LUMINEX™
MODERN MAINFRAME DATA SOLUTIONS

Mainframe Data Integration SecureTransfer (MDI:ST) POC/Implementation Project Overview and Checklist

MDI:ST is a hardware and software solution. This project checklist provides a high-level overview of the steps required for the physical install of the hardware and the install and configuration of the software. In some cases, the software may be installed on an existing Luminex CGX virtual tape system. If that is the case, the hardware installation steps may be bypassed.

The *MDI Site Planning Guide* provides detailed information about the hardware requirements and installation setup. The Luminex Support team works directly with the project team to prepare the site for the hardware installation. The Support team will provide an Install Planning Workbook, customized for your site, to be used as a project plan and checklist for the hardware/software installation process.

Hardware Components and MDI Platform Software

Please read the *MDI Site Planning Guide* thoroughly. It describes the preparation requirements for the physical install of the hardware/software components. It is also important to determine who will be performing the physical installation of the hardware; your sites Facilities team or the Luminex Support team. The chart below describes tasks that would be assigned to Facilities personnel if they are to perform the hardware install. A Mainframe System Programmer and a Network Administrator are also required team members for this project.

The Luminex Support team provides services for the physical hardware installation and software setup on the MDI Platform. The team will schedule System Assurance meetings to review all hardware requirements and configuration options for the MDI Platform.

The following is an overview checklist of the major tasks:

Task #	Description	Assignment
1	Racking of Equipment	Facilities
2	Connection to Storage (FC/IP)	Facilities
3	IOGEN/Switch Configuration	SYSPROG
4	FICON/ESCON connection	Facilities
5	Device Allocation setup (MTL/Esoteric/SMS Rules)	SYSPROG
6	Network Connection to MDI servers	Facilities
7	IP Assignments for MDI server(s)	Network Admin.
8	MDI:ST, SFTP Host configuration – Login/password/home directories	Network Admin.
9	MDI:ST, firewall rules to allow port 22 (MDI Batch Interface Installation Guide)	Network Admin.

Software Components

The software components for the MDI product family provide for communication over the FICON channel between the mainframe and the MDI Platform (server). The MDI Platform appears as a tape device to the mainframe, allowing for the transfer of mainframe data simply by writing data to MDI owned tape. For communication and data movement over FICON to occur, the batch interface components must be installed on the mainframe. MDI product code is also installed and configured for your site on the MDI Platform (server) by the Luminex Support team.

The *MDI Batch Interface Installation Guide* provides instruction for installing the mainframe components, a LOADLIB module and a PROCLIB member. If your MDI solution includes the Pending Data Queue (PDQ) feature (SecureTransfer (MDI:ST) and Cross Platform Data Sharing (MDI:XPDS), The *MDI Pending Data Queue Installation Guide* is also required reading for installing the PDQ started task on the mainframe. If your MDI product does not include PDQ, you may bypass these steps.

The checklist below describes tasks that would be assigned to Mainframe System Programmer (SYSPROG), a Mainframe Security Administrator, required team members for this project.

1	Install LOADLIB module (MDI Batch Interface Installation Guide)	SYSPROG
2	Install PROCLIB member (MDI Batch Interface Installation Guide)	SYSPROG
3	MDI LUMXPROC RACF Setup (MDI Batch Interface Installation Guide)	Mainframe Security
4	Install LUMXPDQ LOADLIB Module - Requires APF Authorization (MDI Pending Data Queue (PDQ) Installation Guide)	SYSPROG
5	Install LUMXPDQ PROCLIB Module (MDI Pending Data Queue (PDQ) Installation Guide)	SYSPROG
6	Define PDQ PassTicket security definitions (MDI Pending Data Queue (PDQ) Installation Guide)	Mainframe Security
7	Define PDQ Started Task and authority definitions (MDI Pending Data Queue (PDQ) Installation Guide)	Mainframe Security
8	Install PDQ Started Task (MDI Pending Data Queue (PDQ) Installation Guide)	SYSPROG
9	Modify/Create MDI JCL (MDI Batch Interface Installation Guide)	SYSPROG
10	Scratch Tape Management – Install LOADLIB (LSCRUP - SCRATCH LIST UPDATE UTILITY Package)	SYSPROG

Step 1: Install LOADLIB module

The MDI Batch Interface Installation Guide provides instructions for unpacking the mainframe file to your site's system. The file is sent to you via email from the Luminex support team. After the file(s) are uploaded to your site's system, place the load module, LUMXPROC, in the appropriate system library for executing using the LUMXPROC procedure.

