



## Appendix A - Plugin Worksheets

Provided in this Appendix are sample worksheets for each source plugin that is available. Specifically, plugins are currently provided to access the following sources:

- Air Force Weather (WX)
- Air Order of Battle Database (AOBD)
- Automated Logistics Information to the AOC (ALIA)
- Automated Message Handling System v3.6 (AMHS36)
- Demand Driven Direct Digital Dissemination (5D)
- Electronic Intelligence (ELINT)
- Facilities Infrastructure Engineering System (FIRES)
- Image Product Library v1.0 (IPL)
- Image Product Library v2.1 (IPL21)
- Image Product Library v2.5 (IPL25)
- Image Product Library v3.0 (IPL30)
- Imagery Exploitation Support System (IESS)
- InfoSphere Management System (ISM)
- Intelink-Hydra (INT)
- Intelink-Meta Search (META)
- Military Equipment Parametric and Engineering Database (MEPED)
- Military Integrated Data Base (MIDB)
- Moving Target Indicator (MTIX)
- Moving Target Indicator Real Time (MTIX\_RT)

## Air Force Weather (WX)

Add New WX Source		
Configuration Item	Value	Item Description
Air Force Weather Description	<input type="text" value="Air Force Weather Source"/>	This field describes Air Force Weather. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Air Force Weather URL	<input type="text" value="http://hostname:80"/>	This field describes the URL for the Air Force Weather Web Server.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-1- Add New WX Source

## Air Order of Battle Database (AODB)

Add New AODB Source		
Configuration Item	Value	Item Description
AODB Description	<input type="text" value="AODB Source"/>	This field describes the AODB. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Network Security Level	<input type="text" value="T"/>	This field will determine the security classification of the returned hits.
AODB Oracle Tnsnames Entry	<input type="text" value="AODB"/>	This field specifies the name in the Oracle tnsnames.ora file the aodb_plugin will use to connect to the AODB Oracle Server.
AODB Database Login	<input type="text" value="flxrps"/>	This field specifies the database login the aodb_plugin will use to Login to the AODB database.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
AODB Database Password	<input type="text"/>	This field specifies the database password the aodb_plugin will use to Login to the AODB database.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-2- Add New AODB Source

**Note:** The *AODB Database Login* needs to be set up on the AODB server with the same permissions as the user *flxrps*.

**Note:** Both AODB and FIRES are backside sources that that require configuration in addition to that provided in the “Backside Sources” section of the interface. After adding the FIRES or AODB source, telnet into the Broadsword server, su to *root* and execute the following:

```
# cd /opt/bswd3.0/odbc/oracle7/network/admin
```

```
# vi tnsnames.ora
```

In this file, there will be a record for the FIRES or AODB source. The IP address and port number listed should be the same as the IP and port numbers listed on the source’s server. For more information on how to get this information from the source’s server, contact your local administrator for that data source.

# Automated Logistics Information to the AOC (ALIA)

Configuration Item	Value	Item Description
ALIA Description	ALIA Source	This field describes the ALIA. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Network Security Level	S	This field will determine the security classification of the returned reports.
ALIA Oracle IP Address	I	This field specifies the IP Address of the ORACLE server the alia_plugin will use to connect to the ALIA database.
ALIA Oracle Port	1521	This field specifies the port of the ORACLE server the alia_plugin will use to connect to the ALIA database.
ALIA Oracle SID Instance Name	BASE	This field specifies the name in the oracle tnsnames.ora file the alia_plugin will use to connect to the ALIA Oracle Server.
ALIA Database Login	hlrddb	This field specifies the database login the alia_plugin will use to Login to the ALIA database.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/group Privileges Administrator functions.
Database Password	I	This field specifies the database password the alia_plugin will use to Login to the ALIA database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-3- Add New ALIA Source

## Automated Message Handling System v3.6 (AMHS36)

Add New AMHS36 Source		
Configuration Item	Value	Item Description
AMHS Description	AMHS 3.6 Source	This field describes the AMHS. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
AMHS URL	http://hostname:80	This field describes the URL for the AMHS Web Server.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-4-Add New AMHS36 Source

**Note:** When a new AMHS36 source is configured, the *Access Control* parameter should not be set to *Local and Remote Users*. This constraint will be forced by the system in a future release of Broadsword.

