

MCST 3901 / BC 10.3.0.1 IP

**Installation Procedures (IP)
for
Mission Command Staff Trainer (MCST)**

**Version 3.9.0.1 / BC 10.3.0.1
for
Army Golden Master (AGM) Windows XP
and
Army Golden Master (AGM) Windows Vista**

21 May 2012

Prepared for:

**Product Director, Strategic Mission Command
Aberdeen Proving Ground, MD 21005**

**These commodities are authorized by the US Government for export. They may not be transferred, trans-
shipped on a non-continuous voyage, or otherwise be disposed of in any other country, either in their original
form or after being incorporated into other end items, without prior written approval of the US Department
of State.**

Table of Contents

1. SCOPE	1
1.1 IDENTIFICATION	1
1.2 SYSTEM OVERVIEW	1
2. REFERENCED DOCUMENTS	2
3. SYSTEM ENVIRONMENT	2
3.1 SYSTEM REQUIREMENTS	2
3.1.1 <i>Hardware Requirements</i>	2
3.1.2 <i>Operating System Requirements</i>	2
3.2 SYSTEM AND SITE PREPARATIONS	2
3.2.1 <i>System Configuration</i>	2
3.2.2 <i>Operating System Preparation</i>	4
3.2.3 <i>Disk Preparation</i>	5
4. INSTALLATION INSTRUCTIONS	5
4.1 INSTALLATION PROCEDURES	5
4.2 INITIALIZING THE SOFTWARE	6
4.2.1 <i>Configuring PASS Client Interface (PCI) for SWB1.5 and SWB2.0 Installations</i>	7
4.2.2 <i>Configuring DDS Client Interface (DCI) for BC Marshall Installation</i>	9
5. DEINSTALLATION PROCEDURES	11
5.1 DEINSTALLATION OF THE MCST APPLICATION ONLY	11
5.2 DEINSTALLATION OF MCST AND ALL PREREQUISITE PACKAGES	11
5.2.1 <i>Windows XP</i>	11
5.2.2 <i>Windows Vista</i>	12
6. LIST OF CHANGES AND ENHANCEMENTS	12
7. NOTES	12
7.1 ACRONYMS AND ABBREVIATIONS	12
8. DOCUMENTATION IMPROVEMENT AND FEEDBACK	13
9. EXPORT CONTROL	13
APPENDIX A. REPLACING SECURITY CERTIFICATES	1
APPENDIX B. KNOWN ISSUES WITH WINDOWS 7 INSTALL	1
LIST OF FIGURES	
FIGURE 1. MCST APPLICATION DESKTOP ICONS	6
FIGURE 2. PCI ADMINISTRATOR UTILITY. CONFIGURING PCI FOR CONNECTIVITY WITH THE PASS SERVER.	8

MCST 3901 / BC 10.3.0.1 IP

FIGURE 3. PCI ADMINISTRATOR UTILITY. RESTART THE LOCAL PCI USING THE NEW PASS
PROPERTIES..... 9

FIGURE 4. DCI CLIENT GUI APPLICATION. CONFIGURING DCI FOR CONNECTIVITY WITH THE DDS
SERVER. 10

FIGURE 5. DCI CLIENT GUI APPLICATION. SUCCESSFUL CONNECTION WITH THE DDS SERVER. .. 10

LIST OF TABLES

TABLE 1-1. PERTINENT DOCUMENTATION 1

TABLE 2-1. REFERENCED DOCUMENTS 2

1. Scope

1.1 Identification

The identification information for the Mission Command Staff Trainer (MCST) Installation Procedures (IP) is as follows:

Segment Name: MCST
Version (V) Number(s): 3.9.0.1 / BC 10.3.0.1
Platform(s): Windows XP SP2 and Windows Vista SP2

1.2 System Overview

MCST is a stand-alone software training tool used for training Mission Command (MC) staff officers in staff operations in pre-deployment environments. It uses real ground force data and allows users to simulate sending various tactical messages on the real battlefield communication networks, as well as, situational awareness (SA) data to the Common Operation Picture (COP) using a built-in lightweight mapping tool.

MCST communicates with the BC network by publishing information to PASS or DDS, by broadcasting to SA multicast groups, and by sending tactical messages directly to BFAs.

MCST is designed for deployment and operation on standard COTS hardware running Microsoft Windows XP SP2 or greater as well as Microsoft Windows Vista SP2 or greater.

The following documents are not referenced within this IP, but provide additional information on the system:

Table 1-1. Pertinent Documentation

Document Identifier	Title	Version	Date
MCST. 3901 / BC 10.3.0.1 UM	User Manual (UM) for Mission Command Staff Trainer (MCST)	3901 / BC 10.3.0.1	21 May 2012

For technical assistance and problem reporting, contact the following:

C4ISR Support Operations Center
Toll Free: 1-877-839-0813
Commercial: 1-254-287-1608
NIPR: c4isr.support@us.army.mil
Web: <https://hd.kc.us.army.mil>

2. Referenced Documents

Table 2-1 lists software product documentation that is specifically referenced within this IP.