Step 2: Install the LUXPROC PROCLIB member

The sample procedure is unpacked along with the LOADLIB module in step 1. Tailor the procedure for your site. See the *MDI Batch Interface Installation Guide* for instructions. Place this procedure in the appropriate system library for executing.

Step 3. SecureTransfer Mainframe Security Setup

The SAF interface is used by all mainframe security products to control what user ID(s) can submit PUT and GET operations at the installation site. The LUMXPROC program verifies that the JOB submitter's user ID has the proper authority to use the specified MDI profile(s).

The MDI Batch Interface Installation Guide describes this setup however, additional information has been added here. First, decide on the profiles to be used, what to name them, and then setup the Facility class profile in your security product.

LUMXPROC Profile Naming

Before creating the RACF Facility class profile rules for the MDI:ST profile(s), one or more profile names need to be determined.

The LUMXPROC procedure calls RACF with the following parameters:

```
RACROUTE REQUEST=AUTH,CLASS='FACILITY',ATTR=READ
```

to check the following entity:

```
LUMXPROC.<mdi-profile-type>.<mdi-direction>.<mdi-profile-name>
```

Where:

- **mdi-profile-type** is a fix value of SFTP.
- **mdi-direction** is either PUT, GET or BOTH.

A PUT operation is described as sending the file from the mainframe to another destination. Defining a security profile for PUT operations allows the installation to control who can execute LUMXPROC to send files from the mainframe to another destination.

A GET operation is described as receiving a file to the mainframe from another source. Defining a security profile for GET operations allows the installation to control who can execute LUMXPROC to receive (pull) files to the mainframe.

BOTH can be used when no specification is required in permitting user IDs to file transfer operations. When BOTH is used, only one security profile is required to be defined to your security system. You don't need to define separate profiles for PUT and GET operations.

- **mdi-profile-name** is a 1 to 10 alpha-numeric character string, unique to your site that you have selected for your installation, such as 'SFTPPUT' or 'SFTPGET', 'SFTP2HOSTA', 'SFTPBOTH' as examples.

The name of the MDI:ST profile is coded in the LUMXPROC JCL. Below are some examples showing where the profile name is coded using differing profile names for PUT, GET or BOTH operations.

JCL Example #1 of specifying the PARM=*'PROFILE=mdi-profile-name'* in the LUMXPROC step of a file transfer execution.

```
//STEPNAME EXEC LUMXPROC,PARM='PROFILE=mdi-profile-name'
```

If the installation site selects **SFTPPUT** as the profile name, the following JCL example shows SFTPPUT as the profile name specified in the job's JCL.

```
//STEP020 EXEC LUMXPROC,PARM='PROFILE=SFTPPUT'
```

Where:

- The "<mdi-profile-name>" is the name that your installation has chosen and is specified in the JCL EXEC statement PARM= parameter.
- The <mdi-direction> for this profile name is PUT. All file transfer executions of LUMXPOC using profile name **SFTPPUT** would be PUT operations only. The installation site permits specific user ID(s) to use this profile for PUT operations.
- The <mdi-profile-class> for this profile name is SFTP, because in this example, we are using SFTP as the mechanism to transfer the data from the MDI Platform to the destination.

JCL Example #2 of specifying the PARM=*'PROFILE=mdi-profile-name'* in the LUMXPROC step of a file transfer execution.

```
//STEPNAME EXEC LUMXPROC,PARM='PROFILE=mdi-profile-name'
```

If the installation site selects **SFTPBOTH** as the profile name, the following JCL example shows SFTPPUT as the profile name specified in the job's JCL.

```
//STEP020 EXEC LUMXPROC,PARM='PROFILE=SFTPBOTH'
```

Where:

- The "<mdi-profile-name>" is the name that your installation has chosen and is specified in the JCL EXEC statement PARM= parameter.
- The <mdi-direction> for this profile name is BOTH. All file transfer executions of LUMXPOC using profile name **SFTPBOTH** can be either PUT or GET operations only. The installation site permits specific user ID(s) to use this profile for both PUT and GET operations.
- The <mdi-profile-class> for this profile name is SFTP, because in this example, we are using SFTP as the mechanism to transfer the data from the MDI Platform to the destination.

