms.</p>	<p>Ask your Administrator to complete the steps in the R3.0 Administrator, Configuration, and Installation document titled Microsoft Outlook Security Form Publication, which was released as a FEN.</p>
<p>Receive the following error message when composing a new DMS mail message and/or opening an existing DMS message, the following message will be displayed:</p> <p>“A program is trying to access an e-mail address you have stored in Outlook. Do you want to allow this? If this is unexpected, it may be a virus and you should choose “No”. &lt;check box&gt; Allow access for X minutes. Yes. No. Help.”</p>	<p>SP2 disables macros, which are needed to publish and/or access DMS Forms.</p>	<ol style="list-style-type: none"> <li>1. It is safe to click <b>Yes</b> to this dialogue box.</li> <li>2. Ask your Administrator to ensure the following registry key is set: [HKEY_Local_MACHINE\Software\Policies\Microsoft\Security] with the following dword key and value: CheckAdminSettings=dword:00000001</li> <li>3. Ask your Administrator to complete the steps in the R3.0 Administrator, Configuration, and Installation document titled Microsoft Outlook Security Form Publication, which was released as a FEN.</li> </ol>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Auto-Populate From Field does not function/the From field remains <blank>.	The X.500 and X.400 address in the Directory must exactly match the address in the Exchange Server.	<p>Have your administrator verify that the X.500 and X.400 address in the Directory matches the address into the Exchange Server. They must match exactly and if they do not exactly match, auto population of the From field will not function.</p> <p>For example, in the <b>directory</b> if the <b>X.500</b> address is the following:</p> <p>ou=Engineering(n), ou=DMS, ou=Organizations, ou=LMCO, ou=Contractors, ou=DISA, ou=DoD, o=U.S. Government, c=US</p> <p>And the <b>X.400</b> in the <b>directory</b> is the following:</p> <p>/OU=DMSEngineering(n)/PRMD=siprce/ADMD=gov+dms/C=us</p> <p>The <b>Exchange Server</b> address would have to be the following:</p> <p>c=us;a=gov+dms;p=siprce;ou=DMSEngineering(n);dda:msxcx500=c=US,o=U.S. Government,ou=DoD,ou=DISA,ou=Contractors, ou=LMCO,ou=Organizations,ou=DMS,ou=Engineering(n)</p>
There is a message sitting in the Outbox that is not displayed in italic font.	Messages that are in the Outbox in italic font are waiting to be sent and will be sent when the client is able to do so. Messages in the Outbox in Roman (not italic) font are just sitting there and will not be sent. This can happen if you cancel sending a message after getting a dialog box saying that one or more of the users can't receive encrypted mail.	Double click the message in the Outbox to open it. View the message, if you did intend to cancel the message, then delete it here. If you decide to send the message, click <b>Send</b> .
<b>FORTEZZA</b>		
Error Message SMAPI 54 FORTEZZA card cannot decrypt this message	The recipients certificate contained within the signed and encrypted messages does not match the certificate on the FORTEZZA card that is being used to decrypt the message.	<ul style="list-style-type: none"> <li>• Ask the message originator to delete the recipient's entry from their PAB or Contacts and re-add the entry from the X.500 Directory to the PAB or Contacts and re-send the message.</li> <li>• If this does not resolve the issue, contact the Directory Administrator and have them investigate the certificate mismatch.</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Attempt to send message and receive "User on CRL 590".	The recipient addressed is on the Certificate Revocation List (CRL) or ICRL and is an invalid user.	<ul style="list-style-type: none"> <li>It is possible that you have an outdated credential for the recipient. Remove the recipient from the PAB or Contacts. Go to directory and add user back into the PAB or Contacts. Re-send Message.</li> <li>Contact Directory Administrator to confirm user on CRL. And if the recipient is on the CRL, remove the user from the directory and remove user from any Personal Address Book or Contacts.</li> </ul>
Error Message "Error Processing Secure Message. Different PQG [323] or Improper Classification error 109" when attempting to send a message.	The client cannot encrypt the message because the issuing authority (PCA) of the sender and the recipient has different universal values. PCAs for unclas users and secret users have different universal values.	Pay close attention to the suffixes of the originator and the recipients. The DN suffix of the originator and all recipients must be consistent. Contact your local Administrator for specific guidance.
Error message "Failed to Connect to host system – Search terminated" during FORTEZZA Logon.	Your client was unable to connect to the Directory Services Agent (DSA).	Attempt to Logon again. If Logon fails a second time, contact LCC.
Error message "Invalid PIN?" is received. Access Denied".	An invalid FORTEZZA PIN has been entered.	Verify correct PIN is entered. Contact the Local Control Center (LCC) if PIN is invalid or in question.
Error message "Too many recent failures. Logon disabled for 5 minutes".	An invalid FORTEZZA PIN has been entered 3 times in a row.	<ul style="list-style-type: none"> <li>Wait 5 minutes.</li> <li>Enter valid PIN at FORTEZZA Logon.</li> <li>Contact the Local Control Center (LCC) if PIN is invalid or in question.</li> </ul>
Error Message "Missing Credentials 17" occurs when message is opened.	The Client could not find a certificate for a given user or any component in the certificate path. Local or remote DSA may not be available.	Contact the LCC and inform them of the error condition.
RAC will encounter errors	One possible error is that selecting the RAC icon does not bring up the RAC screen, but a message box saying 'Variant does not contain an object.'	This indicates that the dmsrac.dll is not properly registered on your client. Your administrator will have to fix this. Another possible error is that when you try to use the pull-down lists to select the Messaging Domain and the Security Policy, they are empty. This means that the <b>pua.txt</b> file is not correctly installed on your workstation. Again, your administrator will have to fix this.
SMAPI 46 and/or MCC error 702	<ul style="list-style-type: none"> <li>FORTEZZA Card is invalid</li> <li>Signature privileges (DSS certificate) are invalid</li> </ul>	<ul style="list-style-type: none"> <li>Delete DMS Security Cache.</li> <li>Run PAB/Contacts Synchronization.</li> <li>If error persists, contact the LCC and inform them of the error condition.</li> </ul>
SMAPI 16 and/or SMAPI - 9	<ul style="list-style-type: none"> <li>FORTEZZA Card is invalid</li> <li>Certificate or revocation list in the certificate path is not current, expired or invalid.</li> </ul>	<ul style="list-style-type: none"> <li>Delete DMS Security Cache.</li> <li>Run PAB/Contacts Synchronization.</li> <li>If error persists, contact the LCC and inform them of the error condition.</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
