

L-Soft Sweden AB



Administrator's Manual

LISTSERV[®] Maestro, version 1.2-6



6/8/2004 10:54 AM

This page left intentionally blank

Information in this document is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. L-Soft International, Inc. does not endorse or approve the use of any of the product names or trademarks appearing in this document.

Permission is granted to copy this document, at no charge and in its entirety, provided that the copies are not used for commercial advantage, that the source is cited and that the present copyright notice is included in all copies, so that the recipients of such copies are equally bound to abide by the present conditions. Prior written permission is required for any commercial use of this document, in whole or in part, and for any partial reproduction of the contents of this document exceeding 50 lines of up to 80 characters, or equivalent. The title page, table of contents and index, if any, are not considered to be part of the document for the purposes of this copyright notice, and can be freely removed if present.

Copyright © 2004, L-Soft Sweden AB
All Rights Reserved Worldwide.

L-SOFT, LISTSERV, LSMTP, and ListPlex are registered trademarks of L-Soft international, Inc. LMail is a trademark of L-Soft international, Inc.

CataList and EASE are service marks of L-Soft international, Inc.

The Open Group, Motif, OSF/1 UNIX and the "X" device are registered trademarks of The Open Group in the United State and other countries.

Digital, Alpha AXP, AXP, Digital UNIX, OpenVMS, HP, and HP-UX are trademarks of Hewlett-Packard Company in the United States and other countries.

Microsoft, Windows, Windows 2000, Windows XP, and Windows NT are registered trademarks of Microsoft Corporation in the United States and other countries.

Sun, Solaris, SunOS, and PMDF are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

IRIX is a registered trademark of Silicon Graphics, Inc. in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Intel and Pentium are registered trademarks of Intel Corporation.

All other trademarks, both marked and not marked, are the property of their respective owners.

This product includes software developed by the Apache Software Foundation

(<http://www.apache.org/>).

Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>

This product includes code licensed from RSA Security, Inc.

Manuals for LISTSERV are available in ASCII-text format from LISTSERV and in PDF format from **ftp.lsoft.com**. They are also available on the World Wide Web at the following URL:

URL: <http://www.lsoft.com/manuals/index.html>

L-Soft invites comment on its manuals. Please feel free to send your comments by e-mail to: MANUALS@LSOFT.COM

Contents

Section 1 Introduction to LISTSERV® Maestro Administration	1
1.1 Remote Version Query	2
1.2 System Requirements	2
1.3 Accessing the Hub Administrator Interface	2
1.4 Understanding the Hub Administrator Interface	3
Section 2 Configuring LISTSERV Maestro for First Use	8
Section 3 Changing the Administrator Password	10
Section 4 The System Database	10
4.1 Configuring the External System Database	10
4.2 Preparing the Database	12
4.2.1 General System Database Preparation	13
4.2.2 Preparing SQL Server	13
4.2.3 Preparing Oracle	14
4.2.4 Preparing DB2	14
4.2.5 Preparing MySQL	15
4.3 General Optimization Hints	16
4.4 Disabling and Enabling the Internal Database	16
Section 5 Defining External Database Connections	16
5.1 Installing JDBC Drivers to Connect to External Databases	18
5.2 Registering a Database Plugin	22
Section 6 LISTSERV and LISTSERV Maestro	23
6.1 Preparing LISTSERV to Process Jobs from LISTSERV Maestro	24
6.2 Preparing LISTSERV Maestro to Send DISTRIBUTE Jobs to LISTSERV	25
6.2.1 Specifying the LISTSERV Host with Different Internal and External Names	26
6.2.2 Specifying a Separate LISTSERV Instance for Processing Bounces	27
6.3 Using Existing Lists with LISTSERV Maestro	27
6.3.1 Topics	28
Section 7 Settings for the Maestro User Interface	29
7.1 Application Settings	29
7.2 Application Default Settings	32
7.3 Setting the Default Tracking URL	36
7.3.1 Multiple Tracking URLs	37
Section 8 Administrative Policies	38
8.1 Configuring Backups	39
8.2 Configuring Logging	39
8.3 Runtime Administration and System Shutdown	39
8.4 User Restrictions	41
8.5 Administrative E-mail Notifications	42
8.5.1 Testing E-mail Notifications	43
Section 9 Creating and Administering User Accounts	43
9.1 Creating a New User Account	44
9.2 Editing Account Information and Assigning Single User Settings	45
9.2.1 Editing General User Settings	45
9.2.2 Editing Component Specific Settings for Single and Group Users	46
Section 10 Special Administrative User Account	54
10.1 Archiving Delivered Jobs	54
10.2 Importing an Archived Job	55
10.3 Changing Job and Report Ownership	56
10.4 Changing Sender Profile, Drop-In Content Element, and Recipients Target Group Ownership	59
Section 11 Saving and Restoring a Backup	61
11.1 Configuring the Backup Time	61
11.2 Configuring External Post-Backup Processes	62
11.3 Configuring the Backup Location	63
11.4 Configuring the Backup History	64

11.5 Saving a Backup to an External Medium.....	65
11.6 Identifying the Backup: The Backup ID	65
11.7 Restoring a Backup	65
Section 12 Maestro Logs.....	68
12.1 Remote Log Access.....	68
Section 13 Using Non-Standard Ports	69
13.1 Ports Used by LISTSERV Maestro.....	69
13.1.1 Ports used by the Administration Hub.....	70
13.1.2 Ports used by the Maestro User Interface.....	70
13.1.3 Ports used by Maestro Tracker	70
13.2 Configuring Port Usage	70
13.2.1 Configuring the HTTP Port.....	71
13.2.2 Configuring the Internal Communication Port	73
13.2.3 Configuring the Tracker Communications Port	74
13.2.4 Configuring the Internal System Database Connection Port	74
13.2.5 Configuring the Application Server Shutdown Port.....	74
Section 14 Defining IP Addresses.....	74
Section 15 Installing Behind a Firewall.....	76
Section 16 Restricting Access to Components	78
16.1 IP Address Restrictions	79
16.2 Disallowing Concurrent Access with the Same User Account	81
Section 17 Securing Access With SSL	84
17.1 Introduction to Secure Communication	84
17.2 Which Components Should Be Secured?	87
17.3 Obtaining and Installing a Server Certificate	88
17.3.1 Securing the Trusted Root Certificate Keystore.....	88
17.3.2 Creating an Unsigned Server Certificate.....	89
17.3.3 Performing a Certificate Signing Request (CSR).....	90
17.3.4 Installing the Signed Server Certificate	91
17.3.5 Installing a Trusted Root Certificate	92
17.3.6 Making LISTSERV Maestro Aware of the Server Certificate	93
Section 18 Tracking and Recipient Profiles	95
Section 19 Editing LISTSERV Maestro INI Files.....	98
19.1 Maestro User Interface INI-File Entries	99
19.2 Administration Hub INI-File Entries	103
19.3 Maestro Tracker INI-File Entries.....	103
Section 20 Distributed Components	104
20.1 Fresh Installation with Distributed Components	105
20.2 Moving Components to Another Server	105
20.2.1 Moving the Maestro User Interface Component to Another Server.....	105
20.2.2 Moving the Administration Hub Component to Another Server	107
20.2.3 Moving the Maestro Tracker Component to Another Server	108
20.2.4 Moving the Database External Component to Another Server	109
20.3 Server Name Aliases and Proxies.....	110
20.3.1 Configuring LISTSERV Maestro components with Server Name Aliases or Proxies	112
Section 21 User Interface Branding	113
21.1 Adding Custom Text Strings.....	114
21.2 Exchanging Logo Images	115
Section 22 LISTSERV Maestro in Evaluation Mode.....	116
Section 23 Using International Character Sets	117
23.1 Defining the Default Mail Charset.....	117
23.2 Allowing or Disallowing Bi-Directional Character Sets	118
Section 24 Glossary of Terms	120
Section 25 Appendix A LISTSERV Maestro Standard Default Ports	122

Figures

Figure 1 Administration Hub Home Page	4
Figure 2 Flow Chart of the Administration Hub	5
Figure 3 Global Component Settings	6
Figure 4 Change Administrator Password	10
Figure 5 System Database Connection	11
Figure 6 System Database Connection Details	12
Figure 7 JDBC Driver Layers	21
Figure 8 ODBC Plugin Layers	21
Figure 9 Database Plugins	22
Figure 10 Add New Database Plugin	23
Figure 11 Global Component Settings for Maestro User Interface	29
Figure 12 General Administration of the Maestro User Interface	30
Figure 13 Database Plugins	31
Figure 14 System Database Connection	32
Figure 15 Default LISTSERV Connection	33
Figure 16 Dedicated Bounce Server	34
Figure 17 Default Tracking URL	34
Figure 18 Default Size Limits	35
Figure 19 Default Content Restrictions	35
Figure 20 Default Recipients Restrictions	36
Figure 21 Administer User Accounts	44
Figure 22 Defining User Account	45
Figure 23 Editing Account Information	45
Figure 24 Editing User Settings	46
Figure 25 Single User Settings for a Non-Group Member	46
Figure 26 Single User Settings for a Group Member	46
Figure 27 User Right Settings	48
Figure 28 Default LISTSERV Connection for a Group with Dedicated Bounce Server	49
Figure 29 LISTSERV Connection for a Single User without a Dedicated Bounce Server	50
Figure 30 LISTSERV Connection for a Group User	50
Figure 31 Tracking URL	50
Figure 32 Size Limits	51
Figure 33 Job ID Prefix	51
Figure 34 Drop-In Content Restrictions	52
Figure 35 Recipients Restrictions	53
Figure 36 Special Administrative User Account	54
Figure 37 Job Administration - Job Archive	55
Figure 38 Archived Jobs	56
Figure 39 Change Job Owner	57
Figure 40 Change Report Owner	57
Figure 41 Change Ownership	59
Figure 42 Select Target Group and Item to Change Ownership	60
Figure 43 Change Target Group Owner	60
Figure 44 General Component Settings for Administration Hub	62
Figure 45 XML Entry for Normal HTTP	71
Figure 46 Example of XML File	74
Figure 47 XML Entry for Normal HTTP	75
Figure 48 XML Entry for IP Address	75
Figure 49 Component Communication Pathways	77
Figure 50 Request Interceptor Entry	79
Figure 51 Request Interceptor Example	80
Figure 52 Request Interceptor Example	81
Figure 53 Multiple Logins	81
Figure 54 XML Entry for the Session Timeout	83

Figure 55 Example of Base64 Encoded Outfile	91
Figure 56 Imported Certificate	93
Figure 57 Editing the Server.XML File to Remove the HTTP Connector	94
Figure 58 Editing the Server.XML File to Remove the HTTP Connector	95
Figure 59 Example of Recipients Profile Data Table	97
Figure 60 Example of Recipients ID in Data Table	97
Figure 61 Sample Proxy Setup	110
Figure 62 Browser Window Branding	114
Figure 63 LISTSERV Maestro Header Branding	114
Figure 64 LISTSERV Maestro Footer Branding.....	115
Figure 65 Right Logo Branding	116
Figure 66 Error Screen Logo Branding	116

Tables

Table 1 Navigational Icons.....	3
Table 2 Backup History	64
Table 3 Maestro User Interface INI-File Entries.....	100
Table 4 Administration Hub INI-File Entries.....	103
Table 5 Maestro Tracker INI-File Entries	103
Table 6 Supported Charsets	117

About This Manual

Every effort has been made to ensure that this document is an accurate representation of the functionality of LISTSERV Maestro. As with every software application, development continues after the documentation has gone to press, so small inconsistencies may occur. We would appreciate any feedback on this manual. Send comments by e-mail to:

MANUALS@LSOFT.COM

The following documentation conventions have been used in this manual:

- Quotations from the screen will appear in italics enclosed within quotation marks.
- Clickable buttons will appear in bold.
- Clickable links will appear in bold.
- Directory names, commands, and examples of editing program files will appear in Courier New font.
- Emphasized words or phrases will be underlined.
- Some screen captures have been cropped for emphasis or descriptive purposes.



This symbol denotes an important note or warning.



This symbol denotes optional advice to save time.

Section 1 Introduction to LISTSERV® Maestro Administration

Designed specifically to work with LISTSERV 1.8e (or later) and LSMTP 1.1b (or later), LISTSERV Maestro allows users to easily create and send personalized e-mail messages using a Web interface. Incorporated into this powerful tool is a tracking component that can collect data every time a recipient opens an e-mail message or clicks on a URL contained within the message.

The LISTSERV Maestro program is comprised of three components that work together:

- **The Administration Hub** – Controls all user and program settings. It is the central component that stores registry and account information. It is accessed both by the Maestro User Interface and by Maestro Tracker to validate login information. It has its own administrator user interface.
- **The Maestro User Interface** – The actual user interface. Individuals and groups use it to create and distribute customized e-mail messages. It is also used to access, view, and download the collected tracking data.
- **The Maestro Tracker** – Receives and compiles tracking data from delivered e-mail messages.

In addition to LISTSERV Maestro's three components, LISTSERV Maestro also relies on the existence of two other external components:

- An installation of **LISTSERV® 1.8e** (or later).
- An installation of **LSMTP® 1.1b** (or later).

These two components must be configured to work together.

For Linux installations of LISTSERV Maestro, it is necessary to connect to a separate database so that the application can store its own system data and retrieve recipient data for mailings. For Windows installations, LISTSERV Maestro comes with its own internal database for storing systems data. However, it is highly recommended that LISTSERV Maestro be connected to an external database installation for high-end production because the internal database is limited in size.

LISTSERV Maestro can use the external database to store its own systems data as well as to select recipient lists from database tables and drop-in content elements. LISTSERV Maestro can connect to several databases in this way. Supported databases are:

- Oracle® 8i, Oracle® 9i and compatible versions
- DB2® V7.2 and compatible versions
- MySQL™ 3.23.42 and compatible versions
- SQL® Server 7.0 and 2000

The three LISTSERV Maestro components, the two external components, and the optional (for Windows installations) database may be installed on any combination of hosts, from one single host shared by all components to six dedicated hosts, one for each component. If different

components are installed on separate servers, it is not necessary that all of the servers have the same operating system. It is possible to install the Maestro User Interface and Administration Hub components on a Windows server and at the same time the Maestro Tracker component on a Linux server (or other combinations). For more information on host restrictions, installing LISTSERV Maestro, and starting and stopping the LISTSERV Maestro service, see the LISTSERV Maestro Installation Manual.

1.1 Remote Version Query

The current version and build number of all components can be queried remotely. This is done with a simple HTTP-request - a URL typed into the address field of any browser. The result of the query will be displayed in the browser. This query can also be used to verify that a fresh installation is operational.