MDI:ST Security System Definitions

The SecureTransfer Profile is an object that resides on the MDI Platform, and is customized for the site by the Luminex Support team. Program LUMXPROC communicates with the SecureTransfer Profile on the MDI Platform via commands and control information passed over FICON using the mainframe tape protocol. The LUMXPROC program obtains information from the SecureTransfer Profile which is used to formulate a call to the z/OS System Authorization Facility (SAF) to determine whether the user ID has the proper authority to use the specified SecureTransfer profile. The key is the SecureTransfer Profile name, which is specified in the JCL EXEC statement PARM= parameter. It has these characteristics:

- **mdi-profile-name** is a 1 to 10 alpha-numeric character string that you have selected for your site, such as 'HOST1PUT', 'DEPT2GET', or 'APP3BOTH' as examples. More examples of SecureTransfer Profile names and RACF statements are provided at the end of this section.

The LUMXPROC mainframe program passes the SecureTransfer Profile name to the MDI Platform and obtains the following information pertaining to security:

- **mdi-profile-type** is a fixed name assigned to each MDI product. The mdi-profile-type is the hierarchy that all security profile names are defined under. For SecureTransfer, the fixed name for type is SFTP.
- **mdi-direction** is either PUT, GET or BOTH.
- A PUT operation is described as sending the file from the mainframe to another destination. Defining a security profile for PUT operations allows the site to control who can execute LUMXPROC to send files from the mainframe to another destination.
- A GET operation is described as receiving a file to the mainframe from another source. Defining a security profile for GET operations allows the site to control who can execute LUMXPROC to receive (pull) files to the mainframe.
- BOTH can be used when no specification is required in permitting user IDs to file transfer operations. When BOTH is used, only one security profile is required to be defined to your security system. You don't need to define separate profiles for PUT and GET operations.

These options are specified by the customer and added to the SecureTransfer Profile by the Luminex Support team at Profile creation. After LUMXPROC obtains the Profile information it makes this SAF call:

```
RACROUTE REQUEST=AUTH,CLASS='FACILITY',ATTR=READ
```

And checks the following entity:

```
LUMXPROC.SFTP.<mdi-direction>.<mdi-profile-name>
```

Security Server Definitions

The Security Administrator at your installation needs to define a FACILITY class profile or profiles to your security server and permit user ID(s) to the profile in order to successfully execute LUMXPROC on your system.

The following examples show how to define the security profiles using IBM's RACF security product. If you are using one of Computer Associates (CA) products, Top Secret or ACF2, and your Security Administrator is not able to convert these RACF commands to your product's syntax, you may open a support ticket with CA and they will convert the commands to either Top Secret or ACF2 for you.

Step 1: Gather the following information:

- mdi-direction – PUT, GET or BOTH
- mdi-profile-name – name of the SecureTransfer profile or profiles determined by the installation site
- owner ID – the name of a user or group that owns the SecureTransfer FACILITY class profile(s).
- access-list – a list of users and groups who are authorized to execute the SecureTransfer profile(s)

Step 2: Define the FACILITY class profile to RACF.

Sample statement:

```
RDEFINE FACILITY LUMXPROC.SFTP.mdi-direction.mdi-profile-name OWNER(owner-ID) UACC(NONE)
```

Step 3: After defining the FACILITY class profile, the Security Administrator needs to issue a SETROPTS refresh command to update the in memory RACF list.

Sample statement:

```
SETROPTS RACLIST(FACILITY) REFRESH
```

Step 4: Lastly, permit users or groups to the security profile to enable those users or group members to execute LUMXPROC.

Sample statement:

```
PERMIT LUMXPROC.SFTP.mdi-direction.mdi-profile-name CLASS(FACILITY) ID(access-list) ACCESS(READ)
```

Examples

Note: The SecureTransfer code on the MDI platform enforces SFTP security in addition to the mainframe SAF call. The SAF call (RACROUTE) only validates access to execute the SecureTransfer profile on the mainframe.

Scenario #1:

SecureTransfer Profile PAYDATA is configured to perform the PUT operation and has no hard-coded destination (IP address, server name or DNS name) in the Secure Transfer Profile on the MDI Platform. When the site uses this Profile, they will specify the destination of the PUT operation in the JCL SYSIN data stream. Only the Production Services (group PRODSERV) and certain developers (DEVEL1 and DEVEL2) can use this profile.

RACF Security Definition Examples for Scenario #1:

```
RDEFINE FACILITY LUMXPROC.SFTP.PUT.PAYDATA OWNER(MDIADMIN) UACC(NONE)
SETR RACLIST(FACILITY) REFRESH
PERMIT LUMXPROC.SFTP.PUT.PAYDATA CLASS(FACILITY) ID(PRODSERV) ACCESS(READ)
PERMIT LUMXPROC.SFTP.PUT.PAYDATA CLASS(FACILITY) ID(DEVEL1) ACCESS(READ)
PERMIT LUMXPROC.SFTP.PUT.PAYDATA CLASS(FACILITY) ID(DEVEL2) ACCESS(READ)
```

Scenario # 2:

SecureTransfer Profiles CLOUD1GET and CLOUD1PUT are configured on the MDI Platform to perform GET and PUT operations respectively from and to the corporate data lake. All programmers who are members of group APPDEV can PUT files to the data lake. Analyst that are members of group CLBUSDEV can GET files from it.