SMAPI 15—No Valid Roles	<ul style="list-style-type: none"> <li>• The certificate on your FORTEZZA card does not match the certificate in the directory.</li> <li>• The certificate cached does not match the information in the directory.</li> <li>• The certificate information in the PAB and/or Contact does not match the information in the directory.</li> <li>• X.500 Address Book Provider entry missing from user's profile.</li> </ul>	<p>The 'Security Provider' could not find any valid FORTEZZA roles on your card.</p> <p>This may be caused by one of the following reasons:</p> <p>[1] None of the roles on the card match the message being processed.</p> <p>[2] All the roles on the FORTEZZA Card have expired.</p> <p>[3] There are no roles on the FORTEZZA Card.</p> <p>[4] There is a problem with the FORTEZZA Card.</p> <p>[5] There is a problem with the FORTEZZA Card driver.</p> <p>[6] There is a problem with the FORTEZZA Card library.</p> <p>[7] There is a hardware fault with the actual FORTEZZA Reader.</p> <p>[8] The FORTEZZA Card is not inserted properly.</p> <p>[9] The Directory Service Agent (DSA) is not accessible.</p> <p>[10] A certificate in the certification path is expired, invalid, or can not be found.</p> <p>Please try the following for error resolution:</p> <p>[1] Ensure the FORTEZZA Card is inserted properly.</p> <p>[2] If you have more than 1 FORTEZZA card or are a Software FORTEZZA user, switch tokens [FORTEZZA card or User Image File (UIF)] and try again to open the message.</p> <p>[3] Verify the DSA is accessible by opening the DIT Browser</p> <p>[4] From the Outlook Client go to Tools&gt;Services and verify X.500 Address Book Provider has been added to the profile and verify that it has also been added to the default search order.</p> <p>[5] Delete smcache.bin by clicking <b>Tools→Delete DMS Security Cache</b> and ensure your certificate is not contained in your PAB and/or contacts (if it is delete it).</p> <p>If error persists, please contact the Administrator.</p>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Error Message "Unknown Error [9]"	The client is not functioning properly.	Exit the application. Make sure FORTEZZA card is properly inserted in the PCMCIA reader. Restart application. If condition persists, contact local administrator.
Error message. "Missing Token 201" is displayed when attempting to open a message. Message may display blank subject and from data. No other data is displayed.	The client cannot decrypt the message because it cannot find the correct credentials. This may be caused by: <ul style="list-style-type: none"> <li>• Recipient has a new certificate and Originator has old certificate in their local address book/cache.</li> <li>• Originator utilized wrong certificate to send message because of duplicate entries in PAB or Contacts for same recipient.</li> </ul>	<ul style="list-style-type: none"> <li>• Originator must delete recipient from Personal Address Book (PAB) or Contacts. Use DIT Browser to find recipient and add new data to PAB or Contacts. Use new entry and send message again.</li> <li>• Originator must delete multiple entries for the same recipient from PAB or Contacts and repopulate PAB or Contacts using DIT Browser. Send message again.</li> </ul>
After clicking Send for an MSP 3.0 Signed and Encrypted message, the following error message is displayed: "Unable to send secure message because the following recipient(s) failed to validate..."	The client cannot obtain a certificate for one or more of the recipients.	<p>You have selected a V1 Role from your FORTEZZA Card. The FORTEZZA Role determines what type of message you can process. i.e. MSP3 Signed or MSP3 Signed &amp; Encrypted. To send an MSP3 message, all the recipients must have a valid V1 Certificate (mosaicKmandSigCertificate). Only a V3 Certificate (userCertificate) can be found for this recipient.</p> <p>V3 Certificates are used to process ACP 120 Signed and ACP 120 Signed &amp; Encrypted messages. You cannot send a message that contains recipients with both V1 and V3 Certificates. To continue sending this message you can either:</p> <p>[1] Remove the invalid V3 recipients using the <b>'Remove recipients and continue'</b> button  [2] Press the 'Cancel Send' button and reselect the recipients in the message.</p> <p>If you receive this error again contact the Administrator.</p>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
After clicking Send an ACP 120 Signed and Encrypted message, the following error message is displayed: "Unable to send secure message because the following recipient(s) failed to validate..."	The client cannot obtain a certificate for one or more of the recipients.	<p>You have selected a V3 Role from your FORTEZZA Card. The FORTEZZA Role determines what type of message you can process. i.e. ACP 120 Signed or ACP 120 Signed &amp; Encrypted. To send an ACP 120 message, all the recipients must have a valid V3 Certificate (userCertificate). Only a V1 Certificate (mosaicKMandSigCertificate) can be found for this recipient.</p> <p>V1 Certificates are used to process MSP3 Signed and MSP3 Signed &amp; Encrypted messages. You cannot send a message that contains recipients with both V1 and V3 Certificates. To continue sending this message you can either:</p> <p>[1] Remove the invalid V1 recipients using the 'Remove recipients and continue' button                      [2] Press the '<b>Cancel Send</b>' button and reselect the recipients in the message.</p> <p>If you receive this error again contact the Administrator.</p>
<b>Inter-Security Domain Messaging</b>		
Guard Rejection Message "Based on 'recipient' setting for ACL entry ... is not allowed to receive messages".	You are attempting to send a message to a user who has been prohibited from receiving messages based on the Guard ACL configuration of either the X.400 ACL settings or the X.500 ACL settings.	Contact your local Administrator.
Guard Rejection Message "Error decrypting and/or validating MSP3 content".	When sending a message through the Guard a token for the Guard is required.	Re-send the message. Include the Guard entry as a CC recipient (low to high only) or contact your local administrator and have them configure your client for automatic Guard token generation (high to low only).
Guard Rejection Message "External bodypart {body #2} 'unstructured-binary' not allowed".	You are sending a message with an attachment that has been prohibited by the local Guard policy.	Re-send the message without the attachment and contact your local Administrator if you have an organizational need for the Guard to pass the type of attachment you attempted to send.
Guard Rejection Message "Message Classification {Secret} not allowed to destination {SBU, Unclas}".	You are attempting to send a message with a high domain classification (Secret) to a lower domain (SBU).	This is prohibited. If applicable, choose a SBU or Unclassified message classification. Otherwise, delete this lower domain recipient.