- To query LUI: `http://LUISEVER/lui/build`
- To query HUB: `http://HUBSERVER/hub/build`
- To query TRK: `http://TRKSERVER/trk/build`

1.2 System Requirements

Depending on the operating system of the client used for the access, the following browsers are supported when accessing the Maestro User Interface or Administration Hub:

- Client with Windows – Microsoft Internet Explorer 5.5 or later, Netscape 7.0 or later and *Mozilla 1.0.0* or later.
- Client with Linux – Netscape 7.0 or later and Mozilla 1.0.0 or later.

To access the Maestro User Interface or the Administration Hub, we strongly recommend that only Windows or Linux be used with the browsers and browser versions listed. Other operating systems, browsers, or browser versions are not supported.

The client does not necessarily have to have the same operating system as the LISTSERV Maestro server. A Linux client can be used to access LISTSERV Maestro on a Windows server and vice versa. Similarly, the different components of LISTSERV Maestro may run on different operating systems, if they are installed on separate servers. For example, the Maestro User Interface and Administration Hub components may be installed on a Windows server, while the Maestro Tracker is installed on a Linux server.

It is important to note that recipients of e-mail being tracked by LISTSERV Maestro may use whatever browser they wish to access the URLs contained in the message. Tracking will occur no matter which browser is used by e-mail recipients.

1.3 Accessing the Hub Administrator Interface

Once the program has been installed, set your compatible browser to:

`http://Your_LISTSERV_Host/hub`. Enter a password to log in and access the program. The default administrator password after a fresh installation is “admin”.



In a Windows installation, a shortcut for this address will appear in the Windows Start Menu under “Programs → L-Soft Application Server”.

1.4 Understanding the Hub Administrator Interface

Administering LISTSERV Maestro involves many different tasks and interaction with more than just the Administration Hub (HUB). Administrators will have to understand how LISTSERV Maestro is situated within the institution’s infrastructure. This understanding is critical for making decisions about settings for all the application’s components to ensure consistency and compatibility with new or existing systems. Consequently, this manual is organized around those different tasks an administrator needs to perform in order to set up, monitor, backup, and change an installation of LISTSERV Maestro. It also serves as a reference for advanced systems configuration, touching on the HUB interface screens as they fit in to each task.

This section of the manual contains a brief overview of the HUB interface. Navigation and functional icons are outlined. References to other sections of the manual containing greater detail, and step-by-step procedures are provided.

The opening screen of LISTSERV Maestro’s Administrator interface contains various sets of functional and navigational icons. At the top right corner of the screen there are two small icons, **log out** and **help**. There are additional navigational icons on other pages within the application.

Table 1 Navigational Icons



Home – Brings the user back to the first screen, the LISTSERV Maestro home page.



Log out – Ends the LISTSERV Maestro session and closes the account.



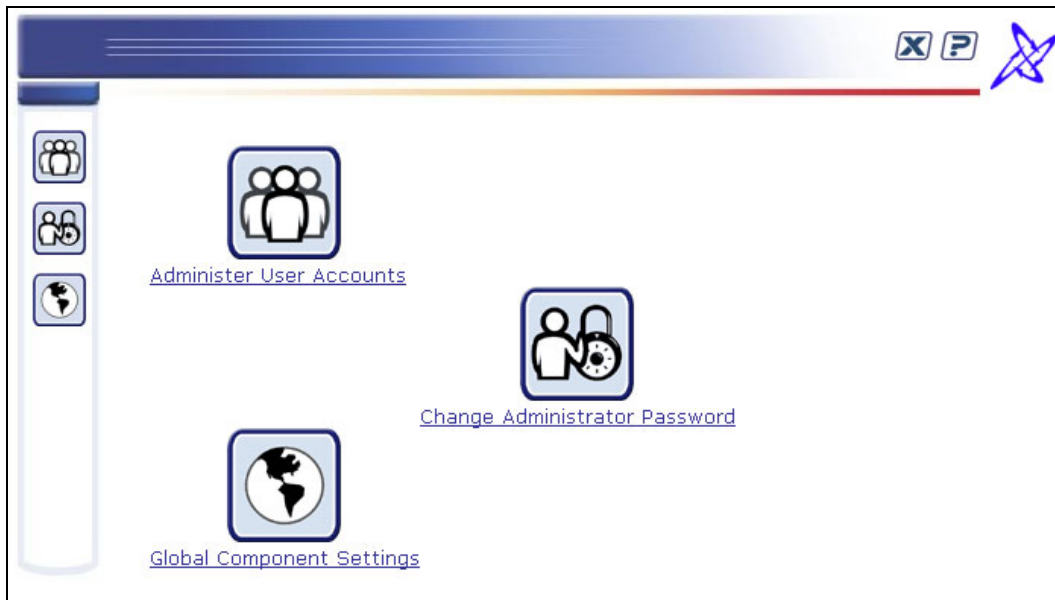
Up One Level – Brings the user up one level in the program, not necessarily back to the previous page.



Help – Provides access to page specific online help.

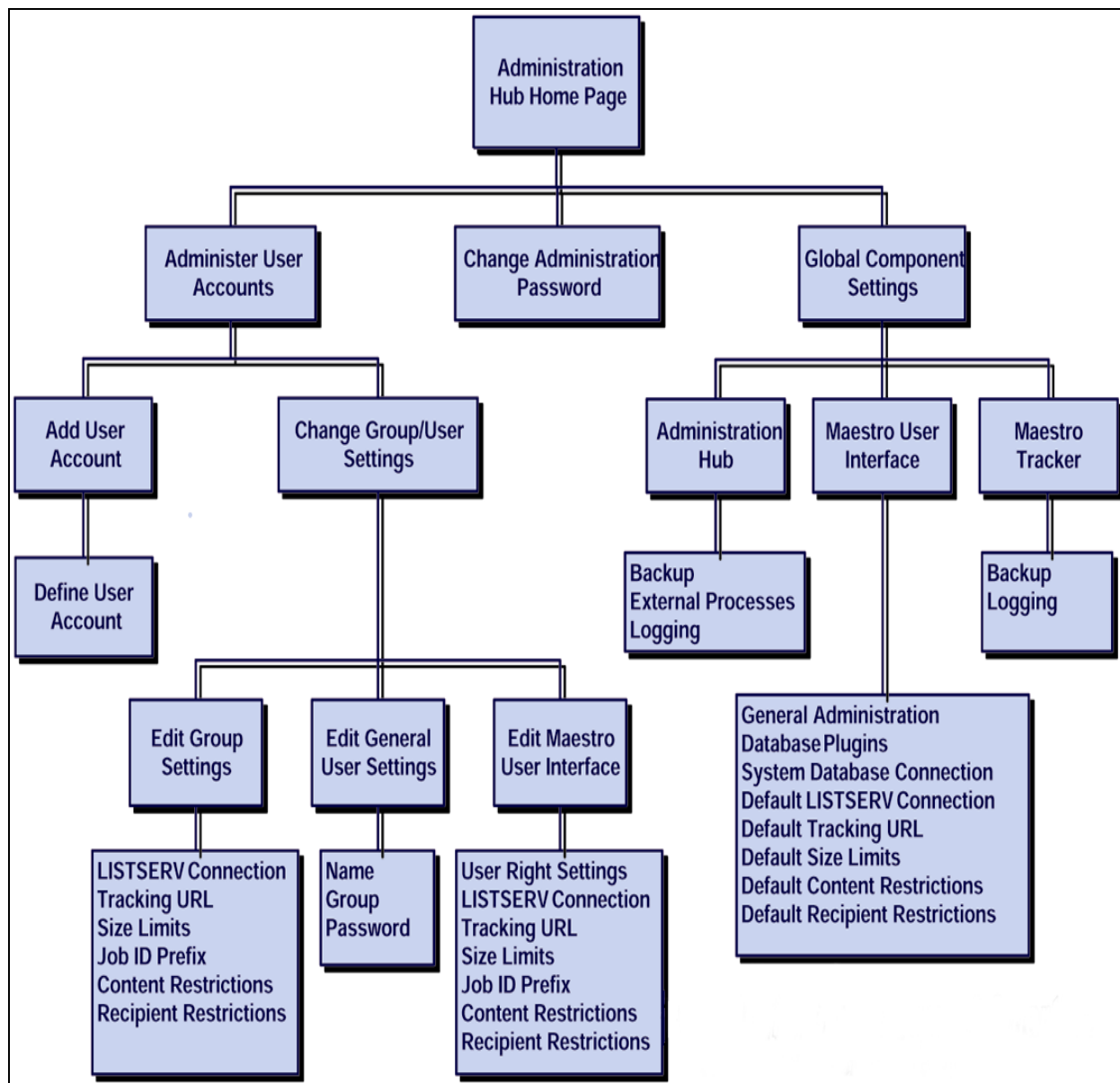
The center of the screen contains large icons that represent the major functions of the Administration Hub. These icons are also repeated along the left side of most screens within the program allowing for easy access from other parts of the administration interface.

Figure 1 Administration Hub Home Page



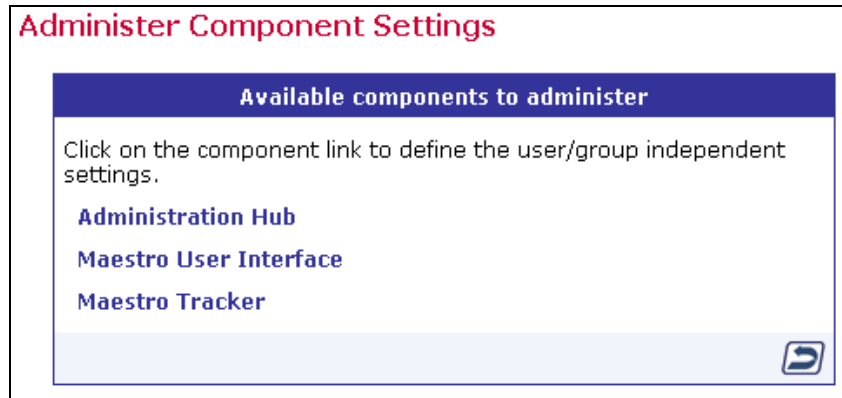
- **Administer User Accounts** – Leads to the section of the application that allows the administrator to add new user accounts and groups, change user and group settings, and delete users and groups. User and group administration is documented in Section 9 [Creating and Administering User Accounts](#).
- **Change Administrator Password** – Leads to the section of the application that allows the password used to log into the HUB and the special administrative user account to be changed. Changing the password is documented in Section 3 [Changing the Administration Password](#). The special administrative user account is documented in Section 10 [Special Administrative User Account](#).
- **Global Components Settings** – Leads to the sections of the application that control the settings for each of the three components, the Administration Hub (HUB), the Maestro User Interface (LUI), and the Maestro Tracker (TRK).

Figure 2 Flow Chart of the Administration Hub



Global component settings control the three components of LISTERV Maestro. Clicking on the **Global Component Settings** icon from the Home page opens a screen that is split into three main areas.

Figure 3 Global Component Settings



- **Administration Hub** – Contains the settings for management of the HUB component.
 - Configure backup parameters for the HUB component, including:
 - Setting the time for the daily backup.
 - Naming the backup folder.
 - Setting the number of previous backup copies to be kept.
 - Configuring any external processes to be run after backup.Backup procedures are documented in Section 11 [Saving and Restoring a Backup](#).
 - Configure logging:
 - Setting the level of severity for logged messages to be written during HUB operation.
 - Logs are discussed in Section 8.2 [Configuring Logging](#) and Section 12 [Maestro Logs](#).
 - Configure Administrative E-mail Notifications:
 - Send or do not send e-mail notification in the event of a system problem.
 - Send or do not send e-mail notification for each system startup.
 - Assign an SMTP Host, SMTP Port, and sender address for notification e-mail messages.
 - Assign e-mail addresses to receive notifications.

-
- **Maestro User Interface** – Contains the settings for management of the LUI component. Settings entered here become the default settings for the system. Default settings can be overridden at the group and user levels. For more information on group and user levels, see Section 9 [Creating and Administering User Accounts](#).
 - Configure General Settings for the LUI component, including:
 - Naming the backup folder.
 - Setting the number of previous backup copies to be kept. Backup procedures are documented in Section 11 [Saving and Restoring a Backup](#).
 - Setting the event transfer interval from Maestro Tracker.
 - Naming the job archive folder.
 - Setting the level of severity for logged messages to be written during LUI operation. Logs are discussed in Section 8.2 [Configuring Logging](#) and Section 12 [Maestro Logs](#)
 - Configuring Runtime Administration for restricting multiple logins, disabling sending, and locking the user interface. These settings are documented in Section 8.3 [Runtime Administration and System Shutdown](#)
 - Register Database Plugins:
 - Adding a database plugin. Registering a database plugins is described in Section 5.2 [Registering a Database Plugin](#).
 - Deleting an existing plugin.
 - Configure the System Database Connection, including:
 - Setting the maximum number of buffered connections.
 - Defining the system database as described in Section 4 [The System Database](#).
 - Define Default LISTSERV Connection:
 - Setting the LISTSERV Host.
 - Setting the LISTSERV TCPGUI Port.
 - Entering the LISTSERV Client Address.
 - Entering the LISTSERV Password. More information on LISTSERV settings is documented in Section 7 [Settings for the Maestro User Interface](#)
 - Setting up a dedicated bounce server.
 - Define the Default Tracking URL:
 - Entering the name of the Tracker Host.
 - Setting the HTTP Port. The default tracking URL is documented in Section 7.2 [Setting the Default Tracker URL](#)
 - Set Default Size Limits:
 - Setting the maximum size for a message.
 - Setting the maximum size for a file upload. For more information on size limits, see Section 7 [Settings for the Maestro User Interface](#)
 - Define Default Content Restrictions:
 - Allowing or disallowing the use of AOL Rich Text formatting for the alternative part of an HTML message. For more information on AOL Rich Text, see Section 5.3.2 AOL Alternative Text for HTML Messages in the LISTSERV Maestro User's Manual.
 - Entering folders and/or URLs that the users are permitting to access for drop-in content elements. For more information on permitted folders and URLs see [Section 7 Settings for the Maestro User Interface](#) or the online help.

-
- Define Recipients Restrictions:
Enabling, disabling, or hiding standard and advanced recipients types.
Entering folder name(s) that users are permitted to access for uploading "just-in-time" recipients lists. For more information see [Section 7 Settings for the Maestro User Interface](#)
 - **Maestro Tracker** – Contains the settings for management of the TRK component.
 - Configure backup settings:
Setting the name of the backup folder.
Setting the number of previous backups to be kept. Backup procedures are documented in Section 11 [Saving and Restoring a Backup](#).
 - Configure the Communications Port. The ports used by Maestro Tracker are described in Section 13.1.3 [Ports used by Maestro Tracker](#).
 - Configure logging:
Setting the level of severity for logged messages to be written during TRK operation. Logs are discussed in Section 8.2 [Configuring Logging](#) and Section 12 [Maestro Logs](#)

Section 2 Configuring LISTSERV Maestro for First Use

After installation, it is necessary to execute a few initial configuration steps in the Administration Hub before LISTSERV Maestro can be fully used. Access the Administration Hub as described in Section 1.3 [Accessing the Hub Administrator Interface](#) and log in with the administrator password. Execute at least the following configuration steps for security and access purposes:

1. **Change Administrator Password** – For security purposes, change the administrator password to something other than the default “admin” immediately after installation. Do not forget the new password, it is not recoverable. See Section 3 [Changing the Administrator Password](#) for more information.
2. **Configure the System Database** – The Maestro User Interface component of LISTSERV Maestro uses a “system database” to store its working data – recipient profiles, job ID numbers, tracking information, and so on.