Table 2-1. Referenced Documents

Document Identifier	Title	Version	Date
MCST. 3901 / BC 10.3.0.1 SVD	Software Version Description (SVD) for the MCST	3901 / BC 10.3.0.1	21 May 2012

3. System Environment

3.1 System Requirements

3.1.1 Hardware Requirements

For the full install (including optional TMS install):

- Software Block (SWB) 1.5 & SWB2: 1.0 GB of disk space (minimum)
- SWB BC Marshall: 1.1 GB of disk space (minimum)
- 2.0 GB Random Access Memory (RAM) (minimum)

3.1.2 Operating System Requirements

MCST must be installed on Microsoft Windows XP SP2 (or greater) or Microsoft Windows Vista SP2 (or greater) operating system.

MCST software has been successfully tested on Windows 7. However, the prerequisite or optional software that are installed with MCST (see sections [3.2.1.3](#) and [3.2.1.4](#)) did not have a requirement from the Army to support Windows 7 at the time of their release, therefore we cannot guarantee that any issues found relating to Windows 7 are addressed.

See [Appendix B](#) of this document for the list of issues found during MCST 3901 test on Windows 7 system.

3.2 System and Site Preparations

3.2.1 System Configuration

3.2.1.1 Security Certificates

MCST 3901 / BC 10.3.0.1 IP

MCST relies on certificates to communicate with ABCS components that require secure links. Certificates at both ends of the link must be compatible and unexpired for communication to occur. When configured for SWB 1.5 and SWB 2, MCST uses a certificate for secure communications with the Battle Command Server (BCS) PASS service. When configured for SWB BC Marshall, MCST uses certificates for secure communications with the Battle Command Common Services (BCCS) C2R Web Service and the Data Dissemination Services (DDS).

Certificates installed with this MCST release are identified with these attributes:

Filename - *truststore.jks*:

Filename - *keystore.jks*:

Owner: CN=BccsServer, OU=USA, OU=PKI, OU=DoD, O=U.S.Government, C=US

Issuer: CN=DOD CA-17, OU=PKI, OU=DoD, O=U.S. Government, C=US

Serial number: efae

Valid from: Wed May 20 08:46:58 EDT 2009 until: Sun May 20 08:46:58 EDT 2012

Certificate fingerprints:

MD5: 06:10:EC:84:36:BB:2B:BB:CC:BF:7F:94:D8:FB:C9:36

SHA1: 76:10:47:6F:D4:7C:21:68:9D:FB:87:B9:C1:5D:75:2E:3A:1B:36:23

Certificates used by the BCS PASS service must be compatible with the **truststore.jks** file installed in MCST.

Certificates used by the BCCS C2R Web Service and the Data Dissemination Services (DDS) must be compatible with the **truststore.jks** and **keystore.jks** files installed in MCST.

NOTE: For procedures on replacing security certificates, please refer to **Appendix A. Replacing Security Certificates**.

3.2.1.2 Saving projects from the previous MCST Install

Starting with the version 3.4.0.0, MCST is backwards compatible. Projects created with version 3.3.0.0 can be used with version 3.4.0.0. Therefore, the following steps should be taken before removing the previous, 3.3.0.0 version of MCST from the system:

1. The user has to make sure that projects directories, such as *C:\Program Files\MCST\data\projects\<project name>*, are copied to a safe location before uninstalling MCST 3.3.0.0.
2. After installing MCST, version 3.4.0.0, saved project directories can be copied to the *projects* directory where MCST can access them.

3.2.1.3 MCST Software Prerequisites for Software Blocks 1.5 and 2

MCST requires these software components for Software Block 1.5 and Software Block 2 operation. The MCST Installer provides and installs, in the order listed, the following prerequisites:

- Java Runtime Environment (JRE) version 6 update 13
- PASS Client Interface (PCI) version 5.0.4.0

MCST 3901 / BC 10.3.0.1 IP

- Common Message Processor (CMP) Client version 5.1.3.0
- Ground Tactical Communications Server (GTCS) Client Tools version 5.1.7.0
- Ground Tactical Communications Server (GTCS) Client FCS Excursion version 5.1.7.3

3.2.1.4 MCST Software Prerequisites for Software Block BC Marshall:

MCST requires these software components for Software Block BC Marshall operation. The MCST Installer provides and installs, in the order listed, the following prerequisites:

- Java Runtime Environment (JRE) version 6 update 13
- MS .NET Framework 2.0
- DDS Client Interface (DCI) version 5.1.5.6
- Common Message Processor (CMP) Client version 5.1.3.0
- Ground Tactical Communications Server (GTCS) Client Tools version 5.1.7.0
- Ground Tactical Communications Server (GTCS) Client FCS Excursion version 5.1.7.3