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>Microsoft DMS Client - Troubleshooting Guide</b>		
<b>Symptom</b>	<b>Problem</b>	<b>Solution</b>
Guard Rejection Message “Message Classification {Unclas} not allowed to destination {SBU, Unclas}”.	You are sending a message that has been prohibited by the local Guard policy.	Contact your local Administrator.
Guard Rejection Message “Based on ‘send’ setting for ACL entry ... is not allowed to send messages”.	<b>Problem 1:</b> You are attempting to send a message from a user who has been prohibited from sending messages.  Or <b>Problem 2:</b> This problem may also occur if the message was not deliverable due to a problem in the Message Handling System.	<b>Solution 1:</b> Contact your local Administrator. The Administrator can determine which of the described problems apply to this situation.  <b>Solution 2:</b> The Guard Rejection Message received at the client is actually a rejection of a Non-Delivery Notification. The actual NDR of the original message is discarded. The MTS Id can be used to correlate the message.
Receive on of the following Guard Rejection Messages: “The following message was rejected by DII Guard and message shows Guard Transaction ID: 6”.  Or “No more information is available at this time”.	This may indicate that you tried to send a message that had an attached encrypted message through the Guard.	You cannot send a message that includes an attached signed and encrypted message through the Guard.

**NON-DELIVERY NOTICES (NDN) AND CORRECTIVE ACTION**

A Non-Delivery Notice (NDN) is a system generated notification that the message did not reach one or more of the intended recipients. This Troubleshooting Guide contains information on NDNs and possible corrective action(s). Also contained in <local\_drive>:\dms\docs is the NDN-SUMM.doc (Non-Delivery Report Summary Document) and NDN.doc (Non-Delivery Document). The NDN-SUMM.doc is written for end-users and the NDN.doc is written for Administrator. These additional documents provide NDN information for all DMS products. Most problems causing an NDN are not directly attributable to something the end-user (YOU) has done, you are encouraged in most cases to seek involvement with your administrator and/or local help desk to resolve the issue(s). The detailed NDN information contained in this section is provided as a general overview of NDNs for those users who seek additional information regarding NDNs.

**NOTE:** The following are the most common non-delivery notices DMS users may experience. If performing the corrective action below does not correct the problem or if you receive a notice not described below, contact your local control center/help desk. Keep the notice to assist in troubleshooting.

NDN	Possible Cause	Originator Corrective Action
554 Invalid Data in Message	<ul style="list-style-type: none"> <li>• Military message has been sent to SMTP recipient</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• See the Microsoft CRG – “Using the Convert Button” to ensure commercial messages are sent to SMTP recipients</li> <li>• Convert and re-send the message</li> <li>• Contact your DMS Local Control Center</li> </ul>
Acknowledgement timeout	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
A conversion required for the message to be delivered is impractical	<ul style="list-style-type: none"> <li>• Originator accidentally pressed ‘convert’ button on client and sent a commercial message rather than a military message.</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message correctly                             <ul style="list-style-type: none"> <li>• See Microsoft CRG-“Using the Convert Button”</li> </ul> </li> </ul>
Address List Error	<ul style="list-style-type: none"> <li>• Originator’s directory entry missing the associatedPLA value</li> <li>• Originator entered an AUTODIN recipient in the BCC field of the message</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> <li>• Remove the AUTODIN recipient from the BCC field of the message and re-send the message</li> </ul>
Ambiguous O/R name	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
A required directory operation was unsuccessful	<ul style="list-style-type: none"> <li>• Problem may be temporary</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send the message</li> <li>• Contact your DMS Local Control Center</li> </ul>
A restriction in the system prevented delivery of the message.	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
A syntax error was detected in the content of the message	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Based on ‘recipient’ setting for ACL entry ... is not allowed to receive messages	<ul style="list-style-type: none"> <li>• Message sent to user prohibited from receiving messages through Guard</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

NDN	Possible Cause	Originator Corrective Action
Based on 'send' setting for ACL entry ... is not allowed to send messages	<ul style="list-style-type: none"> <li>• Originator not allowed to send messages through Guard</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Content type not supported	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Content too long	<ul style="list-style-type: none"> <li>• Too many addressees in the "To" field</li> <li>• Message Journaling feature turned on at client</li> </ul>	<ul style="list-style-type: none"> <li>• Limit addressees to less than 150</li> <li>• Turn off Message Journaling to ensure that no automatic recording is on</li> <li>• Contact your DMS Local Control Center</li> </ul>
Directory operation unsuccessful	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Dirty Word 'XXX' found	<ul style="list-style-type: none"> <li>• Message contains the prohibited word 'XXX'</li> </ul>	<ul style="list-style-type: none"> <li>• Delete the prohibited word and re-send</li> </ul>
Either message size exceeds maximum allowed for recipient or transport, or you have exceeded storage limit on your mailbox	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Error decrypting and/or validating ACP120 content	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Error decrypting and/or validating MSP3 content	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
External bodypart {body #3} 'unstructured-binary' not allowed	<ul style="list-style-type: none"> <li>• Message contains attachment prohibited by Guard</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message without attachment</li> </ul>
Failed MSP Processing	<ul style="list-style-type: none"> <li>• Originator's address book (PAB or Contact) has an invalid certificate entry for an AUTODIN recipient</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Originator must re-cache the AUTODIN recipient's certificate entry in the originator's address book                             <ul style="list-style-type: none"> <li>• See Microsoft CRG – "PAB/Contacts X.500 Synchronization Tool"</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
Gatewayed by MFI Non-Importable Attachment(s) dropped from message	<ul style="list-style-type: none"> <li>• Attachments were included in a message sent to AUTODIN</li> </ul>	<ul style="list-style-type: none"> <li>• Per the Microsoft CRG, messages to AUTODIN cannot have attachments. Re-send message without attachment(s)</li> </ul>
Guard Filter Setup Details: Error setting up filters for this message.	<ul style="list-style-type: none"> <li>• Message through Guard from SECRET to Unclassified requested signed receipts from explicit recipients.</li> </ul>	<ul style="list-style-type: none"> <li>• Request signed receipts from all recipients or none.                             <ul style="list-style-type: none"> <li>• See Microsoft CRG – "Requesting a Delivery Report and/or Message Receipt"</li> <li>• See Lotus CRG – "Requesting a Signed Receipt"</li> </ul> </li> </ul>
Illegal conversion request	<ul style="list-style-type: none"> <li>• Message sent to an AUTODIN address is not signed</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message signed                             <ul style="list-style-type: none"> <li>• See Microsoft CRG – "Signing and Encrypting DMS Mail"</li> <li>• See Lotus CRG – "Setting Message Options"</li> </ul> </li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