In the case of a Windows installation of LISTSERV Maestro, an “internal” database (based on MySQL) is included as part of the application and may be used as the system database. Using this internal database will allow the application to run “out-of-the-box” for evaluation purposes or very light usage. However, this internal database is not recommended for high-end production because the table space is limited to 300 MB, and it has not been optimized for large data volumes. Switching the system database from internal to external and vice versa can be done at a later time, if necessary.

In the case of a Linux installation, an external database must be configured to store this system information before the application can be run.

For more information on configuring an external database, see Section 4 [The System Database](#).

3. **Define User Database Connections** – The Maestro User Interface may optionally access “user databases” to retrieve information to build recipients lists in the recipients wizard or target groups wizard, or to create drop-in content elements.

If a user database is going to be used, LISTSERV Maestro must be configured to access it. The appropriate driver must be installed on the server running the Maestro User Interface (the LUI component) and the appropriate “plugin” must be registered in the Administration Hub (the HUB component). For more information on configuring an external database, see Section 5 [Defining External Database Connections](#).

4. **Set up LISTSERV** – See Section 6 [LISTSERV and LISTSERV Maestro](#) for details on how to set up LISTSERV to work with LISTSERV Maestro.
5. **Configure the Maestro User Interface (LUI)** – Two steps in particular need to be accomplished:
 - A. **Define the default LISTSERV Connection** – This connection is used for all accounts that do not have individual connection parameters configured. If a single LISTSERV connection is shared among all users, configure this connection as the default connection and leave the configuration parameters of individual users (or groups) empty. Leave the default connection parameters empty only if connection parameters for all users and groups on the account or group level will be configured individually.


See Section 7 [Settings for the Maestro User Interface](#) for more information on configuring the LISTSERV default connection.
 - B. **Define the tracking URLs** – If tracking is to be used, it is necessary to define the domain name of the tracking server that will be used in the URLs for tracked links. Leave the default tracking URL parameter empty only if this parameter will be defined individually for all groups. See Section 7.2 [Setting the Default Tracking URL](#) for information on how to define the default tracking URLs.
6. **Configure Global Component Settings** – Establish administrative policies and procedures and configure global component settings to reflect these. In particular decide upon:
 - A. **Backup procedures** – What time to make daily backups, how many backups to keep, whether any external processes will run before or after a backup, where the backup(s) will be saved.
 - B. **Archival procedures** – Decide the circumstances under which old jobs will be archived. Define the archive folder.
 - C. **Level of error and/or event logging** – What types of events will the system log – all events, all errors, or only serious errors.
 - D. **Taking the system down** – When will the system be taken down for maintenance, how will users be warned, what restrictions will be imposed before the system is taken down.
 - E. **User account restrictions** – What, if any, restrictions will be imposed on user accounts based upon the type(s) of user, size limits of uploads, recipients types, drop-in content types, and so on.
 - F. **Tracker event transfer frequency** – Decide how often the tracking information needs to be refreshed. This depends on how current the tracking reports need to be. The default time period is 10 minutes.
7. **Create User Accounts** – Create at least one user account that can be used to access the Maestro User Interface. See Section 9 [Creating and Administering User Accounts](#) for more details on how to proceed with creating user accounts.

-
8. **Secure the Default Keystore** – If any of the LISTSERV Maestro components are going to be secured using SSL (Secure Socket Layer) Change the password for default keystore for trusted root certificates that is shipped with Java. The instructions for this procedure are located in Section 17.3.1 [Securing the Trusted Root Certificate Keystore](#).

Section 3 Changing the Administrator Password

To change the administrator password, click the icon on the Administration Hub home page. Enter the old password in the top field and a new password in the field beneath. Confirm the new password by retyping it in the third field. Click the **Save** button to record the changes or the **Cancel** button to disregard.

Figure 4 Change Administrator Password



The default password after a fresh installation of LISTSERV Maestro is “admin”.

Section 4 The System Database

LISTSERV Maestro uses a “system” database to store its working data – recipient profiles, job ID numbers, tracking information, and so on.

In the case of a Windows installation of LISTSERV Maestro, an “internal” database (based on MySQL) is included as part of the application and may be used as the system database. Using this internal database will allow the application to run “out-of-the-box” for evaluation purposes and very light usage. However, this internal database is not recommended for high-end production because the table space is limited to 300 MB, and it has not been optimized for large data volumes.

In the case of a Linux installation, an external database must be configured to store this system information before the application can be run.

4.1 Configuring the External System Database

In order to use an external database as the system database, the database must be prepared for use with LISTSERV Maestro, and LISTSERV Maestro must be configured to use the prepared database.

When switching from the internal system database to an external database (even before first use) or when switching between two external databases, the application needs to transfer all data from the old database to the new database. To accomplish this, both databases must be running and accessible to LISTSERV Maestro during the transfer.

Follow these steps to configure an external database:

1. If changing the system database for an installation that has been in use, make a backup before making any changes so that the current data may be recovered in case of errors. See Section 11 [Saving and Restoring a Backup](#) for more information.
2. Install the DBMS and prepare the database to be used. Follow the manufacturer's instructions to install the DBMS. See Section 4.2 [Preparing the Database](#) for details on how to create and prepare the system database. Some instructions are different depending on the DBMS in use.
3. Install the corresponding DBMS driver on the server where the Maestro User Interface (LUI) is installed. See Section 5.1 [Installing JDBC Drivers to Connect to External Databases](#) for details.
4. Register the appropriate "Plugin" in the Administration Hub (HUB) component. See Section 5.2 [Registering a Database Plugin](#) for more information.
5. Define the System Database Connection:
 - A. Log into the Administration Hub. Click Global Component Settings. Next, click Maestro User Interface, and then click System Database Connection.

Figure 5 System Database Connection

System Database Connection

Maestro System Database Connection

On this page you define the settings of the System Database that the Maestro User Interface uses to store its internal system data in.

Maximum number of buffered connections:

Use the internal database as the System Database

The following external database is used as the System Database:

Database Plugin:

(Note: Changes in this category require a restart of the Maestro User Interface to take effect.)

- B. Select the option button "The following external database is used as the System Database:"
- C. Select the "Database Plugin" from the drop-down menu.
- D. Fill out the "Connection Details" in the edit boxes that appear below. These details may be different for each type of database selected.
- E. Click **OK** to submit the change.

Figure 6 System Database Connection Details

System Database Connection

Maestro System Database Connection

On this page you define the settings of the System Database that the Maestro User Interface uses to store its internal system data in.

Maximum number of buffered connections:

Use the internal database as the System Database

The following external database is used as the System Database:

Database Plugin:

Connection Details

Database Name:

DB2 Server User Name:

Password:

(Note: Changes in this category require a restart of the Maestro User Interface to take effect.)

This database is for exclusive use by LISTSERV Maestro and prepared according to Section 4.2

The database account must have rights described in Section 4.2

6. Shut down LISTSERV Maestro and then restart.
7. Wait for the transfer of data between the two databases to be completed. Check the LUI logs to verify the successful completion of the transfer before proceeding to the next step. Logs are documented in Section 12 [Maestro Logs](#).
8. If desired, delete the old LISTSERV Maestro database from the original database application. If the default internal database for a Windows installation was previously being used, it can be disabled to save system resources. See Section 4.4 [Disabling and Enabling the Internal Database](#) for further instructions.

Under normal operation, it should never be necessary to revert from an external system database to the internal system database. However, if the need ever arises follow these steps to restore the internal system database:

If the internal database was disabled, re-enable it. See Section 4.4 [Disabling and Enabling the Internal Database](#) for further instructions.

In the “System Database Connection” screen, select the option button for “Use the internal database as the System Database”.

Shut down LISTSERV Maestro and then restart.

Wait for the transfer of data to complete before deleting the external database.

4.2 Preparing the Database

Before the Maestro User Interface can be used together with a freshly installed external database, the database must be prepared in certain ways. Outlined below are explanations of the required preparation steps, followed by details specific to each of the supported database management systems.

4.2.1 General System Database Preparation

LISTSERV Maestro must have its own database, separate from any other databases. The database may use the same database server as another database, but must not interact with the other databases on that server. Even if a database is created for storing recipient information for LISTSERV Maestro or for storing LISTSERV lists, it should be a separate database. LISTSERV Maestro can be given access to these recipient databases separately (see Section 5 [Defining External Database Connections](#)).

A user account must be created within the database server for LISTSERV Maestro to access the system database. This user will then be selected from the Maestro User Interface to connect to the database. Certain privileges are required for the user account, as described in the DBMS-specific sections below.

The database that is used as storage for the Maestro User Interface should be configured in a way that it allows dynamic growth because the data stored by the Maestro User Interface grows over time. The growth rate corresponds to the number and the size of the e-mail jobs that are delivered. Large e-mail jobs with a high volume of collected tracking events will use more database storage space than smaller e-mail jobs.

Some examples of upper limits that might need to be adjusted for large volume environments are:

- **User space quota** – Most databases limit the amount of space that a given user may store in the database. This limit should be set to "unlimited" or a sufficiently large value.
- **Database or tablespace size** – Many database vendors, especially those supporting larger database environments, support the sub-division of the database server in smaller areas, sometimes called "tablespaces" or a similar term (see the database documentation for details). Normally, each database account is assigned to one of these areas, which is then referred to as "default tablespace" or "standard tablespace". This part of the database should be configured in a way that it allows dynamic growth, if possible. **Note:** It is possible to use the Maestro User Interface with a database that does not support this type of dynamic growth. To do so, an administrator should make it part of the daily or weekly routine to check the amount of space available for the Maestro User Interface.
- **File system size** – Like other server applications storing persistent data on the file system, the database storing the Maestro User Interface data must reside on a server whose file system is monitored on a regular basis, either through automated system administration tools or by an administrator who regularly checks the system.



Important: Deleting or archiving old jobs from LISTSERV Maestro on a regular basis will prevent the database from becoming unnecessarily slow.

4.2.2 Preparing SQL Server

In the SQL Server management console, create a new database for sole use by the Maestro User Interface. Please see the SQL Server documentation for details about how to create, configure, and optimize a database.

Once a new database has been created, create a user account that the Maestro User Interface can use to connect to the database. Create a new user with any desired name and give it the `db_public` role for the created or selected database. Next, in the “Permissions” of the database’s “Properties”, grant the `Create Table` privilege to this user.

4.2.3 Preparing Oracle

A new Oracle database for sole use by the Maestro User Interface must be created so that it uses `UTF-8` as its database character set. The database character set `UTF-8` is **required** and the Maestro User Interface will not work with a database that has a different character set. (See the Oracle documentation for details).

Use an Oracle administration tool (such as SQL*Plus), to create a new user. This new user must have the `CREATE SESSION` and the `CREATE TABLE` privilege and a sufficiently large table space quota in the user's default table space.

The Maestro User Interface does not require unusually large rollback segments. If duplicate elimination is performed for large e-mail jobs, larger temporary segments are needed as duplicate elimination is performed with a database sorting operation. See the Oracle documentation for more details on how to configure and optimize databases.

The “maximum key length” value is a feature specific to Oracle. This value is an internal value inherent to each Oracle installation. It is determined mainly by the block size used by the database but may also be influenced by other factors, like the operating system.

For LISTSERV Maestro to be able to create its database table in an optimal manner, it needs to know the maximum key length value used by the Oracle database that is used as the system database. LISTSERV Maestro cannot query the database for this value. The administrator has to determine the maximum key length value used internally by the Oracle database installation and input the correct value.

If the value entered exceeds the actual maximum key length used by the database, runtime errors could result, and LISTSERV Maestro will not work correctly. If a value that is smaller than the actual value is entered, LISTSERV Maestro will tailor its database tables accordingly in order to meet this smaller value. As a result, the database tables will be created with a sub-optimal structure and the user may run into database column size limitations, which would be avoidable, if the correct maximum key length value had been supplied.

Oracle documentation concerning which maximum key length value is used under which circumstances is sparse. A commonly used “rule-of-thumb” value is that with a block size of **4K**, the maximum key length is **1578**. With a block size of **8K**, the maximum key length is double the value of 4K, or **3156**. Generally, the maximum key length seems to be about 38% - 40% of the block size. If in doubt, please consult the Oracle documentation or contact Oracle support.

4.2.4 Preparing DB2

Use the DB2 Control Center application to create a new database and define `UTF-8` as the database code set.

Configure the database with at least one user table space and one system temporary table space with a page size of 32K each. It may also be necessary to create a buffer pool with a

page size of 32K before the table spaces with 32K page size can be created. Next, create a new database user for sole use by the Maestro User Interface. This user must be configured to use a table space with 32K page size; otherwise the Maestro User Interface will not work. The new user needs the `Create Table` privilege.

Having prepared the DB2 database, the next step is to create a database alias on the server that is running the Maestro User Interface component (this is most likely not the server where the database itself is installed). Do this by starting the IBM DB2 Client Configuration Assistant on the server where the Maestro User Interface component is running. This is a runtime client database tool that comes with the IBM DB2 installation and needs to be installed on the Maestro User Interface component server.

In the Client Configuration Assistant, click the **Add** button to create a new alias. Select the "Search the network" option and continue with the wizard. For more details on IBM DB2 database administration and the definition of database aliases, see the IBM DB2 documentation. Note that the name of this alias is the value for the "Database name" parameter of the IBM DB2 database plugin that comes with the Maestro User Interface.

4.2.5 Preparing MySQL

To use the Maestro User Interface with MySQL, set up MySQL to use the "InnoDB Tables" table type (see the MySQL manual for more details). This table type supports transactions, and the Maestro User Interface requires a table type that supports transactions.

Set up MySQL with InnoDB data files and log files of sufficient size to accommodate the planned usage of the Maestro User Interface. After the MySQL database server is set up to use the InnoDB table type, create a new database specifically for use with the Maestro User Interface. Create a user to use with LISTSERV Maestro.