3.2.1.4.1 Setting User Permissions for a Software Block BC Marshall Installation

For proper operation of MCST in Software Block BC Marshall, a system administrator must ensure that all system users, i.e., members of the **Users** group have **Write** privileges to the following GTCS Client configuration files:

GTCS-Org.xml
GTCS-Static.xml

3.2.1.5 Firewall Settings

If the system to be used has a network firewall installed and enabled, the system administrator must configure the firewall to open these ports:

inbound	vmf_msg_port	1581/tcp
inbound	vmf_msg_port	1581/udp
inbound	sr_port	1624/udp

3.2.2 Operating System Preparation

3.2.2.1 Microsoft Windows Vista settings

3.2.2.1.1 Vista User Account Control feature

Before installing MCST on Windows Vista, the system administrator must disable the User Account Control feature as follows:

MCST 3901 / BC 10.3.0.1 IP

1. Select **Start > Control Panel > User Accounts > User Accounts > Turn User Account Control On or Off**
2. Uncheck **Use User Account Control...**
3. Press **OK**
4. Restart the system.

3.2.2.1.2 Post Install Settings

After MCST install is complete, the system administrator must change permissions on two installed files as follows:

1. Select **Start > All Programs > Accessories > Windows Explorer**
2. Navigate to **Desktop > Computer > C:\Program Files\GTCS Client\data\config**
3. Add **Write** permission for **Users** to each of the following lines:
GTCS-Org.xml
GTCS-Static.xml

These permissions may be added through each file's **Properties** dialog by selecting the **Security** tab, pressing **Edit**, choosing the **Users** group, and then selecting the **Allow Write** checkbox.

4. Press **OK** to apply the permission change.

3.2.3 Disk Preparation

The SW is delivered to the Common Software Configuration Management Team on a Compact Disk-Read Only Memory (CD-ROM) and usually is shipped to the customers by FedEx.

4. Installation Instructions

4.1 Installation Procedures

The MCST installer provides a convenient method to install the MCST application and all of its software prerequisites. Before initiating MCST installation, any existing copies of MCST, PCI (for SWB1.5 and SWB2), DCI (for BC Marshall), CMP, GTCS Client, GTCS Client Tools and TMS should be uninstalled from the system. The MCST Installer will install the appropriate versions of these components.

1. Run the MCST installer .exe file by double-clicking it.
2. After self-extracting, the welcome screen of the **MCST - InstallShield Wizard** appears. Click **Next** to proceed to **Software Block Selection**.
3. Select the software block of the system where MCST is to be installed – **SWB1.5, SWB2, or BC Marshall**.
4. Click **Next** to proceed to the **Prerequisite Installations** screen. The **Prerequisite Installations** screen allows you to select whether to install prerequisite packages or not. If a prerequisite package application is already installed, the check box is disabled.

NOTE: For a clean install of MCST and all of its prerequisite software packages, it is strongly suggested to **(i)** take note of the packages with disabled check boxes, **(ii)** cancel the

MCST 3901 / BC 10.3.0.1 IP

InstallShield Wizard, and (iii) use the Control Panel utility (**Add or Remove Programs** for XP, **Programs and Features** for Vista) to uninstall the packages from the system.

5. Click **Next** to accept the default destination folders (or click the corresponding **Change...** button of a prerequisite package to select a different destination folder for that application).
6. In the **Optional TMS Install** panel click **Yes** (to install TMS) or **No** (to ignore TMS installation).

NOTE: TMS installation can significantly extend MCST installation time.

7. In the next MCST **Destination Folder** screen, click **Next** to select the default location (or click the **Change...** button to select a different destination folder for the MCST application).
8. On the next screen, click **Install** to initiate the installation.
9. The **Installing MCST** panel will appear with a status bar showing the installation progress.
10. When the **InstallShield Wizard Completed** panel appears, click **Finish**, then click **Yes** on the **MCST Installer Information** dialog box to reboot the system or you may click **No** to reboot the system later.

NOTE: To ensure that the software is installed properly and all services start as intended, reboot the system after MCST installation.

4.2 Initializing the Software

After the successful installation of the **MCST** application, depending on the software block selected, desktop icons will be displayed as shown in **Figure 1** below.

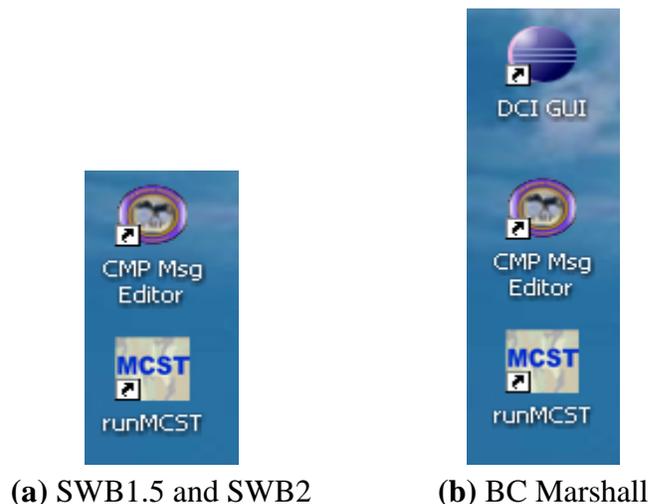


Figure 1. MCST Application Desktop Icons.