## Demand Driven Direct Digital Dissemination (5D)

Configuration Item	Value	Item Description
5D Description	5D Source	This field describes the 5D. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
5D Sybase IP Address		This field specifies the IP Address of the SYBASE server the 5d_plugin will use to Connect to the 5D database.
5D Sybase Port	2025	This field specifies the port of the SYBASE server the 5d_plugin will use to Connect to the 5D database.
5D Database Name	FIVED_DB	This field specifies the name of the SYBASE Database the 5d_plugin will use to Connect to the 5D database.
5D Database Login		This field specifies the database login the 5d_plugin will use to Login to the 5D database.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
5D Database Password		This field specifies the database password the 5d_plugin will use to Login to the 5D database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-5-Add New 5D Source

**Notes:** The *5D Database Login* needs to be created on the 5D server. This sybase user needs to default to the FIVED\_DB database. Within the FIVED\_DB database assign the user the 5D specified group *sel\_only*, which is part of the baseline system.

Sybase will not accept a database login name that begins with a numeric digit. For example, use FIVED not 5D.

## Electronic Intelligence (ELINT)

Add New ELINT Source		
Configuration Item	Value	Item Description
Elint Stream Description	<input type="text" value="Elint Stream Source"/>	This field describes Elint Stream. This will appear in the preferences section of the client.
Elint TCP/IP Port	<input type="text"/>	This is the TCP/IP port where the ELINT Server is running
Elint IP address	<input type="text"/>	This is the IP Address where the ELINT Server is running
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-6 Add New ELINT Source

# Facilities Infrastructure Engineering System (FIRES)

Add New FIRES Source		
Configuration Item	Value	Item Description
FIRES Description	<input type="text" value="FIRES Source"/>	This field describes the FIRES system. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
FIRES Oracle Tnsnames Entry	<input type="text" value="FIRES"/>	This field specifies the name in the Oracle tnsnames.ora file the fires_plugin will use to connect to the FIRES Oracle Server.
FIRES Database Login	<input type="text" value="fires_db_acct"/>	This field specifies the database login the fires_plugin will use to Login to the FIRES database.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
FIRES Database Password	<input type="text"/>	This field specifies the database password the fires_plugin will use to Login to the FIRES database.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-7-Add New FIRES Source

**Note:** Both AODB and FIRES are backside sources that that require configuration in addition to that provided in the “Backside Sources” section of the interface. After adding the FIRES or AODB source, telnet into the Broadsword server, su to *root* and execute the following:

```
# cd /opt/bswd3.0/odbc/oracle7/network/admin
```

```
# vi tnsnames.ora
```

In this file, there will be a record for the FIRES or AODB source. The IP address and port number listed should be the same as the IP and port numbers listed on the source’s server. For more information on how to get this information from the source’s server, contact your local administrator for that data source.

## Image Product Library v1.0 (IPL)

Configuration Item	Value	Item Description
IPL Description	IPL 1.0 Source	This field describes the IPL. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
IPL Host IP Address		This field specifies the IP address the ipl_plugin will use to connect to the IPL "pcr" process.
IPL TCP/IP Port	5004	This is the TCP/IP port that the ipl_plugin will use to connect to the IPL "pcr" process.
IPL Site Name		This is the site name of the IPL to query. This should match the IPL Site Name as configured in the IPL download file.
IPL Host IP Address		This is the IP address of the IPL to query. This should match the IPL IP Address as configured in the IPL download file.
Public Ftp Directory		This is the directory path where users manually ftp files which will be reviewed by the Catalog manager.
IPL Order Status Port	5007	This is the port that IPL will send status messages to after a order request.
Harvest TCP/IP port	8501	This is the TCP/IP port that the Harvest daemon is using.
Format Conversion Flag	N	If this field is set to Y, then Broadsword will perform all conversion/compression.
IPL Account	ipamngr	This is the IPL account Broadsword uses to connect to IPL.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IPL Password		This is the IPL password Broadsword uses to connect to IPL.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Reset Form    Cancel    OK