To connect to the database, start the MySQL client program, `mysql.exe`, from the `bin` folder of the MySQL binary installation. To create a new database, enter the following command in the MySQL client: `create database NAME;` where "NAME" is replaced with the name of the database. Grant privileges by entering the following grant command for the username: `grant all on DBNAME.* to NAME@HOST identified by 'PASSWORD';` where the uppercase values are replaced as follows:

- `DBNAME`: The name of the database to be used with the Maestro User Interface (usually the same name used in the "create database" command, see above).
- `NAME`: The user name of the user to be created and granted privileges.
- `HOST`: The host name of the server where the Maestro User Interface is running that will access this database.
- `PASSWORD`: The password associated with the user name.

Using "grant all" as described above grants all privileges on the given database to the given user. This is usually acceptable if the particular database was created specifically for use with the Maestro User Interface. However, if there is concern about granting the full set of privileges to the user, use the following privilege list instead of "all":

```
select, insert, update, delete, index, create, drop
```

4.3 General Optimization Hints

The following general information about how the Maestro User Interface uses the database can help optimize the database installation for use with the Maestro User Interface.

- The Maestro User Interface does not use large transactions. Any transactions that are opened are then closed after a maximum of a few hundred inserts or updates.
- During normal usage, the Maestro User Interface behaves with OLTP (online transaction processing) characteristics. There is a constant switch between read and write on the database. However, if there are many reports running on the collected tracking data, the characteristics of the Maestro User Interface's behavior shift more and more into OLAP (online analytical processing), where the amount of (complex) reads outnumbers the amount of writes.

Use this information to optimize the database after analyzing the usage of the Maestro User Interface to determine if it is working more with OLTP or OLAP characteristics.

4.4 Disabling and Enabling the Internal Database

If the Maestro User Interface is set up to use an external database as the system database for a Windows installation of LISTSERV Maestro, there is no longer a need to keep the internal database running. To reduce the resource usage of LISTSERV Maestro, disable the internal database after configuring the Maestro User Interface to use an external database.

To disable the internal database, execute the following command:

```
\Program Files\L-Soft\Application Server\commands\DisableInternalDB.cmd
```

This will stop the internal MySQL database if it is currently running and will disable it, so that it will not be started again if LISTSERV Maestro is restarted. Also, the Windows service in which the internal database was run is uninstalled. It is no longer possible to select the option button *“Use the internal database as the System Database”* on the *“System Database Connection”* screen of the Maestro User Interface. See Figure 4. If this choice is selected by mistake, and LISTSERV Maestro is restarted, the Maestro User Interface component will not start, as it will not be able to find the now disabled instance of the internal database. If, at a later point, the internal database is desired, it must be re-enabled with this command:

```
\Program Files\L-Soft\Application Server\commands\EnableInternalDB.cmd
```

This will re-enable the internal database and install the necessary Windows service. The next time LISTSERV Maestro is restarted, the internal database will also be restarted, and can then be used.

Section 5 Defining External Database Connections

The Maestro User Interface component of LISTSERV® Maestro uses a “system database” to store its working data, outlined in Section 4 [The System Database](#). For production environments, the system database should be configured to use an external database.

The Maestro User Interface can also be configured to access an external “user database” to retrieve existing information to build recipients lists in the recipients wizard or target groups wizard, or to create drop-in content elements.

Multiple databases managed by the same or different DBMS software can be configured as user databases so that recipient data and drop-in content elements can be accessed from many sources. The user database(s) may be on the same database server as the system database, or on different ones. By configuring LISTSERV Maestro to be able to access different databases, institutional data can be retrieved from different sources, allowing for great flexibility.

The following databases have been tested and are compatible with LISTSERV Maestro:

- Microsoft® SQL Server 7.0 and 2000
- Oracle® 8i Enterprise/Standard Edition Release 3 (8.1.7)
- Oracle® 9i Release 2 (9.2.0.3) & (9.2.0.1)
- DB2® Universal Database V7.2
- MySQL™ 3.23.42
- Any ODBC compliant database can be used for read-only purposes to retrieve recipients lists and drop-in content elements.

LISTSERV Maestro communicates with external databases with so called “*Plugins*” and drivers. If an external database is going to be used for the system database or the user database, the appropriate driver must be installed and the plugin must be configured first.

Before an external database can be invoked, either as the system database in the HUB System Database Connection screen, or as a user database in the LUI Recipient Definition, Target Group Definition, or Drop-in Definition screens, LISTSERV Maestro must know how to access the particular DBMS software managing the database in question.

The following steps need to be taken once for each DBMS package, which will make all databases running under that software available:

1. Install the driver for the database on the server where the Maestro User Interface (LUI) is installed. See Section 5.1 [Installing JDBC Drivers to Connect to External Databases](#) for details.
2. Register the appropriate “*Plugin*” in the Administration Hub (HUB) component. See Section 5.2 [Registering a Database Plugin](#) for more information.



Important: Connection details for user databases are defined in the recipients target groups wizard, or the recipients wizard in the Maestro User Interface during the recipient definition of a job. Do not enter connection details in the HUB for user databases. Connection details are entered in the HUB only for the system database. After a restart, any database connection details entered in the Global Components Settings will change the system database.

5.1 Installing JDBC Drivers to Connect to External Databases

The Maestro User Interface is a Java server application that uses JDBC to connect to the configured database. Therefore, it is usually necessary to install a compatible JDBC driver for the database. Each database plugin (see Section 5.2 [Registering a Database Plugin](#) for more information) has been developed to use exactly one JDBC driver. There may be several plugins for the same DBMS, each of which uses a different driver to access that DBMS. The specific plugin to be used depends on the DBMS and the JDBC driver available for that DBMS.



Important: After installing a new JDBC driver into LISTSERV Maestro (see descriptions below), it is necessary to restart LISTSERV Maestro to make it aware of the new driver.

The plugins available at the time this document was written support five different drivers for four different databases as well as the ODBC-driver (as a read-only plugin only) that in turn allows access to any database or other data source that has an ODBC driver available.

- **L-Soft MySQL JDBC-driver** – For connection to the MySQL database 3.23.42 or later. This driver is installed together with LISTSERV Maestro and pre-registered. No special installation is necessary to access this driver or its plugin.
- **IBM JDBC-driver for DB2 V7.2** – To use this driver, first install the DB2 run-time clients (from the runtime folder of the DB2 installation package) on the server where the Maestro User Interface is running. Use the client to connect to a database on the DB2 server (see Section 4.2.4 [Preparing DB2](#)). It is important to install the client on the Maestro User Interface server and not on the server where the database is installed (except of course, if both components happen to be on the same server). Next, copy the file “db2java.zip” from the run-time client installation to the LISTSERV Maestro installation (shown for a default installation):

Copy the file “db2java.zip” from the “java” folder in the DB2 run-time client installation

```
\Program Files\IBM\SQLLIB\java
```

into the “lib” folder in the LISTSERV Maestro installation

```
\Program Files\L-Soft\Application Server\lib
```

Run the batch command file “usejdbc2.bat” from the “java12” subfolder in the DB2 run-time client installation, i.e. execute the file:

```
\Program Files\IBM\SQLLIB\java12\usejdbc2.bat
```

This script prepares the DB2 runtime environment for JDK1.2 and later, which is required for a fully functional LISTSERV Maestro installation.

Note: The batch command file creates a different version of the JDBC driver file with the name “db2java.zip”. Make sure to use the newly created file when proceeding to the next step.

Where to find the driver: The run-time clients (which in turn include the JDBC-driver file as described above) are included in the installation package for DB2 when a license is

purchased. At the time this document was written, a 60-day trial version of the database (including the JDBC-driver) was available at IBM's website. A valid license for the DB2 database must be purchased from IBM before using its driver or using it together with the Maestro User Interface.

- **Oracle 8i Thin Driver** – This driver comes in the form of a file called “classes12.zip”. Simply copy this file into the “lib” folder in the LISTSERV Maestro installation

`\Program Files\L-Soft\Application Server\lib`

Where to find the driver: The driver can be downloaded from the Oracle Technology Network: <http://otn.oracle.com/>

Go to the “Downloads” page and find the section titled “Technologies, Utilities, and Drivers”. You will have to establish an account and accept a license agreement before you can actually download anything from this site. Click the “Oracle JDBC Drivers” link. From this page, select the link to download the “Oracle8i Release 2 (8.1.7)”. Click on the `classes12.zip` link located under the “For use with JDK 1.2” heading to begin the download. This description mirrors the structure of the OTN-Web site at the time this document was written. The location of the pages and the names of the links may have changed. A valid license for the Oracle database must be purchased from Oracle before using its driver or using it together with the Maestro User Interface.

- **Oracle 9i Thin Driver** – (Works with Oracle 8i and Oracle 9i databases) This driver comes in form of a file called “ojdbc14.jar”. Simply copy this file into the “lib” folder in the LISTSERV Maestro installation

`\Program Files\L-Soft\Application Server\lib`

Where to find the driver: The driver can be downloaded from the Oracle Technology Network: <http://otn.oracle.com/>

Go to the “Downloads” page and find the section titled “Technologies, Utilities, and Drivers”. Click the “Oracle JDBC Drivers” link. Then follow the link to download the “Oracle9i Release 2 (9.2.0.3) & (9.2.0.1)”. After accepting the license agreement, and establishing an account, click on the “ojdbc14.jar” link in the section “for use with JDK 1.4”. This should trigger the download of the “ojdbc14.jar” file. This description mirrors the structure of the OTN-website at the time this document was written. The location of the pages and the names of the links may have changed since then.) A valid license for the Oracle database must be purchased from Oracle before using its driver or using it together with the Maestro User Interface.

- **Microsoft SQL Server 2000 JDBC-driver** – Install the driver on any desired computer. It is not important that the driver be installed on the same computer as the Maestro User Interface, but it is important that the following files are copied from the installation folder of the driver to the installation folder of LISTSERV Maestro (shown for a default installation):

Copy the files “msbase.jar”, “mssqlserver.jar” and “msutil.jar” from the “lib” folder in the SQL Server JDBC-driver installation

`\Program Files\Microsoft SQL Server 2000 driver for JDBC\lib`

into the “lib” folder in the LISTSERV Maestro installation

`\Program Files\L-Soft\Application Server\lib`

This driver is published by Microsoft as a driver for SQL Server 2000 only. It will probably not work with SQL Server 7.0. L-Soft has not tested it with SQL Server 7.0 and recommends using it only with SQL Server 2000.

Where to find the driver: At the time this document was written, the driver was available for download from this URL at Microsoft's Web site:

<http://msdn.microsoft.com/library/default.asp?url=/downloads/list/sqlserver.asp>

In case this URL is no longer valid, try the MS SQL Server site, and look for the downloads section: <http://www.microsoft.com/sql/>

A valid license for the SQL Server database must be purchased from Microsoft before using it together with the Maestro User Interface.

- **I-net SPRINTA JDBC-driver for MS SQL Server 7.0/2000** – From the SPRINTA download/installation, copy the file "Sprinta2000.jar" into the "lib" folder in the LISTSERV Maestro installation

`\Program Files\L-Soft\Application Server\lib`

Where to find the driver: The driver can be purchased from I-net software:

<http://www.inetsoftware.de/>

At the time this document was written, the SPRINTA driver home page could be found at the following location:

<http://www.inetsoftware.de/English/Produkte/JDBC2/Default.htm>

The evaluation version of this driver, which is (or was at the time this document was written) available for download, may contain a limitation of the number of concurrent database connections that will make the Maestro User Interface fail during operation. The evaluation version is, therefore, not supported for use with the Maestro User Interface.

While the SPRINTA driver also supports MS SQL Server 6.5, the Maestro User Interface does not. The Maestro User Interface requires MS SQL Server 7.0 or later.

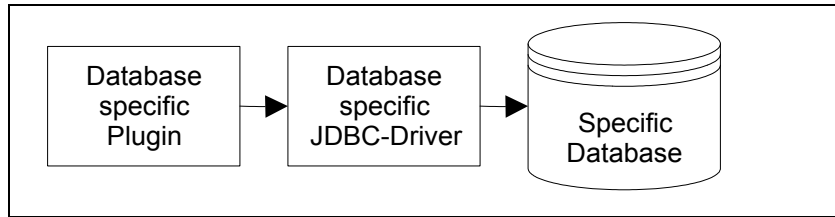
A valid license for the SQL Server database must be purchased from Microsoft before using it together with the Maestro User Interface. Also, a valid license for the SPRINTA driver must be purchased from I-net software before using this driver to access SQL Server.

- **The ODBC Driver** – The ODBC-driver plugin is a read-only plugin. As such, it can only be used to access recipient data or drop-in content data. It cannot be used for the system database connection. After registering this plugin it will not appear in the list of available drivers on the system connection page in the Administration Hub. However, it will appear in the corresponding lists of the recipient wizard, target group wizard, and database drop-in page.

This driver is automatically installed together with LISTSERV Maestro, so the only step required to make this plugin available for usage is to register it as described in Section 5.2 [Registering a Database Plugin](#).

The ODBC driver plugin operates differently when compared to the other database plugins. The other plugins bind a specific JDBC driver to LISTSERV Maestro, allowing access to the specific database for which the JDBC driver has been written. Database access then goes through three layers, from the plugin into the JDBC driver and from there into the database as shown in Figure 7 below.

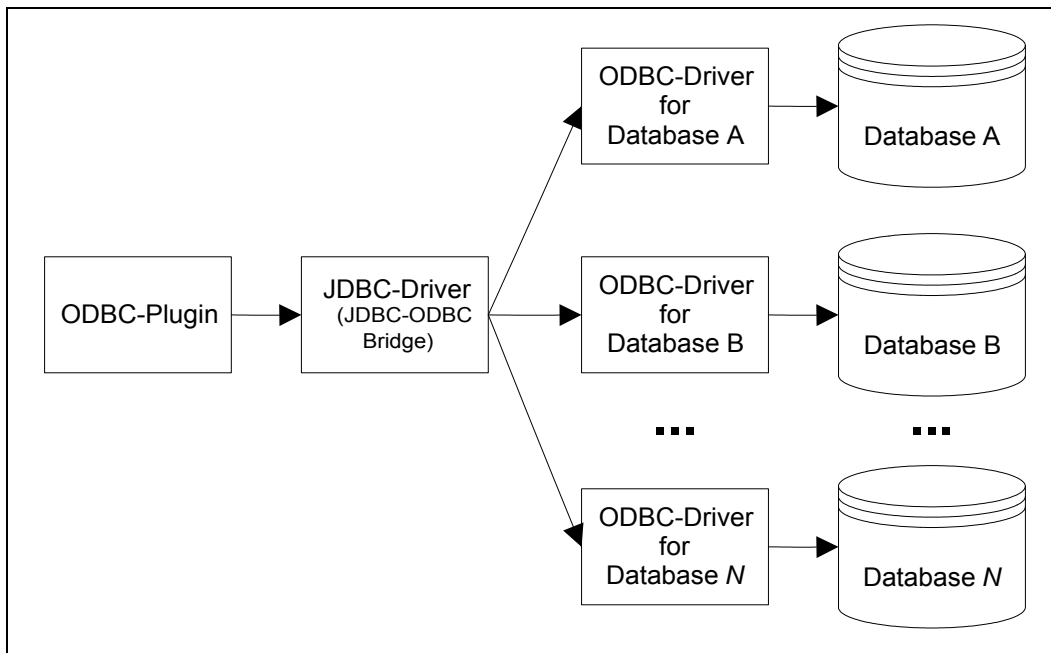
Figure 7 JDBC Driver Layers



In contrast, the ODBC driver plugin has one more layer shown in Figure 7. This plugin binds the JDBC-ODBC bridge driver to LISTSERV Maestro, allowing access to any ODBC driver. The plugin by itself does not define which database is accessible through it. It does however, define that anything that has an ODBC driver available to it is accessible. The ODBC driver for the database in question must also be supplied in addition to the plugin. Installation of the ODBC driver depends on the system and the OS in use. Please see the appropriate documentation for the ODBC driver and the operating system.