NOTE:

For SWB1.5 and SWB2 installation, make sure that the local PASS Client Interface (PCI) is configured to connect to the PASS server. (See Section [4.2.1](#)).

MCST 3901 / BC 10.3.0.1 IP

For BC Marshall installation, make sure that the local DDS Client Interface (DCI) is configured to connect to the DDS server. (See Section [4.2.2](#))

After making sure that the local client interface is properly configured to connect to the message server, double-click the **runMCST** icon located on the desktop to start the application.

4.2.1 Configuring PASS Client Interface (PCI) for SWB1.5 and SWB2.0 Installations

From Windows **Start** menu, select **Run...** to display the **Run** dialog box. In the **Run** dialog box, enter the following:

C:\h\PCI\bin\PCI_StartAdminGUI.bat

and click the **OK** button to run the **PCI Administrator** utility software.

NOTE:

For your convenience you may create desktop short cut for **PCI_StartAdminGUI.bat**.

In the **Main Config** tab, select the **PASS Properties** tab. Update the date fields indicated in **Figure 2:**

1. Username
 2. Password
 3. Server IP
 4. Server Port
 5. Truststore
 6. Truststore Password
- with the configuration data for the PASS server that MCST will connect to, then click **Save**.

NOTE:

Verify that the Server is *reachable* from your computer by using the **ping** command on the *Server IP* address on your computer's DOS window.

To display the DOS window, select **Start→Run...**, then type **command** on the **Run** dialog box's data field and click **OK**.

MCST 3901 / BC 10.3.0.1 IP

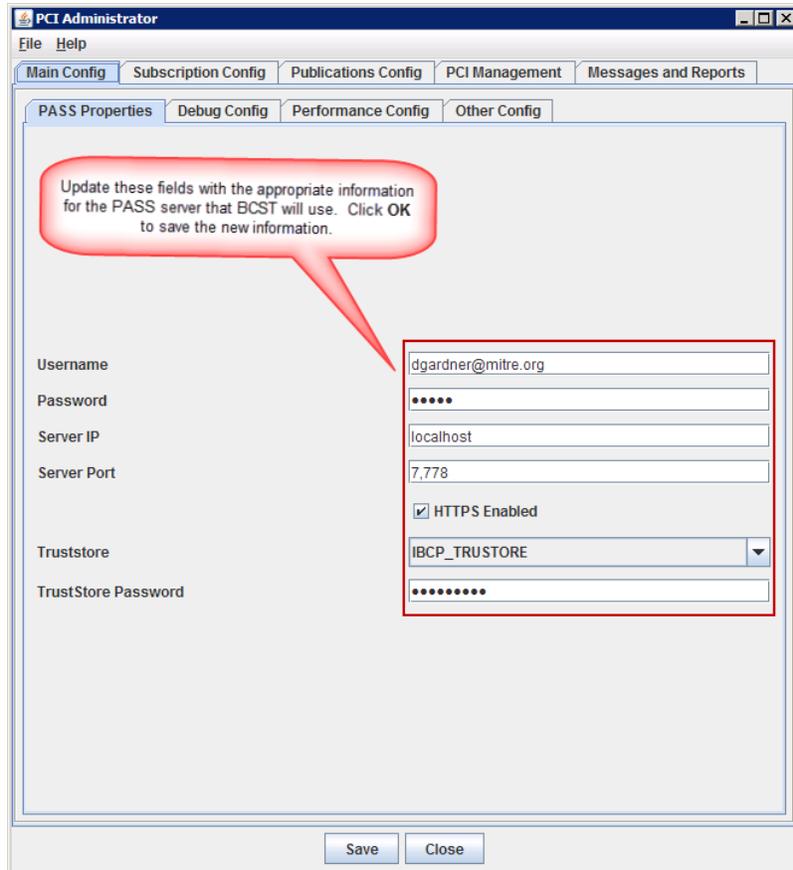


Figure 2. PCI Administrator utility. Configuring PCI for connectivity with the PASS server.

To reset PCI with the new data, select the **PCI Management** tab and click the **Restart PCI** button, as shown in **Figure 3** below.