Figure A-8-Add New IPL Source

## Imagery Product Library v2.1 (IPL21)

Configuration Item	Value	Item Description
IPL 2.1 Description	IPL 2.1 Source	This field describes the IPL 2.1. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
IPL 2.1 Host IP Address		This field specifies the IP address the ipl21_plugin will use to connect to the IPL "pcrpers" process.
IPL 2.1 TCP/IP Port	5990	This is the TCP/IP port that the ipl21_plugin will use to connect to the IPL "pcrpers" process.
IPL 2.1 Site Name		This is the site name of the IPL to query. This should match the IPL Site Name as configured in the IPL download file.
IPL Host IP Address		This is the IP address of the IPL to query. This should match the IPL IP Address as configured in the IPL download file.
Public Ftp Directory		This is the directory path where users manually ftp files which will be reviewed by the Catalog manager.
IPL 2.1 Catalog Ingest Area		This is the directory path to place files being cataloged for a particular LPA.
IPL Order Status Port	5007	This is the port that IPL will send status messages to after a order request.
IPL 2.1 Account		This is the IPL account Broadsword uses to connect to IPL.
IPL 2.1 Sybase IP Address		This field specifies the IP Address of the SYBASE server the ipl21_plugin will use to Connect to the IPL21 database.
IPL 2.1 Sybase Port	8200	This field specifies the port of the SYBASE server the ipl21_plugin will use to Connect to the ipl21 database.
IPL21 Database Name	IPL20db	This field specifies the name of the SYBASE Database the ipl21_plugin will use to Connect to the ipl21 database.
IPL 2.1 SQS Sybase Server IP Address		This field specifies the IP Address of the SYBASE SQS server the ipl21_plugin will use to Connect to perform Geographic queries.
IPL 2.1 SQS Sybase Server Port	8400	This field specifies the port of the SYBASE SQS server the ipl21_plugin will use to Connect to perform Geographic queries.
IPL 2.1 Database Login		This field specifies the database login the ipl21_plugin will use to Login to the IPL21 database.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IPL 2.1 Password		This is the IPL password Broadsword uses to connect to IPL.
IPL 2.1 Database Password		This field specifies the database password the ipl21_plugin will use to Login to the IPL21 database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-9-Add New IPL21 Source

**Note:** On the IPL server create a Sybase user to have *select only* permissions on the desired LPA database user-defined tables. Since the baseline system does not supply a Sybase-defined group, it is recommended that one be created for use thereafter.

## Imagery Product Library v2.5 (IPL25)

Configuration Item	Value	Item Description
IPL 2.5 Description	IPL 2.5 Source	This field describes the IPL 2.5. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
IPL 2.5 Host IP Address		This field specifies the IP address the ipl25_plugin will use to connect to the IPL "pcrpers" process.
IPL 2.5 TCP/IP Port	5990	This is the TCP/IP port that the ipl25_plugin will use to connect to the IPL "pcrpers" process.
IPL 2.5 Site Name		This is the site name of the IPL to query. This should match the IPL Site Name as configured in the IPL download file.
IPL Host IP Address		This is the IP address of the IPL to query. This should match the IPL IP Address as configured in the IPL download file.
Public Ftp Directory		This is the directory path where users manually ftp files which will be reviewed by the Catalog manager.
IPL 2.5 Catalog Ingest Area		This is the directory path to place files being cataloged for a particular LPA.
IPL Order Status Port	5007	This is the port that IPL will send status messages to after a order request.
IPL 2.5 Account		This is the IPL account Broadsword uses to connect to IPL 2.5.
IPL 2.5 Sybase IP Address		This field specifies the IP Address of the SYBASE server the ipl25_plugin will use to Connect to the IPL2.5 database.
IPL 2.5 Sybase Port	8200	This field specifies the port of the SYBASE server the ipl25_plugin will use to Connect to the ipl2.5 database.
IPL25 Database Name	IPL20db	This field specifies the name of the SYBASE Database the ipl25_plugin will use to Connect to the ipl2.5 database.
IPL 2.5 SQS Sybase Server IP Address		This field specifies the IP Address of the SYBASE SQS server the ipl25_plugin will use to Connect to perform Geographic queries.
IPL 2.5 SQS Sybase Server Port	8400	This field specifies the port of the SYBASE SQS server the ipl25_plugin will use to Connect to perform Geographic queries.
IPL 2.5 Database Login		This field specifies the database login the ipl25_plugin will use to Login to the IPL2.5 database.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IPL 2.5 Password		This is the IPL password Broadsword uses to connect to IPL 2.5.
IPL 2.5 Database Password		This field specifies the database password the ipl25_plugin will use to Login to the IPL2.5 database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Reset Form    Cancel    OK

Figure A-10-Add New IPL25 Source

**Note:** On the IPL server create a Sybase user to have *select only* permissions on the desired LPA database user-defined tables. Since the baseline

system does not supply a Sybase-defined group, it is recommended that one be created for use thereafter.