Database access goes through four layers starting with the ODBC plugin to the JDBC-ODBC bridge, to the ODBC driver, and ending with the database.

Figure 8 ODBC Plugin Layers



The performance of LISTSERV Maestro when using this driver is directly dependant on the ODBC driver used for the database in question. Accessing a database through an ODBC driver that is programmed inefficiently will impact the performance of LISTSERV

Maestro. For example, if the ODBC driver uses up a lot of memory when doing large selects, LISTSERV Maestro may be subjected to a memory shortage caused by the ODBC driver. In that case, the driver is not usable unless it can be used to make smaller selects, or the server's memory is upgraded accordingly.



Important: Exhaustive testing with the ODBC driver(s) before employing in a production setting is recommended to determine the impact on memory and CPU usage.



The term “database”, when used with ODBC, is interpreted quite broadly. ODBC drivers for data sources like plain text files or for Microsoft Excel files exist, turning them into “databases” in the sense that they can be used to create recipients lists and drop-in content.

5.2 Registering a Database Plugin

LISTSERV Maestro uses “database plugins” to give access to different JDBC drivers (and through them to different databases) available to the Maestro User Interface. Before a plugin can be used, it must first be registered in the list of known plugins. Some plugins are already pre-registered when LISTSERV Maestro is installed, while others need to be registered after the corresponding JDBC driver has been installed.

To register a new plugin, log into the Administration Hub and click the **Global Component Settings** link, then the **Maestro User Interface** link and finally the **Database Plugins** link. Click on **Register New Database Plugin**. In the text box, enter the full class name of the plugin to be registered.

Figure 9 Database Plugins

Database Plugins

The list below shows all registered database plugins.

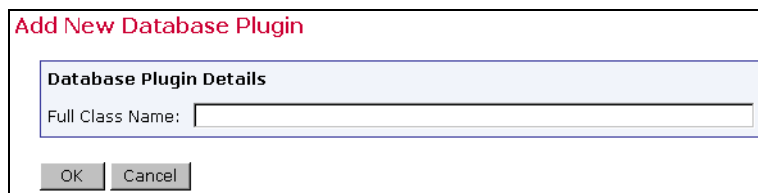
Click on the "unregister" link to unregister it.
Use the "Register New Database Plugin" button to register a new plugin.

[Register New Database Plugin](#)

Plugin Name	Full Class Name
MySQL Driver Database Plugin	com.lsoft.lui.db.mysql.MySQLDriverPlugin Unregister

-
- For the L-Soft MySQL driver plugin:
`com.lsoft.lui.db.mysql.MySQLDriverPlugin`
 - For the IBM DB2 V7.2 driver plugin:
`com.lsoft.lui.db.ibm.DB2V72DriverPlugin`
 - For the Oracle 8i thin driver plugin:
`com.lsoft.lui.db.oracle.Oracle8iThinDriverPlugin`
 - For the Oracle 9i thin driver plugin:
`com.lsoft.lui.db.oracle.Oracle8iThinDriverPlugin`
 - For the Microsoft SQL Server 2000 driver plugin:
`com.lsoft.lui.db.sqlserver.MSSQLDriverPlugin`
 - For the I-net SPRINTA driver for MS SQL Server 7.0/2000 plugin:
`com.lsoft.lui.db.sqlserver.SPRINTADriverPlugin`
 - For the read-only ODBC plugin:
`com.lsoft.lui.db.odbc.ODBCDriverPlugin`

Figure 10 Add New Database Plugin



Click **OK** to submit the class name. If the plugin was registered correctly, it will now appear in the list of plugins. If there was a problem during the registration, an error message describing the problem will appear. The most probable causes for problems are misspellings of the class name (which is case sensitive).

Section 6 LISTSERV and LISTSERV Maestro

LISTSERV Maestro uses an instance of LISTSERV to send e-mail jobs that are prepared in the Maestro User Interface. Any instance of LISTSERV, or multiple instances of LISTSERV, can be used to send jobs as long as each instance has a LISTSERV Maestro license, is reachable over the network, has been configured to accept jobs from LISTSERV Maestro, and LISTSERV Maestro has been configured to connect to it. A hierarchy of LISTSERV Connection settings can be used to configure a global application default connection, a default connection for each group, a separate sender address for group users, and a default connection for each single user not in a group. For more information on configuring individual and group user settings, see [Section 9.2.2 Editing Component Specific Settings for Single and Group Users](#)

The system works by having the Maestro User Interface send a “distribute job” to LISTSERV. A DISTRIBUTE job is a series of commands to LISTSERV that essentially says, “Take this message and send it to these recipients.” In order to successfully process a DISTRIBUTE job, LISTSERV needs to have a list of recipients (e-mail addresses), and the message itself. A complete DISTRIBUTE job must include one or more command lines giving instructions to LISTSERV and an authenticating password. LISTSERV Maestro handles these and many other steps automatically.

Normally, LISTSERV does not accept "distribute" commands from everyone. LISTSERV accepts this command only if the "distribute job" is sent from an account (e-mail address) that is configured in LISTSERV to have the right to DISTRIBUTE jobs. The reason for this is to avoid allowing LISTSERV to be hijacked for spamming and other unethical purposes.

6.1 Preparing LISTSERV to Process Jobs from LISTSERV Maestro

In order to process e-mail jobs from LISTSERV Maestro, LISTSERV needs to be prepared in certain ways. LISTSERV needs to have an e-mail address and password configured to have the right to DISTRIBUTE. (This e-mail address and password will later be entered in to the Administration Hub, see Section 7 [Settings for the Maestro User Interface](#).) In order to do this, it is necessary to have access to LISTSERV's Site Configuration file. The LISTSERV Site Administrator will have the necessary access.

Prepare LISTSERV for processing e-mail jobs from LISTSERV Maestro as follows:

1. In LISTSERV, configure an e-mail address to have the DISTRIBUTE right. The e-mail address must be defined in LISTSERV's Site Configuration file under either of the following parameters:
 - DIST_ALLOWED_USERS: this parameter confers only the right to send distribute jobs and is the recommended one to use.
 - POSTMASTER: this parameter confers full LISTSERV site administration rights to the e-mail address, which includes the right to send distribute jobs. Thus, it is possible to use the e-mail address and password of one of the LISTSERV site administrators, but L-Soft recommends setting up a special address for Maestro instead.

In LISTSERV, configure a password for this e-mail address. There are two ways to do this:

- Send an e-mail message to LISTSERV from that e-mail address with the command "PW REP *newpassword*" where *newpassword* represents the desired password. LISTSERV will send a confirmation message. That confirmation message must be replied to with another message saying "OK" or by visiting the URL provided in the confirmation message.
- Send an e-mail to LISTSERV from the site administrator's address (one defined as "POSTMASTER" in the Site Configuration file), containing the command "PWC ADD *email newpassword PW=createpw*" where *email* is the e-mail address being used for the LISTSERV Maestro jobs, *newpassword* is the password being assigned to that e-mail address, and *createpw* is the password defined in the Site Configuration file as the "CREATEPW".

As a result of configuring LISTSERV with these steps, an e-mail address with its own password now exists that has the right to send DISTRIBUTE jobs. This address and associated password are necessary for LISTSERV to accept a DISTRIBUTE job from LISTSERV Maestro. The configured address, referred to as the "sender" address, is the sender of the DISTRIBUTE job. It is not necessarily (and mostly likely not) the same e-mail address that is used in the Maestro User Interface for the sender definition step of creating a job.

It is possible to have more than one address and password within the LISTSERV instance configured with the DISTRIBUTE right. Follow the steps above to add additional addresses if

desired. Multiple addresses with the DISTRIBUTE right will allow for individual accounts within a group to have individual sender addresses or for distinct groups to use the same LISTSERV instance without sharing other privileges (for example sharing the rights to send to the same LISTSERV lists).

6.2 Preparing LISTSERV Maestro to Send DISTRIBUTE Jobs to LISTSERV

After LISTSERV has been configured with an e-mail address and password with the DISTRIBUTE right, this information needs to be entered into LISTSERV Maestro's Administration Hub, along with the name of the LISTSERV Host, the Host Name for Return Path/List Addresses, and the TCPGUI port if it is different than the default 2306.

The LISTSERV connection can be set at several levels. The widest level of setting is the Global Component Setting, which defines the global default LISTSERV connection on the application level (see Section 7 [Settings for the Maestro User Interface](#)). These settings will be used as defaults for all accounts that do not have individual settings for group or user level. The address and password configured in LISTSERV are entered using the e-mail address as the "*LISTSERV Client Address*" and the password as the "*LISTSERV Client Password*".

The next level is the default setting for a group (see Figure 26). The group default LISTSERV connection may connect to a different instance of LISTSERV, or may use a different client address and password than the global default. To set the LISTSERV settings for an entire group in the user list, click on the group name (appears only if the account belongs to a group, see Figure 19). If defined on the group level, the group settings will override the global default settings for that group. The settings will apply to all accounts in the group, except for the settings "*LISTSERV Client Address*" and "*LISTSERV Client Password*". These two settings may be configured individually for each account in the group, provided LISTSERV is configured with additional addresses with the DISTRIBUTE right. Accounts in the group for which they are not configured will use the group's settings as the default.

Individual accounts are the last level of settings for the LISTSERV Connection. Individual accounts can belong to a group (group user) or not belong to a group (single user). Settings for individual accounts will override default group and global settings. To set the LISTSERV connection for an individual account, click on the user name from the user list. The screen that opens is different depending on whether the account is a group user or a single user.

Single user accounts can use a separate LISTSERV instance and would therefore need to have all LISTSERV connection settings defined (see Figure 27). Or, single user accounts may use a different client address and password than the global default. Group user accounts can only define the settings for "*LISTSERV Client Address*" and "*LISTSERV Client Password*" (see Figure 28). These individual group settings result in a different LISTSERV e-mail address for each user so that jobs can be identified by owner in the LISTSERV logs.

Properly specifying the LISTSERV host name settings, found on the "*LISTSERV Connection*" screens, is another important aspect to preparing LISTSERV Maestro to process DISTRIBUTE jobs from LISTSERV. This is important for three reasons:

- **LISTSERV Maestro to LISTSERV system communication** – LISTSERV Maestro communicates with LISTSERV using the TCPGUI port. For this reason, LISTSERV Maestro needs to know the name of the server where LISTSERV is running.

-
- **Host Name For Return Path** – When e-mail is sent out over the Internet, the “return path”, which allows undeliverable messages to be returned to the sender, (also known as the RFC 821 `Mail From:` address) must include a known external name, otherwise the bounced mail cannot be returned and LISTSERV Maestro cannot automatically process and report on bounces.
 - **Host Name For List Addresses** – When doing mailings that are based on a normal LISTSERV list, the address of the list in use must include a known external name of the server hosting the LISTSERV instance for list communication to function correctly (something like `listname@hostname`).

Often, a server is only given a single host name by which it can be reached from other computers, including both internal intranet computers and external computers on the Internet. In this case, enter that name into the “*LISTSERV Host*” field of the LISTSERV Connection screen (see Figure 13). Select “*Use LISTSERV host name as given above*” from the pull-down menu beside “*Host name for Return Path/List Addresses*”.

When the LISTSERV server is given several different names (or appears to have several names) a different set up is required. These situations often stem from optimizing a high performance installation of LISTSERV Maestro. In this case, follow the instructions in Section 6.2.1 [Specifying a LISTSERV Host Name with Different Internal and External Names](#).

For very high volumes, it may be desirable to have a separate LISTSERV installation solely for the purpose of processing bounces. In that case, follow the instructions in Section 6.2.2 [Specifying a Separate LISTSERV Instance for Processing Bounces](#)

6.2.1 Specifying the LISTSERV Host with Different Internal and External Names

A common optimizing set up is to have LISTSERV on one server inside a firewall with only an internal name, and LSMTP on another server outside the firewall with an external name. With this set up, LISTSERV, installed on the server with the internally known name, is visible by this name to inside users. For all outside purposes, such as the return path and list e-mail addresses, LISTSERV “appears” to actually be running on the LSMTP server with the external name. This is because LSMTP is connected to the actual LISTSERV instance on the internal server. When viewed remotely, LISTSERV appears to have two host names: one internally known and one externally known.

To enter a separate external host name, select “*Use special external LISTSERV host name specified below:*” from the pull down menu. An edit box will appear. Enter the host name in the edit box (see Figure 14).

Use the following rules for entering information on the LISTSERV Connection screen:

- For the internal communication, (the “*LISTSERV Host*” field) always specify a host name that points to the server where LISTSERV is actually running, not to the instance where LISTSERV only “appears” to be running, when in reality it is LSMTP running on that server. Also, the LISTSERV Maestro server must be able to resolve that host name to the actual IP address of that server.

-
- For the “*Host Name for Return Path/List Addresses*” field, always specify the host name of LISTSERV as seen by outside clients (the Internet), even if that name is actually only an alias for the host or if it points to a server where only the LSMTP instance is running.



Important: The “*Host Name for Return Path/List Addresses*” field is labeled (and used) differently depending on the current selection:

- When specifying the standard LISTSERV connection settings and not using a dedicated bounce server:
The field is labeled “*Host Name for Return Path/List Addresses*” and the host name entered is used both to assemble the sender address for the return path and the LISTSERV list e-mail addresses.
- When specifying the standard LISTSERV connection settings but are also using a dedicated bounce server:
The field is labeled “*Host Name for List Addresses*” and the host name entered is used only to assemble the LISTSERV list e-mail addresses.
- When specifying the LISTSERV connection settings for a dedicated bounce server:
The field is labeled “*Host Name for Return Path*” and the host name entered is used only to assemble the sender address for the return path.