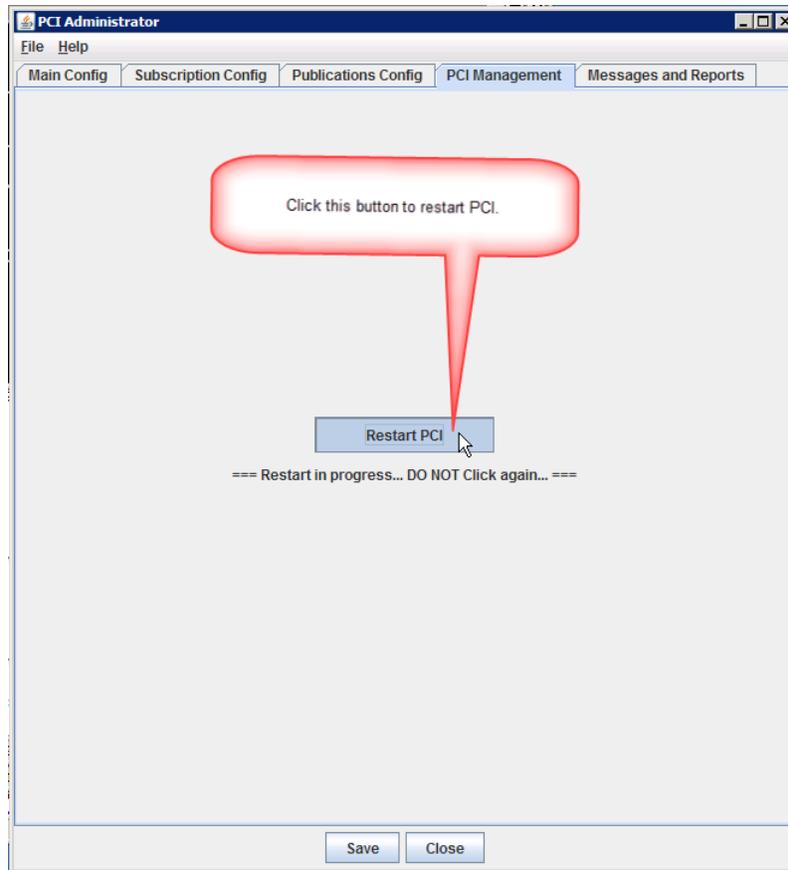


Figure 3. PCI Administrator utility. Restart the local PCI using the new PASS properties.

After the **Restart PCI** button is clicked, the message:

=== Restart in progress... DO NOT click again... ===

appears below the button.

At the completion of the restart process, the following the message above is replaced with:

=== PCI Restart DONE ===

Select the **Messages and Reports** tab, then select the **PCI Messages** sub-tab to determine whether PCI successfully connected to the PASS server or not. If the PASS server was verified to be reachable (using **ping**) and if the information entered in the **PASS Properties** tab is correct, the **PCI Messages** sub-tab will display a message that PCI had successfully connected to the PASS server.

4.2.2 Configuring DDS Client Interface (DCI) for BC Marshall Installation

Double click on the **DCI GUI** desktop icon (see **Figure 1(b)** above) to display the DCI GUI application. Update the fields in the **DDS Configuration** Bundle with data for the DDS server that MCST will connect to, then click **Save**. DCI will automatically restart and attempt to connect to the DDS server using the new set of DDS configuration data.