NDN	Possible Cause	Originator Corrective Action
Illegal message format	<ul style="list-style-type: none"> <li>• Message sent to an Mail List/Address List address is not signed</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message signed               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “Signing and Encrypting DMS Mail”</li> <li>• See Lotus CRG – “Setting Message Options”</li> </ul> </li> </ul>
Invalid message classification	<ul style="list-style-type: none"> <li>• Message classification not on first line of message (in DMS 2.2 only)               <ul style="list-style-type: none"> <li>• ‘UNCLAS’</li> <li>• ‘UNCLASSIFIED’</li> <li>• ‘C O N F I D E N T I A L’ (spaces between letters in DMS 2.2)</li> <li>• ‘S E C R E T’ (spaces between letters in DMS 2.2)</li> <li>• ‘T O P S E C R E T’ (spaces between letters in DMS 2.2)</li> </ul> </li> <li>• An invalid character exists in the body of the Message</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message with proper classification as first line of body of message.               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “Addressing and Sending a Message to AUTODIN”</li> <li>• See Lotus CRG – “AUTODIN Messages”</li> </ul> </li> <li>• Check the sent-item to determine if the sent message contains an att.dat attachment. This indicates that an extended ASCII character was used (e.g. “é”). Messages to AUTODIN must use basic ASCII characters. Remove the invalid character. Re-send the message</li> </ul>
Loop detected	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Mail List Authorization Error	<ul style="list-style-type: none"> <li>• Originator not an authorized submitter on this mail list</li> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Mail List member in error	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Maximum time expired	<ul style="list-style-type: none"> <li>• Client computer date and time may be incorrect</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Check time and reset it; if you do not have this capability, call your DMS Local Control Center</li> <li>• Contact your DMS Local Control Center</li> </ul>
Message Classification {Secret} not allowed to destination {SBU, Unclas}	<ul style="list-style-type: none"> <li>• Originator not allowed to send a message from a high security domain (Secret) to a lower security domain (Unclassified) with the high domain’s classification.</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message at the lower security domain’s classification or delete lower domain recipients</li> </ul>
Message failed to convert	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention.</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Message Structure Error	<ul style="list-style-type: none"> <li>• Body of message going to AUTODIN contains non-US ASCII data. (Can be caused by pasting text from Word, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message with only US ASCII data going to AUTODIN</li> <li>• Ensure attachments are not pasted into body of message</li> </ul>
Message type unrecognized or content conversion failed	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
MSP encryption is required for all messages	<ul style="list-style-type: none"> <li>• Message through a Guard was not encrypted.</li> </ul>	<ul style="list-style-type: none"> <li>• Encrypt the message and re-send</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

NDN	Possible Cause	Originator Corrective Action
MSP Failure – Security Processing Error	<ul style="list-style-type: none"> <li>• Originator’s PAB has an invalid certificate entry for the AUTODIN recipient</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Run PAB Sync to update the AUTODIN recipient’s certificate entry in your PAB               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “PAB/Contacts X.500 Synchronization Tool”</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
MSP non-repudiation signature is required for all messages	<ul style="list-style-type: none"> <li>• Message is not signed</li> </ul>	<ul style="list-style-type: none"> <li>• Sign message and re-send               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “Signing and Encrypting DMS Mail”</li> <li>• See Lotus CRG – “Setting Message Options”</li> </ul> </li> </ul>
MTS Congestion	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention.</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
No more information is available at this time	<ul style="list-style-type: none"> <li>• Message through Guard may contain an embedded message as an encrypted attachment. (The Guard will not support transference of that type of message).</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message without encrypted email attachment</li> <li>• If needed, include all information in the body of the attached message in the body of the message and re-send</li> <li>• Contact your DMS Local Control Center</li> </ul>
No Proxy for recipient	<ul style="list-style-type: none"> <li>• There may be mixed commercial and military recipients</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Send message to only commercial or military recipients</li> <li>• Contact your DMS Local Control Center</li> </ul>
O/R name unrecognized	<ul style="list-style-type: none"> <li>• Problem with the recipient address in your PAB</li> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Run PAB Sync to obtain latest address and certificate for all recipients in the PAB and re-send message               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “PAB/Contacts X.500 Synchronization Tool”</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
OSRI Error	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Proxy Error Unknown	<ul style="list-style-type: none"> <li>• The cause for this NDN is unknown</li> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Reboot the client and re-send the message</li> <li>• Otherwise, contact your DMS Local Control Center</li> </ul>
Recipient Name is Ambiguous	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Recipient name is not recognized	<ul style="list-style-type: none"> <li>• May be a problem with the recipient entry in your PAB</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Run PAB Sync to obtain latest address and certificate for all recipients in the PAB and re-send message               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “PAB/Contacts X.500 Synchronization Tool”</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
Recipient was unable to take delivery of this message	<ul style="list-style-type: none"> <li>• May be a problem with the recipient entry in your PAB</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Run PAB Sync to obtain latest address and certificate for all recipients in the PAB and re-send message               <ul style="list-style-type: none"> <li>• See Microsoft CRG – “PAB/Contacts X.500 Synchronization Tool”</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

NDN	Possible Cause	Originator Corrective Action
Size Constraint Violation	<ul style="list-style-type: none"> <li>• Too many recipients addressed</li> <li>• Message is larger than allowed by recipient's mailbox limits</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce number of recipients in message and re-send</li> <li>• Contact your DMS Local Control Center</li> </ul>
The following message was rejected by DII Guard and message shows Guard Transaction ID: xx	<ul style="list-style-type: none"> <li>• Message through Guard may contain an embedded message as an encrypted attachment. (The Guard will not support transference of that type of message).</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message without encrypted email attachment</li> <li>• If needed, include all information in the body of the attached message in the body of the message and re-send</li> <li>• Contact your DMS Local Control Center</li> </ul>
This string is not used currently	<ul style="list-style-type: none"> <li>• Source of this problem is unknown</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Transfer failed	<ul style="list-style-type: none"> <li>• May be a problem with the recipient entry in your PAB</li> <li>• Otherwise, problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Run PAB Sync to obtain latest address and certificate for all recipients in the PAB and re-send message                             <ul style="list-style-type: none"> <li>• See Microsoft CRG – "PAB/Contacts X.500 Synchronization Tool"</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
Unable to deliver the message due to a communications failure	<ul style="list-style-type: none"> <li>• This NDN is typically accompanied by supplemental data that more precisely identifies the reason the message was NDNed. Typical accompanying supplemental data include:                             <ul style="list-style-type: none"> <li>• Mail List member in error</li> <li>• Undefined associated PLA for Originator</li> <li>• Unknown Address Error</li> <li>• Failed MSP processing</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Review the supplemental data in the NDN and refer to the specific error in this document. .</li> </ul>
Unable to deliver the message due to a recipient problem	<ul style="list-style-type: none"> <li>• Microsoft originator accidentally composed a commercial message rather than a military message to a Lotus recipient</li> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message correctly                             <ul style="list-style-type: none"> <li>• See Microsoft CRG-"Using the Convert Button"</li> </ul> </li> <li>• Contact your DMS Local Control Center</li> </ul>
Unauthorized Proxy Originator	<ul style="list-style-type: none"> <li>• Originator is not defined in the PUA as an authorized proxy originator</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Undefined associated PLA for Originator	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>
Unknown Address Error	<ul style="list-style-type: none"> <li>• Recipient directory read failure; may be temporary</li> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Re-send message</li> <li>• Contact your DMS Local Control Center</li> </ul>
Unknown Delivery Error	<ul style="list-style-type: none"> <li>• Problem requires administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Contact your DMS Local Control Center</li> </ul>