6.2.2 Specifying a Separate LISTSERV Instance for Processing Bounces

For very large volume installations of LISTSERV Maestro a separate instance of LISTSERV can be used just to process bounces. By selecting the option button on the LISTSERV Connection screen labeled “*Use dedicated server (settings to be supplied when this option is selected)*” more settings for this LISTSERV instance will appear (see Figure 14).

If the dedicated bounce processing host has only a single name, enter that name into the “*LISTSERV Host*” field of the LISTSERV Connection screen (see Figure 14). Select “*Use LISTSERV host name as given above*” from the pull-down menu beside “*Host name for Return Path*”. Fill in the other appropriate information, the TCPGUI port, LISTSERV client address and password following the same rules outlined in Section 6.2 [Preparing LISTSERV Maestro to Send DISTRIBUTE Jobs to LISTSERV](#).

If the dedicated bounce processing host has more than one name (or appears to) select “*Use special external LISTSERV host name specified below:*” from the pull down menu. An edit box will appear. Enter the host name in the edit box (see Figure 14).

6.3 Using Existing Lists with LISTSERV Maestro

LISTSERV Maestro can provide access to existing LISTSERV lists, presenting a drop-down menu of available lists on the Source page of the recipients definition wizard when “*Send to an Existing LISTSERV List*” is selected on the Options page. In order to do this, follow these instructions:

For each list to be added to the drop-down menu, insert a line in the list header containing the keyword `Owner=` . Add the e-mail address that was configured with the DISTRIBUTE right (LISTSERV client address) to the right side of the “=” sign. This can be accomplished using the List Configuration Wizard in LISTSERV’s Web Interface.

For example, in the sample list header below, the lines highlighted in gray have been added. The address to the right of the "=" sign is the address that has the DISTRIBUTE right in the LISTSERV instance where this list is located. The line before that sets this owner to "quiet" meaning that no mail will ever be sent to take address, in case that address does not resolve into a real mailbox, but only exists to allow DISTRIBUTE jobs through LISTSERV Maestro:

Women's Club

```
Notify= Yes
Editor= user@mycompany.com
Owner=someone@mycompany.com
Owner=quiet:
Owner= maestro@companyserver.name.com
Moderator= All
Sizelim= 1M
Subscription= By Owner
Subscription= Confirm
Ack= Yes
Confidential= Yes
Validate= No
Reply-to= Sender, Respect
Send= Private
Errors-To= Owner
Owner= user@mycompany.com, Quiet:, user@worldnet.att.net
Notebook= Yes, E:\LISTS\WOMENS_CLUB, Weekly, Private
```

For institutions that have many lists, it is likely that different people will need to have access to different lists. If this is the case, people that work on the same list or sets of lists will have to be placed in the same group. The group can have its own default LISTSERV connection and/or LISTSERV client address and password. If different addresses are assigned to individuals in a group (multiple LISTSERV client addresses) then all those addresses must appear in the list headers as `Owner=.`

6.3.1 Topics

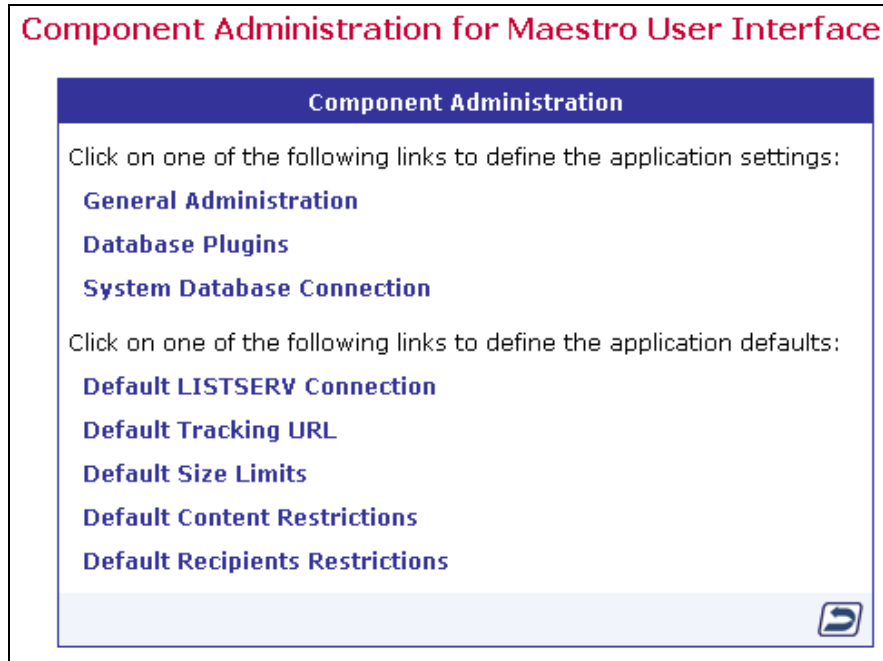
Large active LISTSERV lists often use "sub-groups" within the list to give subscribers the opportunity to receive only the posts to the list they are most interested in. Sub-groups are created in LISTSERV by defining the keyword `Topics` in the list header. Lists can have up to 23 topics defined in the header. List subscribers can elect to receive only those messages that fit into the topic(s) they are interested in reading. Similarly, list members can post their messages to only those topics their messages are relevant to. For example, a large list could have the general subject of Antique Autos. Topics could be defined by time period, by make and model of auto, or by geographic area.

LISTSERV Maestro can take advantage of defined topics in a list to send mail to a specific topic or topics so that subscribers will only receive the message if they are subscribed to that topic(s). Topics are only supported for mail that is sent as "*standard list messages to list members*" in the recipients wizard. For more information on Topics, see the 1.2 Maestro User's Manual.

Section 7 Settings for the Maestro User Interface

To select settings for the Maestro User Interface, click on the Global Component Setting icon from the home page of the Administration User Interface. Next, click on the **Maestro User Interface** link.

Figure 11 Global Component Settings for Maestro User Interface



The top three selections define application settings, and the bottom five selections define application defaults. Click on a link to define or edit the settings.

7.1 Application Settings

Application settings are general settings that affect the LISTSERV Maestro globally. They can be changed by the Administrator.

General Administration – Defines general Maestro User Interface settings.

Figure 12 General Administration of the Maestro User Interface

General Administration of Maestro User Interface

General Settings

Backup folder:
(Leave empty for default: "backup".)

Number of previous backups to keep:

Event transfer interval (from Maestro Tracker): min.

Job archive folder:
(Leave empty for default: "archive".)

Log Level

Only log severe messages.

Log severe and standard operational messages.

Log all messages.

Runtime Administration

Multiple Logins: Disallow multiple logins with the same user account.

Outbox: Sending is disabled.

Login Access: LISTSERV Maestro User Interface is locked.

Message that will be shown instead of login page while login is locked:

Message that will be shown at top of each page while login is locked:

Outbox: Sending is disabled.

Login Access: LISTSERV Maestro User Interface is locked.

Message that will be shown instead of login page while login is locked:

Message that will be shown at top of each page while login is locked:

OK Cancel

- **Backup folder** – Defines the folder where the daily backup of the Maestro User Interface will be written. If left empty, the default backup folder will be used. Use a relative or absolute path. Relative paths are relative to the Maestro User Interface’s home folder.
- **Number of previous backups to keep** – Defines the number of previous backups that will be kept each time a new backup is made. If set to “0” (zero), then only the most current backup is saved.
- **Event transfer interval** – Tracking events are initially collected in Maestro Tracker, but before they become available for reports, they need to be transferred to the Maestro User Interface. So as not to over burden the components, these transfers happen in “bursts,” and this parameter defines the time interval between bursts. As a result, there will not be any apparent changes in reports until the next interval has past, transferring more tracking data from Maestro Tracker to the Maestro User Interface.

- **Job archive folder** – Defines the folder where archived jobs are saved. Archived jobs are special ZIP archive files that are removed by the administrator from the Delivered Jobs listing in the Maestro User Interface. If left empty, the folder named “archive” inside the Maestro User Interface application home folder will be used.
- **Log level** – Sets the level of logging for the Maestro User Interface Component.
- **Runtime Administration** – These settings allow the administrator to influence the availability of the Maestro User Interface, for example in the event of a system shutdown. The administrator can disable the Outbox, lock login access, present a text message at the top of each screen to actively logged in users while the login is locked, and create a message that appears to any user trying to login while the login is locked.



Decide on a time slot each week to perform non-emergency maintenance of the server (for example software upgrades). Let your users know about this in advance so they know to avoid sending jobs right before that time slot. When taking the system down for non-emergency maintenance, disable the outbox and login access an hour ahead (or whatever time seems appropriate) to give the users time to finish their current activities and log out in time.

Database Plugins – Register and unregister database plugins. Database plugins allow LISTSERV Maestro to communicate with databases. For more information see Section 5.2 [Registering a Database Plugin](#).

Figure 13 Database Plugins

Database Plugins

The list below shows all registered database plugins.

Click on the "unregister" link to unregister it.
Use the "Register New Database Plugin" button to register a new plugin.

Plugin Name	Full Class Name	
MySQL Driver Database Plugin	com.lsoft.lui.db.mysql.MySQLDriverPlugin	Unregister

System Database Connection – Defines the settings for the Maestro System Database. For more information on the system database, see Section 4 [The System Database](#)

Figure 14 System Database Connection

System Database Connection

Maestro System Database Connection

On this page you define the settings of the System Database that the Maestro User Interface uses to store its internal system data in.

Maximum number of buffered connections:

Use the internal database as the System Database

The following external database is used as the System Database:

Database Plugin:

Connection Details

Database Name:

MySQL User Name:

Password:

Database Host Name:

TCP/IP Port:

(Note: Changes in this category require a restart of the Maestro User Interface to take effect.)

- **Maximum number of buffered connections** – Defines the maximum number of “open” database connections the Maestro User Interface will keep open at any time. After the Maestro User Interface has finished using a connection, it will not close the connection again, but keep it open as a buffered open connection.
- **System Database connection choice** – Select the option button “*Use the internal database as the System Database*” to use the internal database (based on MySQL) as the system database. Select the option button “*The following external database is used as the System Database.*” to use an external database as the system database. In this case, select the corresponding database plugin from the drop-down menu. Once a plugin has been selected, a set of input fields will appear where it is necessary to enter details for the database connection such as server name, database port, database name, user name and password. The exact details depend on the plugin selected.

7.2 Application Default Settings

Application default settings are used to set system-wide defaults. LISTSERV Maestro will use default settings if no other settings have been entered at the group or user level. To use default settings, leave all other settings at the group and user level blank. If different settings are entered at the group or user level, they will override the default settings.

Default LISTSERV Connection – Defines the default LISTSERV connection and the LISTSERV Connection for automatic bounce handling. The default setting is used for all accounts that do not have single user or group LISTSERV connections defined. LISTSERV settings defined at the user or group level will override the default settings for only those users or groups. As a result, it is possible to have some users and groups using the default LISTSERV settings and other users and groups using settings defined at the user or group level.

- **LISTSERV Host** – Enter the host name of the server that is actually running LISTSERV. LISTSERV Maestro will use this host name to look up the server running LISTSERV and connect to it using the TCPGUI port. Do not use a server name or alias that appears to the outside clients to be running LISTSERV, such the server name that LSMTMP is

running on. For more information, see Section 6.2.1 [Specifying the LISTSERV Host Name](#)

- **Host Name for Return Path/List Address** – If different from the LISTSERV Host, enter the host name of the server running LISTSERV as seen by outside clients such as Internet. This host name can be an alias or point to the server where LSMTP is running. For more information, see Section 6.2.1 [Specifying the LISTSERV Host Name](#)
- **LISTSERV TCGUI Port** – Enter the port number on the LISTSERV host where LISTSERV listens special TCGUI connections. The default is 2306.
- **LISTSERV Client Address** – Enter the e-mail address that has been configured in LISTSERV to have the right to send DISTRIBUTE jobs. See Section 6.1 [Preparing LISTSERV to Process Jobs from LISTSERV Maestro](#).
- **LISTSERV Client Password** – Enter the password configured with the LISTSERV Client Address. See Section 6.1 [Preparing LISTSERV to Process Jobs from LISTSERV Maestro](#).

Figure 15 Default LISTSERV Connection

LISTSERV Connection

LISTSERV Connection
Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

LISTSERV Host: < default undefined >

Host Name for Return Path/List Addresses:

LISTSERV TCGUI Port:

LISTSERV Client Address: < default undefined >

LISTSERV Client Password: < default undefined >

LISTSERV Connection for Automatic Bounce Handling
Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

No dedicated bounce server
(use standard LISTSERV server, see above)

Use dedicated server
(settings to be supplied when this option is selected)

In high volume environments, a special LISTSERV instance that is dedicated to handling bounced mail may be used. If this is the case, select the option button labeled "Use *dedicated server*" and then define the settings of this second LISTSERV instance in the lower fields. For more information on preparing LISTSERV and LISTSERV Maestro to work together, see Section 6 [LISTSERV and LISTSERV Maestro](#).

Figure 16 Dedicated Bounce Server

LISTSERV Connection

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

LISTSERV Host: < default undefined >

Host Name for List Addresses:
 < default undefined >

LISTSERV TCPGUI Port: Default: 2306

LISTSERV Client Address: < default undefined >

LISTSERV Client Password: < default undefined >

LISTSERV Connection for Automatic Bounce Handling

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

No dedicated bounce server
(use standard LISTSERV server, see above)

Use dedicated server as follows:

LISTSERV Host: < default undefined >

Host Name for Return Path:
 < default undefined >

LISTSERV TCPGUI Port: Default: 2306

LISTSERV Client Address: < default undefined >

LISTSERV Client Password: < default undefined >

OK Cancel

Default Tracking URL – Generates the tracking URL for all accounts where no explicit tracking URL is defined on either the single user or group level. For more information on the default tracking URL, see Section 7.1 [Setting the Default Tracking URL](#).

- **Tracker Host** – Enter the host name of the server running the Maestro Tracker component.
- **HTTP Port** – Enter the port where the Maestro Tracker component on the Maestro Tracker host listens for HTTP connections. The default port number is 80.

Figure 17 Default Tracking URL

Tracking URL

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Tracker Host: < default undefined >

HTTP Port: Default: 80

OK Cancel



Important: All accounts and groups must use tracking URLs that point to the same physical Maestro Tracker server, using the same HTTP port. Although it is possible to enter different Maestro Tracker host names and port settings on the same global application, group level, or individual user level, all those entries must point back to the same physical server, using the same HTTP port. For more information, see Section 7.1.1 [Multiple Tracking URLs](#) and the online help.

Default Size Limits – Sets a size limit for e-mail messages and any file uploaded to the system. The size limit for an e-mail message applies to the total byte size of the message (after all transfer encoding and MIME multipart wrappers have been applied). If the message exceeds the size limit, the delivery will fail. The size limit for all uploaded files includes recipient lists, attachments, image files and so on.