MCST 3901 / BC 10.3.0.1 IP

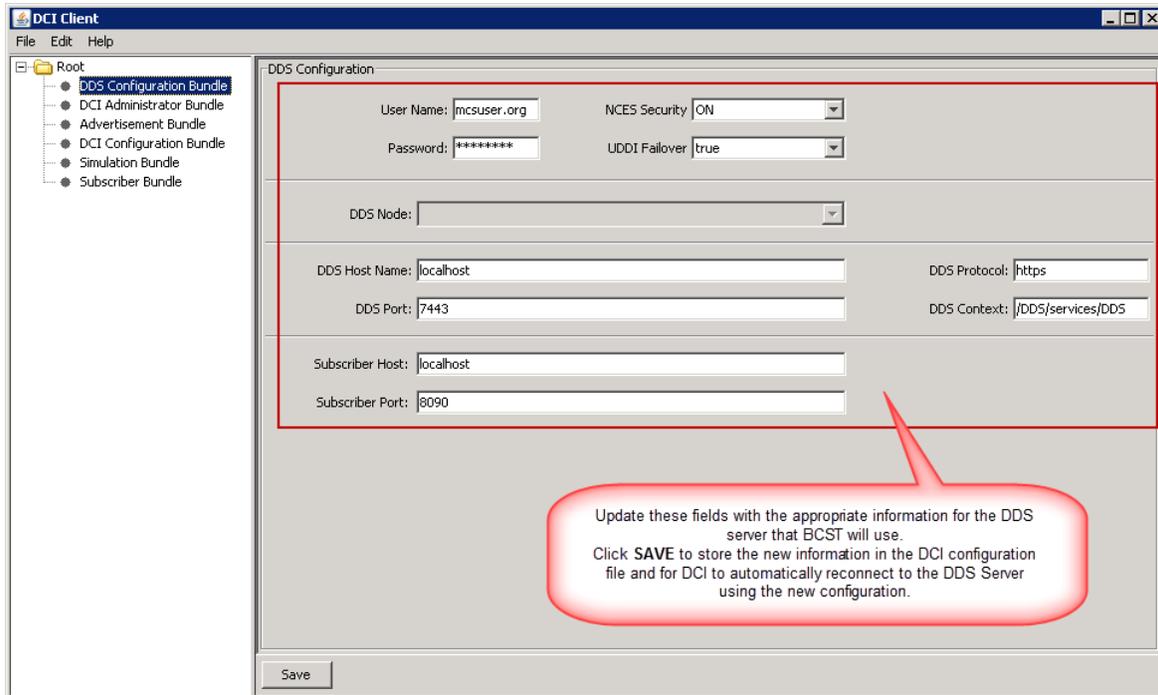


Figure 4. DCI Client GUI application. Configuring DCI for connectivity with the DDS server.

NOTE:

For *DDS Host Name*, use the IP address of the DDS host computer. Also, verify that the server IP address is *reachable* from your computer by using the **ping** command on DDS IP address.

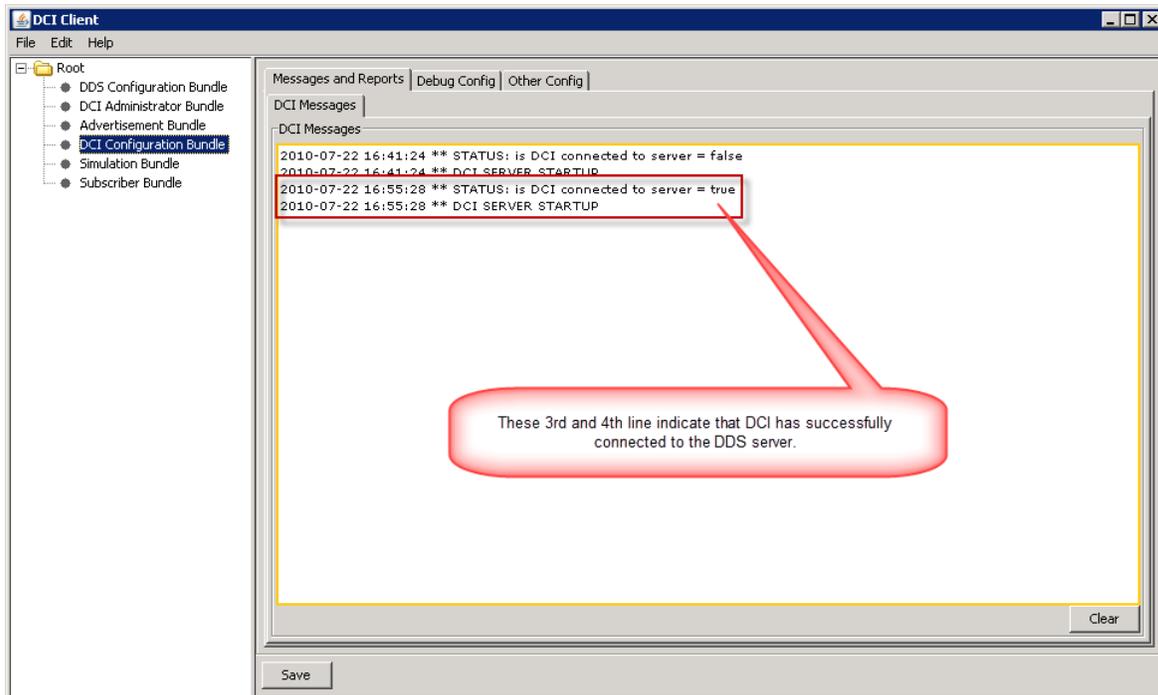


Figure 5. DCI Client GUI application. Successful connection with the DDS server.

If the DDS host computer is verified to be reachable from the MCST host computer (using **ping**) and the information entered in the **DDS Configuration Bundle** is correct, then the successful connection with the DDS server will be indicated in the **DCI Configuration Bundle's DCI Message** sub-tab similar to the 3rd and 4th text lines of **Figure 5** above.

5. Deinstallation Procedures

5.1 Deinstallation of the MCST Application Only

To deinstall the **MCST** application only, you may use the MCST installer .exe file.

1. Run the MCST installer .exe file by double-clicking on it.
2. Click **Next** to continue.
3. Choose the **Remove** option and click **Next**.
4. Click **Finish** to complete the deinstallation process.
5. After a successful deinstallation of MCST, a dialog box appears informing the user to reboot the system. Click **Yes**.

The deinstallation procedure will only remove files placed on the machine during installation. Any data files created during earlier use of MCST will remain on the system. If desired, you may manually delete the folder **C:\Program Files\MCST**, if MCST was installed in the default folder destination) or whatever non-default folder MCST was installed,

Also, the MCST deinstallation procedure shown above will not remove any of the prerequisite packages installed during the MCST installation process.