## Imagery Product Library v3.0 (IPL30)

Configuration Item	Value	Item Description
IPL 3.0 Description	<input type="text" value="IPL 3.0 Source"/>	This field describes the IPL 3.0. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
IPL 3.0 Site Name	<input type="text"/>	This is the site name of the IPL to query. This should be the LPA name configured at the IPL.
IPL Host IP Address	<input type="text"/>	This is the IP address of the IPL to query.
Public Ftp Directory	<input type="text"/>	This is the directory path where users manually ftp files which will be reviewed by the Catalog manager.
IPL 3.0 Catalog Ingest Area	<input type="text"/>	This is the directory path to place files being cataloged for a particular LPA.
IPL 3.0 Account	<input type="text"/>	This is the IPL account Broadsword uses to connect to IPL 3.0.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IPL 3.0 Password	<input type="text"/>	This is the IPL password Broadsword uses to connect to IPL 3.0.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-11-Add New IPL30 Source

Comment:

**Note:** On the IPL server create a Sybase user to have *select only* permissions on the desired LPA database user-defined tables. Since the baseline system does not supply a Sybase-defined group, it is recommended that one be created for use thereafter.

**Note:** The IPL 3.0 site name can be determined by executing the following command: `$BOSWD_HOME/bin/GetIplLpaNames.csh`

# Imagery Exploitation Support System

Configuration Item	Value	Item Description
IESS Description	IESS Source	This field describes the IESS. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Exploitation Database Name	Exploitation	This field describes the name of the IESS Exploitation Database. This is used by the iess_plugin to perform a query.
Exploitation Sybase IP Address		This field describes the IP Address of the Sybase Server which the iess_plugin will use to access the Exploitation database.
Exploitation Sybase Port		This field describes the port of the Sybase Server which the iess_plugin will use to access the Exploitation database.
Imagery_Coverage Database Name	Imagery_Coverage	This field describes the name of the IESS Imagery_Coverage Database. This is used by the iess_plugin to perform a query.
Imagery_Coverage Sybase IP Address		This field describes the Ip Address of the Sybase Server which the iess_plugin will use to access the Imagery_Coverage database.
Imagery_Coverage Sybase Port		This field describes the port of the Sybase Server which the iess_plugin will use to access the Imagery_Coverage database.
IIR Database Name	IIR	This field describes the name of the IESS IIR Database. This is used by the iess_plugin to retrieve IIR and target reports.
IIR Sybase IP Address		This field describes the Ip Address of the Sybase Server which the iess_plugin will use to access the IIR database.
IIR Sybase Port		This field describes the port of the Sybase Server which the iess_plugin will use to access the IIR database.
IESS Sybase Login		This field specifies the database login the iess_plugin will use to Login to the IESS databases.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IESS Database Password		This field specifies the database password the iess_plugin will use to Login to the IESS database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-12-Add New IESS Source

**Note:** The *IESS Sybase Login* must be created on the IESS server. This Sybase login must have access to the *Imagery Coverage*, *Exploitation* and *IIR* databases. In each of these databases, assign this user to the IESS defined *rogrp* group, which is part of the IESS baseline.

In addition, this Sybase login requires execute permission on the following stored procedures in each database:

In the ***Exploitation database:***

- Fac\_s\_11532\_002
- FacilityGeo\_s\_14012\_006
- FacRqmt\_js\_11050\_007
- Ins\_s\_11532\_001
- InstGeo\_s\_14012\_006
- Interim\_Image\_i\_14012\_003
- Interim\_Target\_i\_14012\_008

In the ***Imagery Coverage database:***

- Hoc\_js\_11050\_013
- HocGeo\_s\_14012\_006
- ImageGeo\_s\_14012\_006
- Target\_Qry\_i\_14012\_007

In the ***IIR database:***

- Iir\_s\_11050\_001
- Iir\_s\_11050\_002
- Iir\_s\_11050\_003
- Iir\_s\_11050\_005