## **HOW DO I KNOW MY DMS MESSAGE WAS DELIVERED?**

Where is my message? Commercial messaging can be frustrating and adding high grade secure encryption can make it even more complex but there are easy ways to determine if your message made it to its destination. You can request delivery confirmation. In fact, there are two types of delivery confirmation: delivery reports and read/signed receipts. The following is a summary of each type of delivery confirmation:

### **Types of Delivery Confirmation:**

1. Delivery Reports:
  - Indicate that the message was delivered to the originator's MTA.
  - Delivery Reports do **NOT** indicate that the message was opened by the recipient.
2. Read/Signed Receipt<sup>2</sup>
  - Indicate that the message was received and opened by the recipient.
  - Contain the signature of the message recipient (signed receipts only).
  - Note: For high grade secure messages, it is recommended to ask for a signed receipt for delivery confirmation. This ensures that the recipient received the message. A signed receipt with the recipient's signature confirming the message was opened by the recipient is delivered to the sender.

### **Typical Scenario Overview:**

The following is an overview of a typical scenario that will be used to demonstrate how you can track a message:

1. User 1 sends a Signed or Signed and Encrypted message to User 2 and asks for a signed receipt.
2. User 2 receives and opens the message.
3. A Signed Receipt is generated and sent back to the originator, User 1.
4. User 1 receives the signed receipt as confirmation that the recipient received and opened the message.

What happens if you never receive the read/signed receipt confirming the message was delivered? "Did the Message Get to its Destination?" Here are some important questions to ask when message reception is in question:

1. Did the originator send the message to the recipient?
2. Did the originator ask for a signed receipt?
3. Did the recipient receive the message?
4. Did the recipient generate a signed receipt?

The following table will walk you through the process of tracing a message. In many situations, if you collect this information you can determine what happened to the message. However, the recommended data collection will also help to expedite message trace by your local Administrator in the event you can not determine what happened to the message. You will need to coordinate these efforts with the message recipient to collect the appropriate data.

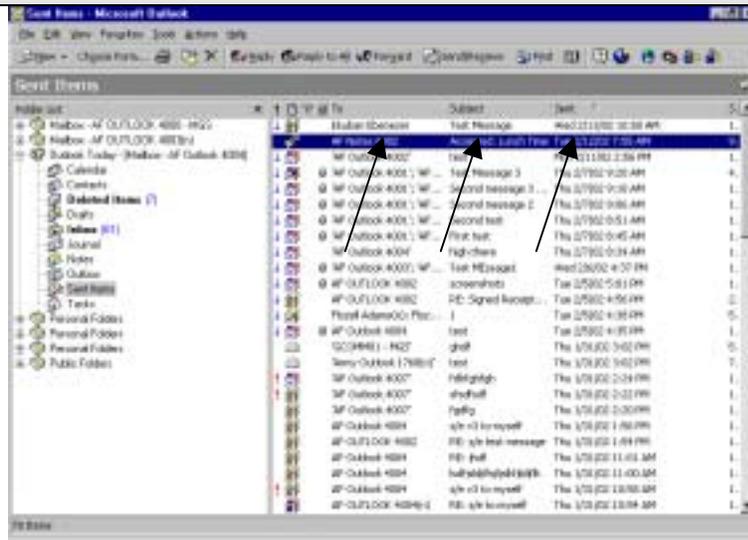
---

<sup>2</sup> Read Receipt is generated for p772 messages. Signed Receipt is generated for Signed Only (V1 or V3) or Signed and Encrypted messages (V1 or V3)

**Did The Originator Send The Message To The Recipient?**

Confirm the message was sent by searching the originators Sent Items for:

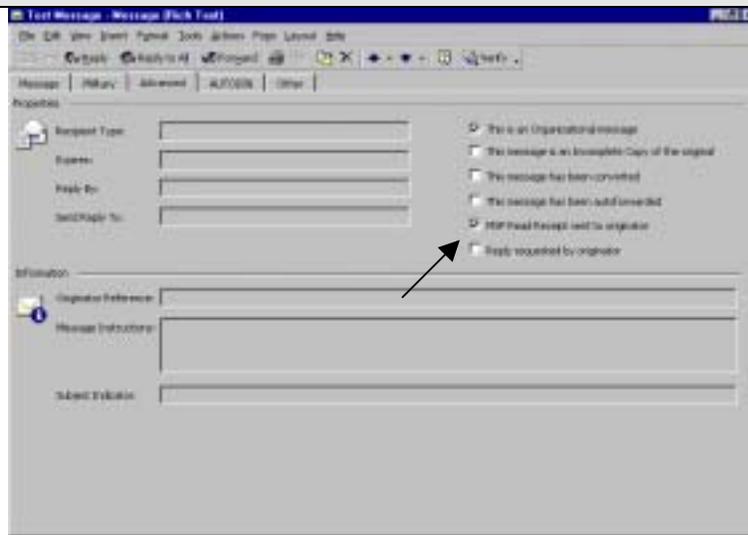
- To
- Subject
- Sent (Time/Date)



**Did The Originator Ask For A Signed Receipt?**

Once it has been confirmed the message was sent, verify that a signed receipts was requested:

1. Open the message in the originators Sent Items.
2. On the **Advanced** tab, verify the check box beside **MSP Read Receipts sent to originator** is checked.





Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients

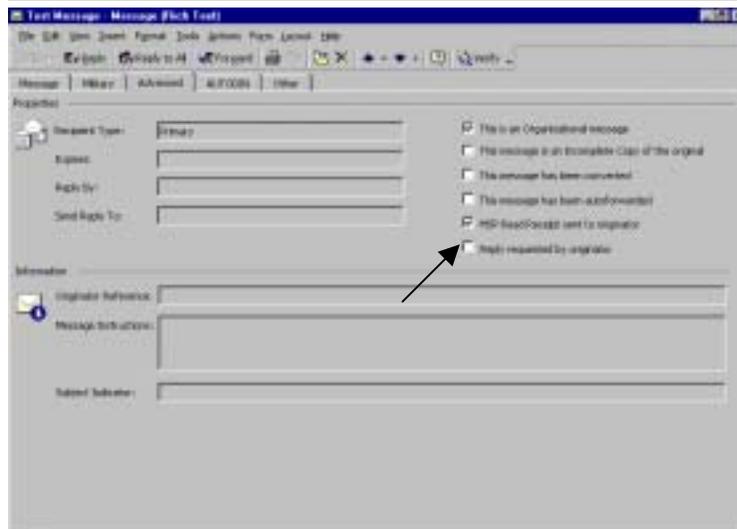
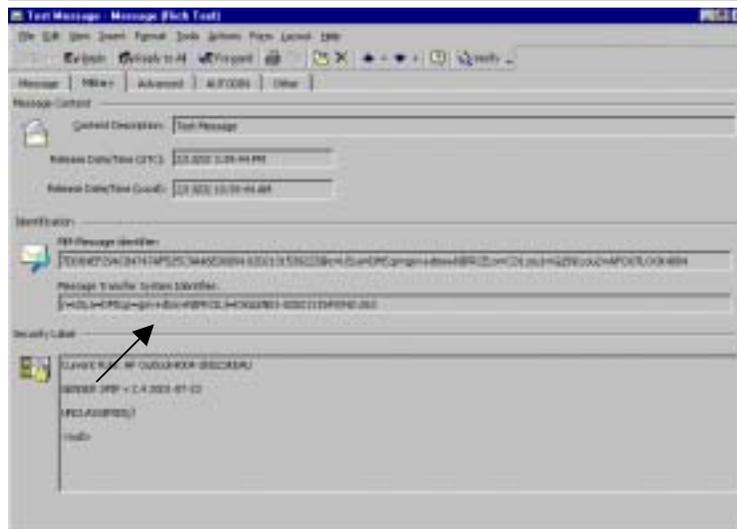
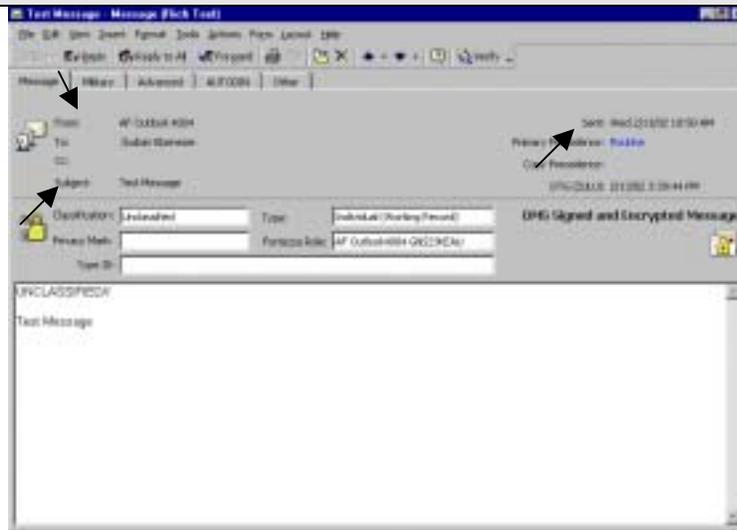
Lockheed Martin

Version 3.0.2M.0

**Did The Recipient Generate A Signed Receipt?**

Verify the information in the message matches the originator's information:

1. On the **Message** tab, record the following information:
  - From:
  - Subject:
  - Sent: (Date/Time)
2. On the **Military** tab, record the following information:
  - MM-Message identifier: (MMID)
  - Message Transfer System Identifier (MTSID)
3. Click on the **Advanced** tab, and verify that a receipt was requested by ensuring **MSP Read Receipt sent to Originator** checkbox is checked.





**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

**SUPPORTED AND UNSUPPORTED ASCII CHARACTERS CHARTS**

For reference purposes the following charts list the supported and unsupported ASCII Character Sets. The first table, ASCII Characters Chart I, represents the AUTODIN supported character sets and thus those characters that can be included in a DMS message to AUTODIN. The second table, ASCII Character Chart II, represents the AUTODIN unsupported character sets. These characters can not be included in a DMS message to AUTODIN.

<b>ASCII Characters Chart I</b>			
ASCII Character	Hex Value	Decimal Value	ASCII Character Description
<b>SUPPORTED ASCII CHARACTERS</b>			
	20	32	Space
!	21	33	Exclamation Mark
"	22	34	Quotation Mark
#	23	35	Number Sign
\$	24	36	Dollar Sign
%	25	37	Percent Sign
&	26	38	Ampersand
'	27	39	Apostrophe
(	28	40	Left Parenthesis
)	29	41	Right Parenthesis
*	2A	42	Asterisk
+	2B	43	Plus Sign
,	2C	44	Comma
-	2D	45	Hyphen-Minus
.	2E	46	Full Stop
/	2F	47	Solidus
0	30	48	Digit Zero
1	31	49	Digit One
2	32	50	Digit Two
3	33	51	Digit Three
4	34	52	Digit Four
5	35	53	Digit Five
6	36	54	Digit Six
7	37	55	Digit Seven
8	38	56	Digit Eight
9	39	57	Digit Nine
:	3A	58	Colon
;	3B	59	Semicolon
<	3C	60	Less-Than Sign
=	3D	61	Equals Sign
>	3E	62	Greater-Than Sign
?	3F	63	Question Mark
@	40	64	Commercial At
A	41	65	Latin Capital Letter A

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>ASCII Characters Chart I</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>SUPPORTED ASCII CHARACTERS</b>			
B	42	66	Latin Capital Letter B
C	43	67	Latin Capital Letter C
D	44	68	Latin Capital Letter D
E	45	69	Latin Capital Letter E
F	46	70	Latin Capital Letter F
G	47	71	Latin Capital Letter G
H	48	72	Latin Capital Letter H
I	49	73	Latin Capital Letter I
J	4A	74	Latin Capital Letter J
K	4B	75	Latin Capital Letter K
L	4C	76	Latin Capital Letter L
M	4D	77	Latin Capital Letter M
N	4E	78	Latin Capital Letter N
O	4F	79	Latin Capital Letter O
P	50	80	Latin Capital Letter P
Q	51	81	Latin Capital Letter Q
R	52	82	Latin Capital Letter R
S	53	83	Latin Capital Letter S
T	54	84	Latin Capital Letter T
U	55	85	Latin Capital Letter U
V	56	86	Latin Capital Letter V
W	57	87	Latin Capital Letter W
X	58	88	Latin Capital Letter X
Y	59	89	Latin Capital Letter Y
Z	5A	90	Latin Capital Letter Z
[	5B	91	Left Square Bracket
\	5C	92	Reverse Solidus
]	5D	93	Right Square Bracket
^	5E	94	Circumflex Accent
_	5F	95	Low Line
`	60	96	Grave Accent
a	61	97	Latin Small Letter A
b	62	98	Latin Small Letter B
c	63	99	Latin Small Letter C
d	64	100	Latin Small Letter D
e	65	101	Latin Small Letter E
f	66	102	Latin Small Letter F
g	67	103	Latin Small Letter G
h	68	104	Latin Small Letter H