5.2 Deinstallation of MCST and All Prerequisite Packages

5.2.1 Windows XP

To deinstall the **MCST** application and all the prerequisite packages installed in the system, use the **Add or Remove Programs** utility in the **Control Panel**.

1. Select **Start > Control Panel > Add or Remove Programs**
2. Select the **MCST** icon on the list.
3. Click the **Remove** button that appears on the right.
4. A dialog asking if the user wants to uninstall MCST appears. Click **Yes**. A dialog box appears showing the progress of the deinstall process.
5. After Windows uninstalled MCST a dialog box appears asking the user to reboot the system. Click **Yes**.
6. After the system successfully rebooted, using the **Add or Remove Programs**, uninstall the following pre-requisite packages in the order (reverse order that they were installed into the system) given below:
 - a. GTCS Client Tool
 - b. GTCS Client FCS Excursion
 - c. CMP

MCST 3901 / BC 10.3.0.1 IP

- d. PCI (for SWB1.5 and SWB2) or DCI (for BC Marshall)
- e. Java Runtime Environment (jre)

You may or may not reboot the system after a package is uninstalled. However, make sure to reboot the system after all pre-requisite packages were deinstalled.

5.2.2 Windows Vista

To deinstall the **MCST** application and all the prerequisite packages installed in the system, use the **Programs and Features** utility in the **Control Panel**.

1. Click on the start (Windows Logo) icon and open the **Control Panel**. From the **Control Panel**, select **Programs and Features**.
2. From the list of programs listed in the **Programs and Features** window, highlight **MCST** and click on the **Uninstall** button located at the toolbar.
3. A dialog asking if the user wants to uninstall MCST appears. Click **Yes**. A dialog box appears showing the progress of the deinstall process.
4. After Windows uninstalled MCST a dialog box appears asking the user to reboot the system. Click **Yes**.
5. After the system successfully rebooted, using **Programs and Features**, uninstall the following pre-requisite packages in the order given below:
 - a. GTCS Client Tool
 - b. GTCS Client FCS Excursion
 - c. CMP
 - d. PCI (for SWB1.5 and SWB2) or DCI (for BC Marshall)
 - e. Java Runtime Environment (jre)

You may or may not reboot the system after a package is uninstalled. However, make sure to reboot the system after all pre-requisite packages were deinstalled).

NOTE: Starting with version 3.4.0.0, MCST is backwards compatible. Projects created with version 3.3.0.0 can be used with subsequent versions. Therefore, the user has to make sure that projects directories are copied to a safe location before uninstalling MCST. After installing MCST, version 3.4.0.0, saved project directories can be copied to the *projects* directory where MCST can access them.

6. List of Changes and Enhancements

Refer to [Appendix A](#) of the companion SVD document

7. Notes

7.1 Acronyms and Abbreviations

ABCS	Army Battle Command System
BCS	Battle Command Server
BCCS	Battle Command Common Services

MCST 3901 / BC 10.3.0.1 IP

C2R	Command and Control Registry
CD-ROM	Compact Disk-Read Only Memory
CMP	Common Message Processor
COP	Common Operation Picture
DCI	DDS Client Interface
DDS	Data Dissemination Services
GTCS	Ground Tactical Communications Server
IP	Installation Procedures Internet Protocol
MB	Megabyte
MCST	Mission Command Staff Trainer
MSI	Microsoft Installer
PASS	Publish and Subscribe Services
PCI	PASS Client Interface
PD	Product Director
RAM	Random Access Memory
SVD	Software Version Description
SW	Software
SWB	Software Block

8. Documentation Improvement and Feedback

Comments and other feedback on this document should be directed to:

C4ISR Support Operations Center
Toll Free: 1-877-839-0813
Commercial: 1-254-287-1608
NIPR: c4isr.support@us.army.mil
Web: <https://hd.kc.us.army.mil>

9. Export Control

The MCST contains components of the Common Message Processor (CMP). CMP is ITAR Restricted-Use Data and is not to be copied or transferred to unauthorized third parties. It may not be transferred, trans-shipped on a non....approval of the US state Department. The CMP software is copyright 2002 JB Management, Inc- Sponsored by US Government under Task

MCST 3901 / BC 10.3.0.1 IP

Orders 02FM22625A and GST0205CJ009 issued against JB Management, Inc's GSA Schedule Contract No GS-35F-0106M. The US Government has a paid-up, non-exclusive, irrevocable worldwide license in the CMP Software product to reproduce, prepare derivative works, and utilize the CMP software by and on behalf of the US Government. However, the US Government's license does not include the right to distribute the CMP Software to the general public or otherwise outside the US Government for work not specifically on behalf of the US Government. That right belongs exclusively to JB Management, Inc.