Figure 18 Default Size Limits

Size Limits

Size Limits

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.
(Values without a suffix are interpreted as "Bytes". To specify a value in "Kilobytes" or "Megabytes", append a "K" or "M", respectively. (Samples: "150K" or "5M").

Maximum Message Size: Default: No Limit.

Maximum File-Upload Size: Default: 50M

OK Cancel

Default Content Restrictions – Define AOL Rich Text settings for an alternative part of an HTML message. Create a set of parameters to set up a list of files or URLs that are available to use as drop-in content elements. See the online help for more information on using this setting.

Figure 19 Default Content Restrictions

Content Restrictions

Content Restrictions

Allow usage of AOL format alternative in HTML mail
 Do not allow usage of AOL format alternative in HTML mail

Drop-In Content Restrictions

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Security Issue: Drop-In content elements of type "file" and "URL" will access the files or URLs entered by the user in the context of the **server**. Therefore, in order to protect sensitive or other non-public information, you need to designate specific files, folders, and URLs that users will be able to access. See the help page for more information.

Prefix-Strings of files to which access is allowed:
 Default: No file access allowed

Prefix-Strings of URLs to which access is allowed:
 Default: No URL access allowed

OK Cancel

Default Recipients Restrictions – The screen is split into two sections. The top section, "Recipients Type Restrictions" sets the type of recipients the user is able to use for an e-mail job. If "Disabled" is selected, the option will appear grayed out in the Maestro User Interface, and the user will not be able to select it. If "Hidden" is selected, the recipient type will be disabled and will not appear at all in the Maestro User Interface.

The bottom section, "Recipients Upload Restrictions" contains a text box for the administrator to enter in allowable paths or path prefixes leading to files on a server accessible to the Maestro User Interface. These files are used for uploading "just-in-time" CVS files for recipients definitions. If left blank, CSV files used for just-in-time recipients definitions in the recipients definition wizard will not be allowed.

Figure 20 Default Recipients Restrictions

Recipients Restrictions

Recipients Type Restrictions

Define which recipients types are available to the user.
 Select "Use Default" to inherit the default settings from application level.
 Select "Enabled" to enable a recipients type.
 Select "Disabled" to disable but still display a certain recipients type.
 Select "Hidden" to disable and hide a certain recipients type.

Standard recipients types
 Enable at least one of the following standard recipients types.

	Enabled	Disabled	Hidden	Use Default	
Upload a Recipients Text File	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Use Existing Recipients Target Group	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Select Recipients From a Database	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Send to an Existing LISTSERV List	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Let LISTSERV Select Recipients From a Database	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled

Advanced recipients type
 You can additionally enable the following advanced recipients type.

	Enabled	Disabled	Hidden	Use Default	
Determine Recipients by Inspecting the Reaction on another Job	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled

Recipients Upload Restrictions

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Security Issue: Recipient upload of type "file" will access the files entered by the user in the context of the **server**. Therefore, in order to protect sensitive or other non-public information, you need to designate specific files and folders that users will be able to access. See the help page for more information.

Prefix-Strings of files to which access is allowed:

Default: No file access allowed

7.3 Setting the Default Tracking URL

Before a user can send mail with open-up or click-through tracking, the administrator first has to configure the host name and port that LISTSERV Maestro will use for the tracking URLs generated for the message. The global default setting is used for all accounts that do not have single user or group settings. The default settings, single user settings, and group settings can be combined to offer separate tracking URL settings for different accounts and groups so that

the administrator has greater flexibility in terms of customizing the tracking URL for certain accounts or groups.

When LISTSERV Maestro tracks open-up or click-through events, it does so by inserting special tracking URLs into the messages that are delivered. A typical click-through tracking URL looks something like the example below:

```
http://hostname/trk/click?ref=z4bx39x&
```

In this URL, the “hostname” points to the server where the Maestro Tracker component is installed. If the Maestro Tracker component is configured to use a non-standard HTTP port, then the tracking URL has to include the HTTP port, like the example below:

```
http://hostname:port/trk/click?ref=z4bx39x&
```

All account holders that do not have separate single user or group tracking URLs configured use the default tracking URL. The administrator can define the tracking URL host and port on an individual account level (for accounts that are not part of a group) or on group level (in which case the settings are shared by all accounts in the group).

To define the tracking URL host and HTTP-port:

- **Default Tracking URL** – For all accounts and groups that do not have individual settings, click **Global Component Settings**, then **Maestro User Interface** and then **Default Tracking URL**. The settings defined here will affect all accounts that do not have a tracker host or HTTP-port configured on a single user or group level.
- **Single User Tracking URL** – For an individual account that is not part of a group, click **Administer User Accounts**. Click on the user name of the account to be configured (must be an account without a group) then click on **Maestro User Interface**. The settings defined here affect only the selected account.
- **Group Tracking URL** – For all accounts in a group, click **Administer User Accounts** and then click on the group name of any account that is a member of the group to be configured. The settings defined here affect all accounts in the selected group.

For all three choices, there are two possible settings:

- **Tracker Host:** Enter the host name to be used in the tracking URL. Leave empty to accept the default (if any). If left empty with no default given, users of this account or group will not be able to send e-mail messages with tracking.
- **HTTP Port:** Enter the HTTP port to be used in the tracking URL. Leave empty to accept the default.

7.3.1 Multiple Tracking URLs

There are many uses for setting up multiple tracking URLs. One use of multiple tracking URLs is to customize the look of the tracked URL within the message. Another use of separate tracking URLs would be in the case of using a proxy where the host name of the tracker host used in the internal network is different than the host name that external users would have to use.

Customization is useful in an environment where the same LISTSERV Maestro setup is shared between several distinct groups that want to differentiate themselves in the tracking URL that is merged into the messages they send. For example, the fictitious organization “MyCorp” has two divisions, one for consumer electronics and one for home appliances. The administrator of MyCorp sets up a single LISTSERV Maestro and creates two groups, “electro” and “homeapp”. These group accounts are created in order to be used by the members of the two divisions (which can also employ team collaboration inside of each group).

The name of the server where the Maestro Tracker component is installed is “tracker.mycorp.com”, but the users do not want this host name to appear in the tracking URL in the messages that are delivered. Therefore the administrator also sets up two DNS names “electro.mycorp.com” and “homeapp.mycorp.com” as aliases for the same server. Next, the administrator uses the procedure described above to set the tracker host name of the “electro” and “homeapp” groups to the corresponding aliases. As a result, even though both divisions are sharing the same LISTSERV Maestro installation, the tracking URLs generated for the e-mail they send are “customized” to contain a host name that matches each division’s name.

Another example is if LISTSERV Maestro is installed behind a proxy, where URLs for external access need to use the proxy’s host name and port, which then transparently forwards the requests to the actual tracker host behind it. In this case, the administrator would set the proxy’s host name and the proxy-port that is forwarded to the HTTP port on the tracker host as the default “Tracker Host” and “HTTP Port” setting, to be used by all accounts.



HTTP Port should always be left empty unless there is a proxy at the new host/port pair that redirects the connection to the single port on the TRK server that processes all tracking events, as described in Section 7.1.1 [Multiple Tracker URLs](#)

Section 8 Administrative Policies

Every institution and business using networked computers will have its own administrative policies for data backup, error reporting, access to software on the network, user accounts, and so on. Assimilating LISTSERV Maestro into the existing administrative structure is done through “*General Administration*” and “*Administrative E-mail Notification*” settings.

General Administration settings are available for each of the three components, HUB, LUI, and TRK. Each component can have its own settings for saving backups and logging activity. The Administration Hub component has additional general administrative settings for external processes to be run after a backup completes (See Section 11.2 [Configuring External Post-Backup Processes](#) for details). The Maestro User Interface has additional settings for transferring events from the Maestro Tracker component, job archiving, and runtime administration.

Administrative E-mail Notification settings allow for the set up of special e-mail notification messages to be sent to a configured address or addresses in the event of a system problem and/or a system startup.

8.1 Configuring Backups

The Administration Hub component of LISTSERV Maestro acts as the backup master for all three components. This way any problems that might arise from having different components that store data independently and reside on different servers is avoided.

The Administration Hub will centrally trigger a backup on all connected components (including itself) in order that the backup data saved by each component is consistent with the backup data of all other components. This backup is initiated based on the values entered in the Global Component settings for the Administration Hub. See Section 11 [Saving and Restoring a Backup](#) for additional information.

Each component can save its backup in its own folder configured in the “*General Component Settings*” section of the component. See Section 11.3 [Configuring the Backup Location](#) for more information. Each component also has a setting to determine how many backups are saved to ensure against the possibility of restoring a backup containing corrupted data. See Section 11.4 [Configuring the Backup History](#) for more details.

8.2 Configuring Logging

Logging application messages uses system resources. The level of logging selected will determine how much of the system’s resources will be devoted to this task and what will be recorded. Choose the logging level based on resources available and what events need to be recorded. A new installation or an installation that has upgraded, moved, or otherwise changed may have logging set at its highest level during a testing phase, and then dropped back once the system is running smoothly. Logging levels can be changed at any time and can be set at different levels for different components.

LISTSERV Maestro has three levels of logging. Choose the level of logging in General Component Settings for each component. Click the option button adjacent to the level of logging desired.

- “*Only log severe messages*” – Logs only unexpected problems and errors.
- “*Log severe and standard operational messages*” – Logs all severe messages and general informational messages about normal operations such as logins, or new jobs.
- “*Log all messages*” – Logs all severe messages, all operational messages, and additional detailed messages to describe the ongoing processes such as databases opened and closed, or files created or deleted. These messages are usually used for troubleshooting.

For more information about logging in LISTSERV Maestro see Section 12 [Maestro Logs](#).

8.3 Runtime Administration and System Shutdown

These settings allow the administrator to influence the availability of the Maestro User Interface. For example, they can be used in preparation of the system shutdown for maintenance by disallowing new logins, disabling the outbox to prevent outgoing jobs from being sent, and sending a warning message to users already logged on to the system.

Runtime Administration settings are located under **Global Component Settings -> Maestro User Interface -> General Administration of Maestro User Interface**. Use these settings to reach a safe shutdown state, where shutting the system down will not disrupt jobs being sent or users in the midst of preparing a job. Follow these steps to safely shut down LISTSERV Maestro:

1. Open a browser and access the Maestro User Interface, log in with the administrative account. See Section 10 [Special Administrative User Account](#) for more information.
2. Open a second browser and access the Administration Hub. Go to the "*General Administration of Maestro User Interface*" screen.
3. Check the option "*Sending is disabled.*" This will stop any new jobs from starting their send process.
4. Check the option "*LISTSERV Maestro User Interface is locked.*" This will stop any new users from logging in.
5. In the top text box, enter an informational message such as "The system will shortly go down for maintenance, therefore login is currently not possible" so users denied login will know why.
6. In the bottom text box, enter an informational message such as "The system will shortly go down for maintenance. Please finish your current work and log out as soon as possible or contact the administrator" so that all current users will now see this warning at the top of every page they access and will know to wrap up whatever they are doing. Consider adding a message telling users exactly when the system will shutdown and for how long.
7. In the browser that is logged into the administrative user account, click on the **Outbox** icon. All of the pending jobs will be listed in a table. Click on the **State** link to sort the jobs according to their processing status. Jobs that are in the process of sending will be indicated by a yellow arrows icon. Refresh the screen to renew the list. When the jobs have finished processing they will no longer appear in the table after refreshing the screen. New deliveries will not start since the "*Sending is disabled*" option in the Administration Hub has been set.
8. After all jobs that were in the process of sending have finished and currently logged in users have had enough time to wrap up what they were doing, LISTSERV Maestro can be safely shut down and maintenance tasks can be executed.
9. After the restart, return to the HUB and uncheck the "*Sending is disabled*" and "*LISTSERV Maestro User Interface is locked*" options to make the Maestro User Interface available and working normally again.



Important: When the LISTSERV Maestro Tracker component is shut down, all tracking URLs become unavailable, and all other tracking activity stops. Mail recipients will not be able to click on links in the message and no tracking events will be recorded. If at all possible, install the tracker component on its own server to minimize down time. Try to schedule system shutdowns at a time that disrupts the fewest users and the fewest possible mail recipients.

Note: LISTSERV Maestro can be put into "Maintenance Mode" by setting the INI file `MaintenanceMode = true` and then restarting the component. While in this mode, no users will be able to log into the Maestro User Interface, so maintenance tasks can be executed. To

return the component to normal, change the setting to `false`, delete the entry, or comment it out with a leading `"#"` or `"!"` and restart.

8.4 User Restrictions

LISTSERV maestro has many features that allow regular users' activities within the system to be limited. Some limitations occur on a system-wide level such as not allowing multiple logins from the same account, and some limitations can be configured to occur on a system, group, or individual level.

User access to LISTSERV Maestro can be limited to a single login per account or allow multiple logins per account. This setting is located in the Runtime Administration section of the Maestro User Interface. See Section 16.2 [Disallowing Concurrent Access with the Same User Account](#) for more information.

Each of the LISTSERV Maestro components (HUB, LUI, and TRK) can be configured to restrict access based upon the IP address of the computer where the browser/e-mail-client is running that is used to access the component. This means that it is possible, for example, to define that everyone (all IP addresses) is allowed to access the Maestro Tracker component, but only certain addresses (a local subnet, perhaps) are allowed to access the Maestro User Interface and Administration Hub components. See Section 16.1 [IP Address Restrictions](#) for more information.

Other user restrictions that can be configured at the system level are:

- **Maximum size limit for an e-mail message** – Set a limit for the total byte size of the message after all transfer encoding and MIME multipart wrappers have been applied. This setting can be set as the default in the **Global Component Settings -> Maestro User Interface -> Default Size Limits**. The default can be overridden by setting this limit at the group or user level when administering user accounts. See Section 9.2 [Editing Account Information and Assigning Single User Settings](#).
- **Maximum file size for uploaded files** – Applies to all types of files uploaded to the system including recipients lists, HTML and text messages, attachments, images, and so on. This setting is only available application wide. It is not available at the group or user levels.
- **Content Restrictions** – Allow special AOL Rich Text formatting as part of defining an e-mail message or not. If allowed users can choose to include an AOL alternative in any HTML message created. This setting is available application wide as a default setting, and users can inherit or override the setting.
- **Drop-in Content Restrictions** – Create a positive list for files and a positive list for URLs that are going to be used as drop-in content elements. This helps prevent security breaches into local files and URLs. If this setting is left blank on the system level it must be set on the group or user level to allow those accounts to use files and/or URLs as drop-in content. If left blank on every level, drop-in content of these types will not be allowed. See Section 9.2 [Editing Account Information and Assigning Single User Settings](#) for more information.
- **Recipients Restrictions** – The top section, "*Recipients Type Restrictions*" sets the type of recipients the user is able to use for an e-mail job. If "*Disabled*" is selected, the option

will appear grayed out in the Maestro User Interface, and the user will not be able to select it. If *“Hidden”* is selected, the recipient type will be disabled and will not appear at all in the Maestro User Interface. The default can be overridden when configured at the group and user level. See Section 9.2 [Editing Account Information and Assigning Single User Settings](#) for more information.