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>ASCII Characters Chart I</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>SUPPORTED ASCII CHARACTERS</b>			
i	69	105	Latin Small Letter I
j	6A	106	Latin Small Letter J
k	6B	107	Latin Small Letter K
l	6C	108	Latin Small Letter L
m	6D	109	Latin Small Letter M
n	6E	110	Latin Small Letter N
o	6F	111	Latin Small Letter O
p	70	112	Latin Small Letter P
q	71	113	Latin Small Letter Q
r	72	114	Latin Small Letter R
s	73	115	Latin Small Letter S
t	74	116	Latin Small Letter T
u	75	117	Latin Small Letter U
v	76	118	Latin Small Letter V
w	77	119	Latin Small Letter W
x	78	120	Latin Small Letter X
y	79	121	Latin Small Letter Y
z	7A	122	Latin Small Letter Z
{	7B	123	Left Curly Bracket
	7C	124	Vertical Line
}	7D	125	Right Curly Bracket
~	7E	126	Tilde
	7F	127	Space

<b>ASCII Characters Chart II</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>UNSUPPORTED ASCII CHARACTERS</b>			
Ç	80	128	Latin Capital Letter C With Cedilla
ü	81	129	Latin Small Letter U With Diaeresis
é	82	130	Latin Small Letter E With Acute
â	83	131	Latin Small Letter A With Circumflex
ä	84	132	Latin Small Letter A With Diaeresis
à	85	133	Latin Small Letter A With Grave
å	86	134	Latin Small Letter A With Ring Above
ç	87	135	Latin Small Letter C With Cedilla
ê	88	136	Latin Small Letter E With Circumflex
ë	89	137	Latin Small Letter E With Diaeresis
è	8A	138	Latin Small Letter E With Grave
ï	8B	139	Latin Small Letter I With Diaeresis

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>ASCII Characters Chart II</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>UNSUPPORTED ASCII CHARACTERS</b>			
î	8C	140	Latin Small Letter I With Circumflex
ì	8D	141	Latin Small Letter I With Grave
Ä	8E	142	Latin Capital Letter A With Diaeresis
Å	8F	143	Latin Capital Letter A With Ring Above
É	90	144	Latin Capital Letter E With Acute
æ	91	145	Latin Small Letter Ae
Æ	92	146	Latin Capital Letter Ae
ô	93	147	Latin Small Letter O With Circumflex
ö	94	148	Latin Small Letter O With Diaeresis
ò	95	149	Latin Small Letter O With Grave
û	96	150	Latin Small Letter U With Circumflex
ù	97	151	Latin Small Letter U With Grave
ÿ	98	152	Latin Small Letter Y With Diaeresis
Ö	99	153	Latin Capital Letter O With Diaeresis
Ü	9A	154	Latin Capital Letter U With Diaeresis
¢	9B	155	Cent Sign
£	9C	156	Pound Sign
¥	9D	157	Yen Sign
₪	9E	158	Peseta Sign
ƒ	9F	159	Latin Small Letter F With Hook
á	A0	160	Latin Small Letter A With Acute
í	A1	161	Latin Small Letter I With Acute
ó	A2	162	Latin Small Letter O With Acute
ú	A3	163	Latin Small Letter U With Acute
ñ	A4	164	Latin Small Letter N With Tilde
Ñ	A5	165	Latin Capital Letter N With Tilde
ª	A6	166	Feminine Ordinal Indicator
º	A7	167	Masculine Ordinal Indicator
¿	A8	168	Inverted Question Mark
¬	A9	169	Reversed Not Sign
¬	AA	170	Not Sign
½	AB	171	Vulgar Fraction One Half
¼	AC	172	Vulgar Fraction One Quarter
¡	AD	173	Inverted Exclamation Mark
«	AE	174	Left-Pointing Double Angle Quotation Mark
»	AF	175	Right-Pointing Double Angle Quotation Mark
░	B0	176	Light Shade
▒	B1	177	Medium Shade
▓	B2	178	Dark Shade

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>ASCII Characters Chart II</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>UNSUPPORTED ASCII CHARACTERS</b>			
	B3	179	Box Drawings Light Vertical
├	B4	180	Box Drawings Light Vertical And Left
┤	B5	181	Box Drawings Vertical Single And Left Double
├┤	B6	182	Box Drawings Vertical Double And Left Single
└	B7	183	Box Drawings Down Double And Left Single
┘	B8	184	Box Drawings Down Single And Left Double
├┘	B9	185	Box Drawings Double Vertical And Left
├┘┘	BA	186	Box Drawings Double Vertical
└┘	BB	187	Box Drawings Double Down And Left
└┘┘	BC	188	Box Drawings Double Up And Left
└┘┘┘	BD	189	Box Drawings Up Double And Left Single
└┘┘┘┘	BE	190	Box Drawings Up Single And Left Double
└┘┘┘┘┘	BF	191	Box Drawings Light Down And Left
└┘┘┘┘┘┘	C0	192	Box Drawings Light Up And Right
└┘┘┘┘┘┘┘	C1	193	Box Drawings Light Up And Horizontal
└┘┘┘┘┘┘┘┘	C2	194	Box Drawings Light Down And Horizontal
└┘┘┘┘┘┘┘┘┘	C3	195	Box Drawings Light Vertical And Right
└┘┘┘┘┘┘┘┘┘┘	C4	196	Box Drawings Light Horizontal
└┘┘┘┘┘┘┘┘┘┘┘	C5	197	Box Drawings Light Vertical And Horizontal
└┘┘┘┘┘┘┘┘┘┘┘┘	C6	198	Box Drawings Vertical Single And Right Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘	C7	199	Box Drawings Vertical Double And Right Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘	C8	200	Box Drawings Double Up And Right
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	C9	201	Box Drawings Double Down And Right
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CA	202	Box Drawings Double Up And Horizontal
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CB	203	Box Drawings Double Down And Horizontal
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CC	204	Box Drawings Double Vertical And Right
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CD	205	Box Drawings Double Horizontal
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CE	206	Box Drawings Double Vertical And Horizontal
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	CF	207	Box Drawings Up Single And Horizontal Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D0	208	Box Drawings Up Double And Horizontal Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D1	209	Box Drawings Down Single And Horizontal Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D2	210	Box Drawings Down Double And Horizontal Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D3	211	Box Drawings Up Double And Right Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D4	212	Box Drawings Up Single And Right Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D5	213	Box Drawings Down Single And Right Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D6	214	Box Drawings Down Double And Right Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D7	215	Box Drawings Vertical Double And Horizontal Single
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D8	216	Box Drawings Vertical Single And Horizontal Double
└┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘┘	D9	217	Box Drawings Light Up And Left