Appendix A. Replacing Security Certificates

Security certificates expire and must be replaced periodically with compatible certificates at both ends of a link to maintain communication.

- **MCST for SWB1.5 and SWB2**

For SWB 1.5 and SWB 2, MCST uses a **truststore.jks certificate file** to secure communications with the **BCS Publish and Subscribe Services (PASS) Server**. This certificate may be upgraded as follows:

1. Turn off the PCI Service

- a. From the desktop, select **Start > All Programs > Administrative Tools > Services**
- b. Select **PASS Client Interface** in the list.
- c. Click the **Stop** button or right-click **PASS Client Interface** and select the **Stop** menu item.

2. Save the current PCI certificate file

- a. Open the File Manager.
- b. Go to the directory *C:\h\PCI\data*.
- c. Rename the file **truststore.jks** to **truststore.jks.sav**.

3. Copy the new certificate file to the PCI directory

- a. Copy the new **truststore.jks** file to the *c:\h\PCI\data* directory.

4. Restart the PCI service

- a. From the desktop, select **Start > All Programs > Administrative Tools > Services**
- b. Select **PASS Client Interface** in the list t.
- c. Click the **Start** button or right-click **PASS Client Interface** and select the **Start** menu item.

Certificates used by the BCS PASS service must be compatible with the **truststore.jks** file installed in MCST.

- **MCST for SWB BC Marshall**

For SWB BC Marshall, MCST uses **truststore.jks** and **keystore.jks** certificate files to secure communication with the BCCS C2R Web Service and the Data Dissemination Service (DDS). These certificates may be upgraded as follows:

1. Exit the MCST application

- a. Select **File > Quit**

2. Turn off the DCI Service

- a. From the desktop, select **Start > All Programs > Administrative Tools > Services**
- b. Select **DDS Client Interface** in the list
- d. Click the **Stop** button or right-click **DDS Client Interface** and select the **Stop** menu item.

3. Save the current C2R certificate files

- a. Open the File Manager.

MCST 3901 / BC 10.3.0.1 IP

- b. Go to the directory *C:\Program Files\MCST\data\C2R\wsdata\SSLData\Certificates*.
- c. Rename files **truststore.jks** and **keystore.jks** to **truststore.jks.sav** and **keystore.jks.sav**, respectively.
- 4. Save the current DCI certificate files**
 - a. Go to directory *C:\Program Files\DCI\bin\Certificates*
 - b. Rename files **truststore.jks** and **keystore.jks** to **truststore.jks.sav** and **keystore.jks.sav**, respectively.
- 5. Copy the new certificate files to the C2R and DCI directories**
 - a. Copy the new **truststore.jks** and **keystore.jks** files to the directories named above.
- 6. Restart the DCI service**
 - a. From the desktop, select **Start > All Programs > Administrative Tools > Services**
 - b. Select **DDS Client Interface** in the list.
 - e. Click the **Start** button or right-click **DDS Client Interface** and select the **Start** menu item.
- 7. Resume using MCST**

Certificates used by the BCCS C2R Web Service and the Data Dissemination Services (DDS) must be compatible with the **truststore.jks** and **keystore.jks** files installed in MCST.

Appendix B. Known Issues with Windows 7 Install.

NOTE: The following issues were found during testing on Windows 7 operating system. This material is provided for informative purposes only. See [section 3.1.2](#).

1. Mouse wheel zooming on MCST map may not be working properly even if the latest drivers used. To fix the issue, go to Control Panel -> Hardware & Sound -> Devices & Printers -> Mouse. When "Mouse Properties" window pops up, select "Wheel" tab and click "Identify programs that don't scroll correctly..." link in the middle of GUI. When new pop up window opens use "Add" button to place 'java' on the list if it is missed. Please Note: Windows 7 does not save this setting permanently (could be related to removing programs process) so this procedure needs to be repeated once mouse wheel zooming on MCST map fails again.
2. On a monitor with the screen resolution 1280 x 1024, the Add New Hostile/Other GUI opens up collapsed. When touched by the mouse on the edge, dialog appears.
3. For optional TMS Install feature, TMSConfig can install all three versions of ICSF (4.5.2.8, 4.5.3.4, 4.5.3.8) on Windows 7. Generation of tracks using TMS Generator on Windows 7 is unpredictable. TMS Generator occasionally crashes in the native code.
4. GTCS-GUI application may fail to update CMP inbound/outbound folder monitoring (Win7x64). It sets Outbound Data to CMP_HOME\data\inbound instead of CMP_HOME\data\outbound.
In this case, manual configuration is required:
 1. Open C:\Program Files (x86)\GTCS Client\data\Config\GTCS-AppInterface.xml
 2. Change <outbound>C:\Program Files (x86)\CMP\data\inbound</outbound> to <outbound>C:\Program Files (x86)\CMP\data\outbound</outbound> and save.
 3. Restart GTCS.