RACF Security Definition Examples for Scenario #2:

```
RDEFINE FACILITY LUMXPROC.SFTP.GET.CLOUD1GET OWNER(MDIADMIN) UACC(NONE)
RDEFINE FACILITY LUMXPROC.SFTP.PUT.CLOUD1PUT OWNER(MDIADMIN) UACC(NONE)
SETR RACLIST(FACILITY) REFRESH
PERMIT LUMXPROC.SFTP.GET.CLOUD1GET CLASS(FACILITY) ID(CLBUSDEV) ACCESS(READ)
PERMIT LUMXPROC.SFTP.GET.CLOUD1PUT CLASS(FACILITY) ID(CLBUSDEV APPDEV) ACCESS(READ)
```

Scenario # 3:

Profile FINBOTH was configured to send (PUT) and receive (GET) Finance department data to and from the company EDI server. Only members of the finance department who are in group FINEDI are able to use this profile, as well as batch jobs that are executed via the job scheduler, user ID JOBSCHEDA.

RACF Security Definition Examples for Scenario #3:

```
RDEFINE FACILITY LUMXPROC.SFTP.BOTH.FINBOTH OWNER(MDIADMIN) UACC(NONE)
SETR RACLIST(FACILITY) REFRESH
PERMIT LUMXPROC.SFTP.BOTH.FINBOTH CLASS(FACILITY) ID(FINEDI JOBSCHEDA) ACCESS(READ)
```

Scenario # 4:

A company has implemented SecureTransfer and has decided to restrict usage to scheduled batch jobs that have met rigorous change control requirements and the SecureTransfer administration group. In this example, a single generic profile is all that is required for the enterprise. The SecureTransfer user ID is MDIADMIN and the job scheduler user ID is JOBSCHEDA.
RACF Security Definition Examples for Scenario #4:

```
RDEFINE FACILITY LUMXPROC.** OWNER(MDIADMIN) UACC(NONE)
SETR RACLIST(FACILITY) REFRESH
PERMIT LUMXPROC.** CLASS(FACILITY) ID(MDIADMIN JOBSCHEDA) ACCESS(READ)
```

Step 4 – 8: PDQ Mainframe Setup

These steps are reserved for MDI:ST V2 which is to be announced soon.

Step 9: Creating the MDI:ST JCL

MDI:ST uses JCL on the mainframe to copy the file to the MDI:ST Platform, via virtual tape, and transmit the file to a destination. The *MDI SecureTransfer Profile Specification* guide contains information about how to setup the JCL to transmit a file. JCL examples are provided in this guide.

This guide also contains information about the operational arguments available to be configured in the JCL and control the file transmission processing. These operation arguments include but are not limited to:

- Login user ID and password to sign on to the destination server
- Destination IP address, DNS name or server name
- The type of encryption cipher to be used
- Pre-actions that can be performed on the destination server such as "make directory"
- Post-actions that can be performed after the file transfer such as "list file"

Converting the data from EBCDIC to ASCII or ASCII to EBCDIC with the *oformat* operational argument. More information on converting mainframe data can be found in the *MDI Data Conversion Guide*.

ICEGENER or SYNCGENR (if licensed) should be used in place of IEBGENER for better performance and better use of system resources.

Step 10: LSCRUP

The Scratch List Update Utility or LSCRUP is a package that will be provided to you by the Luminex Support Team member assigned to your site. This package contains a LOAD module and sample JCL. LSCRUP is used to extract a list of scratch VOLSERs from your existing tape management report. A subsequent IEBGENER step them writes that scratch list to the Luminex MDI Platform (server).

Licensing

Product licensing is provided by the Luminex Support team. The team configures the MDI:ST Platform with all of the license keys required for your POC or implementation. POC licenses are generally 30 days in length. If the POC is to be extended, a new license key needs to be configured on the MDI:ST Platform. The MDI:ST platform is an annual license. Three-year licenses are also available. Check with your Luminex Account Representative for license key renewal information.

Support

If support is needed during your POC period, please call 888 LUMINEX or 888-586-4639 within the USA or if you are outside of the USA call +1 (951) 781-4100. Select the Support option #1 and then press 2. Identify yourself as a POC client and indicate the MDI product that you are evaluating.