**Client Reference Guide for  
Microsoft DMS Outlook Win NT and Win2000 Clients**

Lockheed Martin

Version 3.0.2M.0

<b>ASCII Characters Chart II</b>			
<b>ASCII Character</b>	<b>Hex Value</b>	<b>Decimal Value</b>	<b>ASCII Character Description</b>
<b>UNSUPPORTED ASCII CHARACTERS</b>			
␣	DA	218	Box Drawings Light Down And Right
█	DB	219	Full Block
▀	DC	220	Lower Half Block
▄	DD	221	Left Half Block
▌	DE	222	Right Half Block
▒	DF	223	Upper Half Block
α	E0	224	Greek Small Letter Alpha
β	E1	225	Latin Small Letter Sharp S
Γ	E2	226	Greek Capital Letter Gamma
π	E3	227	Greek Small Letter Pi
Σ	E4	228	Greek Capital Letter Sigma
σ	E5	229	Greek Small Letter Sigma
μ	E6	230	Micro Sign
τ	E7	231	Greek Small Letter Tau
Φ	E8	232	Greek Capital Letter Phi
Θ	E9	233	Greek Capital Letter Theta
Ω	EA	234	Greek Capital Letter Omega
δ	EB	235	Greek Small Letter Delta
∞	EC	236	Infinity
φ	ED	237	Greek Small Letter Phi
ε	EE	238	Greek Small Letter Epsilon
∩	EF	239	Intersection
≡	F0	240	Identical To
±	F1	241	Plus-Minus Sign
≥	F2	242	Greater-Than Or Equal To
≤	F3	243	Less-Than Or Equal To
∫	F4	244	Top Half Integral
∫	F5	245	Bottom Half Integral
÷	F6	246	Division Sign
≈	F7	247	Almost Equal To
°	F8	248	Degree Sign
·	F9	249	Bullet Operator
·	FA	250	Middle Dot
√	FB	251	Square Root
<sup>n</sup>	FC	252	Superscript Latin Small Letter N
<sup>2</sup>	FD	253	Superscript Two
■	FE	254	Black Square
	FF	255	No-Break Space

## Appendix A: Using the old 2.2 DMS Directory Browser



This browser is not recommended for use with R3.0.

### SETTING THE SEARCH PATHS

When searching the directory, the DMS Directory Browser uses preset search paths to determine where to look. To edit these search paths do the following:

1. From the main Outlook menu, pull down **Tools**→**Services**.
2. Double click the **X.500 Address Book Provider**.
3. Click the **Searching** tab.

The following procedures explain how to Add, Remove, and Edit entries in the Search Paths list.

#### ADDING AN ENTRY TO THE SEARCH PATHS LIST

1. Click the **Add** button next to the **Search Paths** list.
2. Type the desired search path in the **Add Search Path** dialog box.
3. Click **OK**.

#### REMOVING AN ENTRY FROM THE SEARCH PATHS LIST

1. Click the desired entry in the **Search Paths** list to highlight it.
2. Click the **Delete** button next to the **Search Paths** list. **Note:** If there is only one entry in the list, you cannot delete it. You can edit it or add another and then delete the first one.
3. Click **Yes** at the prompt: **Do you want to delete the selected search base?**

#### EDITING AN ENTRY IN THE SEARCH PATHS LIST

1. Click the desired entry in the **Search Paths** list to highlight it.
2. Click the **Edit** button next to the **Search Paths** list.
3. Make the desired changes to the search path in the **Edit Search Base Property** dialog box.
4. Click **OK**.

### ACCESSING THE DMS DIRECTORY USING THE DIRECTORY BROWSER

1. Open Outlook
2. Select the **Directory Browser** button on the toolbar.
3. This opens the DMS Directory using the Directory Browser

### MANUALLY SEARCHING THE DMS DIRECTORY

1. Start the DMS Directory Browser Application. If the DMS Directory Browser is set to automatically open the Directory, then a browse window will appear.

**Hint** If a browse window does not appear, then manually open one by selecting **Connect** and then selecting **Open** from the **File** menu. If the DN shown in the Base DN field is correct, click **OK**. Otherwise, correct the DN and click **OK**.

2. Browse to the part of the directory that you want to search by clicking the 'Plus' ( + ) symbols next to the entries in the left column. Start the search as low in the tree as you can. The higher you start the search, the longer the search will take. For example, starting the search at the "C=US, O=U.S. Government" level will take a very long time and impact directory performance.
3. Once a browse window is open and you have browsed to the level to start your search, from the **File** menu button, select **Search** to display the 'Search Parameters' dialog box.
4. Click the **Define Filter** button to display the 'Define Search Filter' dialog box.
5. Type a descriptive name in the **Name:** field.
6. Leave the **Subtree** radio button checked.
7. Click the drop-down arrow next to the **Attribute** field and choose the attribute that you want to search for from the list (probably **cn** or **ou**).
8. Click the pull-down arrow next to the **Operator** field and choose the operator for the type of search you want to perform. ("Contains" and "Equals" are the two most common operators).

**Hint** Searches can also be performed by clicking the **Search** (binoculars) icon.



If you use the **Equals** operator, you must type the search value exactly as it appears in the directory. If you use the **Contains** operator, you can type a partial value and get all of the entries that contain that partial value. Remember to make the value as specific as possible. If you searched on 'cn contains Smith'; you would get all of the entries whose common name contains Smith. This might return so many entries that the search results would be useless.

7. Type the target phrase (i.e., a name) into the **Value** field.
8. Click the **OK** button to save the filter, close the 'Define Search Filter' dialog box and display the 'Search Parameters' dialog box
9. Click the **OK** button to start the search.
10. Once you have found the entry, you can add it to your Personal Address Book by highlighting it and clicking the **Add to Address Book** button in the toolbar (or selecting **Add to PAB** from the Edit menu).



An alert window may appear to confirm over-writing an existing entry.

- Click the **Yes** button to overwrite the existing entry; otherwise, click **No**.
- An alert window may appear to warn you that the certificate will not be copied due to DN mismatch. (e.g., when copying AUTODIN PLA address with MFI's DN when MFI privilege bit is not set). This indicates a problem in the directory that you should report to your administrator.
- Rather than expanding (browsing) large subtrees in the directory (e.g., AUTODIN PLA subtree), use the Search feature. Performance and DIT Browser response will greatly improve.