# InfoSphere Management System (ISM)

Add New ISM Source		
Configuration Item	Value	Item Description
ISM Description	<input type="text" value="ISM Source"/>	This field describes the ISM. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
ISM URL	<input type="text" value="http://hostname:80"/>	This field describes the URL for the ISM Web Server.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-13- Add New ISM Source

## Intelink-Hydra (INT)

Add New INT Source		
Configuration Item	Value	Item Description
Intelink-Hydra Description	<input type="text" value="Intelink-Hydra Source"/>	This field describes Intelink-Hydra. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Intelink-Hydra URL	<input type="text" value="http://hostname:80"/>	This field describes the URL for the Intelink-Hydra Web Server.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

### A-14-Add New INT Source

**Note:** The SIPRNET Intelink-Hydra URL has changed. As of the date of publication of this document, the URL is <http://search.ismc.sgov.gov>

## Intelink-Meta Search (META)

Add New META Source		
Configuration Item	Value	Item Description
Meta Search Description	<input type="text" value="Meta Search Source"/>	This field describes Meta Search. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Meta Search URL	<input type="text" value="http://hostname:80"/>	This field describes the URL for the Meta Search Web Server.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-15- Add New META Source

## Military Equipment Parametric and Engineering Database (MEPED)

Add New MEPED Source		
Configuration Item	Value	Item Description
Meped Description	<input type="text" value="Meped Source"/>	This field describes Meped. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
Meped URL	<input type="text" value="http://hostname:80"/>	This field describes the URL for the Meped Web Server.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-16-Add New MEPED Source

Modernized Integrated Data Base (MIDB)

Add New MIDB Source		
Configuration Item	Value	Item Description
MIDB Description	MIDB Source	This field describes the MIDB. This will appear in the preferences section of the client.
Query Max Hits	0	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
MIDB Database Name	GMI	This field specifies the name of the database the midb_plugin will query.
MIDB Sybase IP Address		This field specifies the IP Address of the SYBASE server the midb_plugin will use to Connect to the MIDB database.
MIDB Sybase Port	2500	This field specifies the port of the SYBASE server the midb_plugin will use to Connect to the MIDB database.
MIDB Database Login	midbuser	This field specifies the database login the midb_plugin will use to Login to the MIDB database.
Network Security Level	T	This field will determine the security classification of all MIDB reports generated.
Access Permission Override	Don't Override	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
MIDB Database Password		This field specifies the database password the midb_plugin will use to Login to the MIDB database.
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-17-Add New MIDB Source

**Note:** The *MIDB Database Login* needs to be created on the MIDB server. This Sybase user must default to the *GMI database*. Within the *GMI database* assign the user the MIDB specified group *read\_only*, which is part of the baseline system.

## Moving Target Indicator (MTIX)

Configuration Item	Value	Item Description
MTIX Description	MTIX Archival Server	This field describes the MTIX Server system. This will appear in the preferences section of the client.
Server Host IP address		This is the IP Address where the MTIX Server is running
Backend server TCP/IP Port	80006	This is the TCP/IP port where the backend server is running
Backend Server Type	MTIX_TRACK	Specifies specific backend server type (TRACK, MTI, IMAGE, REPORT, NAV, SENSOR_TASK, MISSION)
Scratch Data Path	/tmp	Scratch directory path for Mtx Plugin and Server use
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure A-18-Add New MTIX Source

## Moving Target Indicator Real Time (MTIX\_RT)

Configuration Item	Value	Item Description
MTIX Description	MTIX Realtime streaming	This field describes the MTIX Server system. This will appear in the preferences section of the client.
Server Host IP address		This is the IP Address where the MTIX Server is running
Backend server TCP/IP Port	9002	This is the TCP/IP port where the backend server is running
Backend Server Type	MTIX_RT_TRACK	Specifies specific backend server type (TRACK, MTI)
Backend Message Server Type	STREAM	Specifies specific type of message server supporting communications
Scratch Data Path	/tmp	Scratch directory path for Mtix Plugin and Server use
Access Control:	No Access	This denotes whether to allow no users, only Local users, or All users access to this source.

Reset Form    Cancel    OK

Figure A-19-Add New MITX Real Time Source

This page left intentionally blank