The bottom section, *“Recipients Upload Restrictions”* contains a text box for the administrator to enter in allowable paths or path prefixes leading to files on a server accessible to the Maestro User Interface. These files are used for uploading “just-in-time” CVS files for recipients definitions. If left blank, CSV files used for just-in-time recipients definitions in the recipients definition wizard will not be allowed.

Other restrictions can be placed on individual accounts when configuring *“Team Collaboration”* settings. Team collaboration settings allow the job owner to give or revoke privileges to group members affecting their abilities to create jobs, work on particular parts of jobs like defining recipients, and use jobs in reports. These settings can be configured at a default level for all jobs that an account owns under user settings for an account, and they can be set at the job level for individual jobs.

8.5 Administrative E-mail Notifications

E-mail messages can be sent to an e-mail address or addresses by LISTSERV Maestro in the event of a system problem or system startup. Once configured, errors and/or startups that occur on any component will trigger a message. If an error occurs on three components, three separate messages will sent to each configured recipient address. To have administrative e-mail notifications sent, select the option button to send e-mail notifications. If notification is desired for system start, check the box for *“Send a notification e-mail at each startup.”* The following settings need to be configured to use e-mail notifications:

- **SMTP Host** – Enter the host name for the SMTP server that will be used to mail the notifications. This is a mandatory field must be filled out with a valid host name. This host name will be used to send mail by the LISTSERV Maestro component that encounters the problem. Make sure to specify a host name that is reachable from all servers running a LISTSERV Maestro component.
- **SMTP Port** – Enter the SMTP port that the SMTP server on the host specified listens for SMTP connections. This field is optional. If left empty, the standard SMTP port 25 is used.
- **Sender Address** – Enter a sender address that will be used as the sender address for all the e-mail notifications. This field is mandatory and must be filled out with a valid Internet e-mail address.
- **Notification e-mail will be sent to the following addresses** – Specify at least one valid Internet e-mail address that will be the recipient of the notifications sent from LISTSERV Maestro. This field is mandatory. Multiple addresses can be entered, one per row, with no separator characters. All addresses entered here will appear in the “To:” field of the e-mail notification, so each recipient will be able to see the addresses of all other recipients.

8.5.1 Testing E-mail Notifications

It is important to test the settings for e-mail notifications to make sure that they do work, and that the specified addresses receive the mail sent by the system. This verification is done with the checkbox at the bottom of the page, labeled "*Send a test e-mail to the addresses listed above*".

Checking this option and then submitting the page with **OK** will send test e-mail to all recipients specified. Test e-mail will be generated by each of the LISTSERV Maestro components so that each of the addresses will receive three different test messages, one from each component.

As the next step, verify that all specified addresses received three test-notification e-mail messages. If this is not the case, then the notification sending needs some troubleshooting. Follow these steps to troubleshoot the e-mail notification settings:

1. Check the log file(s) of the component(s) that did not send e-mail notification. Verify that the log(s) contains an entry with the following text:
*"Administrative e-mail notifications have been enabled.
This message is for testing that administrative e-mail notifications have been enabled correctly, there is no problem with the application!"*
If this message does not appear, then the checkbox "*Send a test e-mail to the addresses listed above*" was not actually checked when the page was submitted, or the **OK** button was not clicked and the screen was exited by the **Cancel** button or any of the shortcut icons.
2. If the message above appears in the log file, then check the log file for an error message that appears right after the message quoted above. The error message will read: "*Error when trying to send notification e-mail about previous log entry: Error description here...*"
The error description will provide an idea of what needs to be changed to make the messaging work (for example, the error could be caused by an incorrect host name or SMTP port).
3. If the first message appears in the logs, but not the second, (the error message) LISTSERV Maestro presumes the e-mail notification was successfully sent. If this happens, take a closer look at the SMTP server and the other components in the mail delivery chain to find out where the mail went missing.

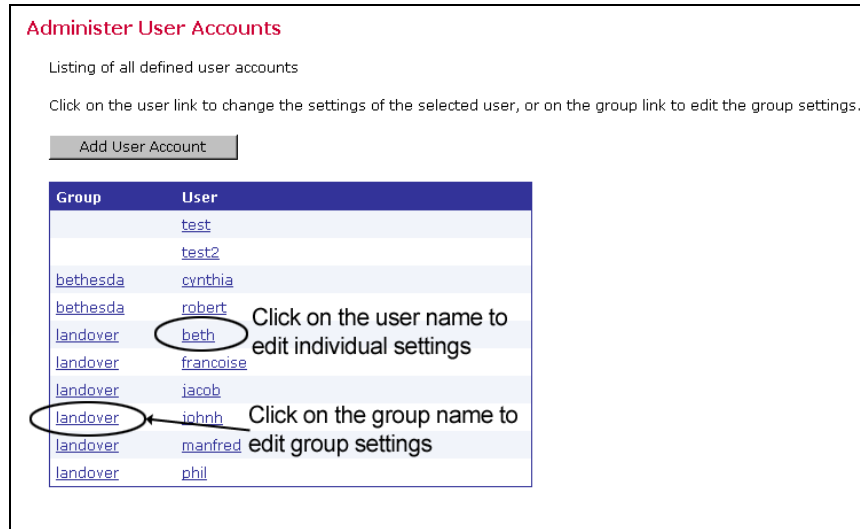
Section 9 Creating and Administering User Accounts

The "*Administer User Accounts*" screen displays a list of all defined user accounts. Each user name is a link that opens the "*Define User Account*" screen. Links on this screen lead to user settings that can be changed for only that single user account. If the user is a member of a group, the group name is a link that opens the "*Group Settings*" screen, containing settings that can be changed for the entire group.

From the Administer User Accounts screen it is possible to:

- Add a new user account
- Assign users to a group
- Edit existing user account settings, including deleting the accounts
- Edit existing group settings

Figure 21 Administer User Accounts



9.1 Creating a New User Account

To create a new user account, click the **Add User Account** button.

- **User** – Fill in a user name. User names are not case sensitive, and can be composed of letters, numbers and symbols. User names can also contain spaces. User names must be unique if users are not assigned to a group. Users assigned to different groups may have the same user name as long as the combination of user name and group name is unique.
- **Group** – Assign the user to a group if desired. Groups are optional and can be left blank. However, users must be assigned to a group in order to use the team collaboration features. Only members of the same group can collaborate on e-mail jobs. The combination of user name and group name must be unique. There cannot be two users with the same name in the same group, although there may be two users with the same name in different groups.
- **Password** – Assign a password. All passwords are case sensitive, and must be at least five characters long.
- **Confirm Password** – Retype the password to confirm it.

Figure 22 Defining User Account

Define User Account

Change the user data as required:
Leave both password fields empty to keep the old password.

- Username (case-insensitive) [mandatory]
- Group (case-insensitive) [optional]
- Password, with a minimum length of 5 characters (case-sensitive) [mandatory]

User:

Group:

Password:

Confirm Password:

The user is allowed to change his password.

Check the box next to “*The user is allowed to change his password.*” to grant the user permission to change his or her password. Uncheck the box to revoke this privilege. Click **Save** to save account information and continue. Click **Cancel** and a new user will not be created.

9.2 Editing Account Information and Assigning Single User Settings

Once a new account has been created, it must be edited to assign it single user settings. To edit existing account information, click on the user name link. From here it is possible to “*Edit general user settings*” including user name, group, and password. Or, “*Edit component specific settings*” which controls how the user interacts with the Maestro User Interface.

Figure 23 Editing Account Information


Currently selected user: maria

Define User Account

Account Administration

Edit general user settings:
[User name, group and password](#)

Edit component specific settings:
[Maestro User Interface](#)



Click the **Up One Level** icon again to return to the Administer User Accounts screen.

9.2.1 Editing General User Settings

Change the user name, group, or password of an existing account from this screen. To keep an old password while changing other settings, leave both password fields blank. To delete an account, click the **Delete** button.

Figure 24 Editing User Settings

Define User Account

Change the user data as required:
Leave both password fields empty to keep the old password.

- Username (case-insensitive) [mandatory]
- Group (case-insensitive) [optional]
- Password, with a minimum length of 5 characters (case-sensitive) [mandatory]

User:

Group:

Password:

Confirm Password:

The user is allowed to change his password.

9.2.2 Editing Component Specific Settings for Single and Group Users

After an account is initially created, click on the **Maestro User Interface** link located under the heading “*Edit component specific settings:*” to open the selection list for all user specific settings. This list will vary depending on whether the user is a member of a group (a group user) or not (a single user). The selection list displayed in Figure 23 is for a single user who is not part of a group. The selection list displayed in Figure 24 is for a group user.

To edit settings at the group level, click on the name of the group from the Administer User Accounts screen (see Figure 18).

Click on any setting to open a screen to edit the setting.

Figure 25
Single User Settings for a Non-Group Member

Single User Settings

Component Administration

Click on one of the following links to define the single user settings:

- [User Right Settings](#)
- [LISTSERV Connection](#)
- [Tracking URL](#)
- [Size Limits](#)
- [Job ID Prefix](#)
- [Content Restrictions](#)
- [Recipients Restrictions](#)





Figure 26
Single User Settings for a Group Member

Group User Settings

Component Administration

Click on one of the following links to define the group user settings:

- [User Right Settings](#)
- [LISTSERV Connection](#)



Settings can include any of the following:

- **User Right Settings** – The user rights apply only to the configured user, even if the user belongs to a group. Check the boxes next to the privileges to be granted to the user.

Uncheck the boxes next to the privileges to be revoked from the user. User rights settings include:

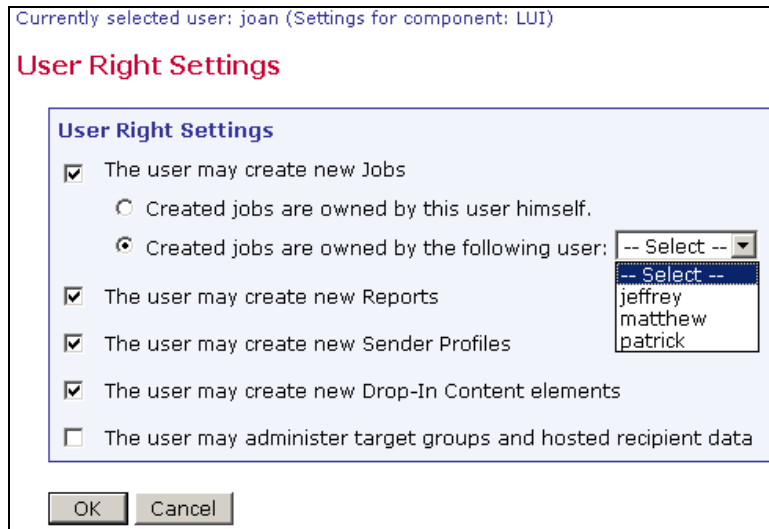
- **The user may create new Jobs** – Grants the right to create new jobs. If the user is a member of a group with the right to create new jobs, it is necessary to also define who owns the jobs that are created by this account. Jobs can be owned by the account that creates them, or by another group member, selected from a drop-down menu of existing accounts in the group.
- If jobs created by one account are owned by another group member, when the user creates a new job, the ownership will be set to the other group member and the team collaboration default preferences of that account are applied.



- **Important:** If the owner account of a job that another account tries to create has not given that account at least one right in their team collaboration default settings, the creating account will not be able to start a new job, and an error message will appear on the "Start New Job" screen.
- **The user may create new Reports** – Grants the right to create new reports. Existing reports are available for all members in a group.
- **The user may create new Sender Profiles** – Grants the right to create new sender profiles. Existing sender profiles are available for all members in a group.
- **The user may create new Drop-In Content Elements** – Grants the right to create new drop-in content elements. Existing drop-ins are available for all members in a group.
- **The user may administer target groups and host recipient data** – Grants the right to administer existing target groups and to create new recipient target groups by providing access to Recipients Target Groups Wizard.

New users will default to having all privileges granted except the right to "...*administer target groups and hosted recipient data.*" (For more information on target groups and hosted recipient data, see the LISTSERV Maestro Database Administrator's Manual.) If certain privileges are revoked, the user will see a slash through the icon(s) in the Maestro User Interface that accesses the corresponding function(s).

Figure 27 User Right Settings



- **LISTSERV Connection** – The LISERVER Connection can be set at several levels. The widest level of setting is the Global Component Setting, which defines the global default LISERVER Connection on the application level (see Section 7.2 [Application Default Settings](#)). These settings will be used as defaults for all accounts that do not have individual settings for group or user level.

The next level is the default setting for a group (see Figure 26). To set the LISERVER settings for an entire group in the user list, click on the group name rather than the user name (appears only if the account belongs to a group, see Figure 18). If defined on the group level, the group settings will override the global default settings for that group. The settings will apply to all accounts in the group, except for the settings "LISTSERV Client Address" and "LISTSERV Client Password". These two settings may be configured individually for each account in the group. Accounts in the group for which they are not configured will use the group's settings as the default.

Individual accounts are the last level of settings for the LISERVER Connection. Individual accounts can belong to a group (group user) or not belong to a group (single user). Settings for individual accounts will override default group and global settings. To set the LISERVER Connection for an individual account, click on the user name from the user list. The screen that opens is different depending on whether the account is a group user or a single user. Single user accounts can have all LISERVER Connection settings defined (see Figure 26). Group user accounts can only define the settings for "LISTSERV Client Address" and "LISTSERV Client Password" (see Figure 27). These individual group settings result in a different LISERVER e-mail address for each user so that jobs can be identified by owner in the LISERVER logs.

For information and instructions on how to fill out the fields for setting the LISERVER Connection, see Section 6 [LISTSERV and LISERVER Maestro](#). For information about setting a special external host name, see Section 6.2.1 [Specifying the LISERVER Host with Different Internal and External Names](#). For information on setting up a dedicated LISERVER instance for processing bounces, see Section 6.2.2 [Specifying a Separate LISERVER Instance for Processing Bounces](#).

Figure 28 Default LISTSERV Connection for a Group with Dedicated Bounce Server

Use the information on this line to determine which settings are being edited.
Currently selected group: landover (Settings for component: LUI)

LISTSERV Connection

LISTSERV Connection for a group become the default for the group, overriding the Global default LISTSERV settings.

LISTSERV Connection
Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

LISTSERV Host: Default: yourserver.company.com

Host Name for List Addresses: ▾

LISTSERV TCPGUI Port: Default: 2306

LISTSERV Client Address: Default: maestro@yourserver.company.com

LISTSERV Client Password: Default: *****

LISTSERV Connection for Automatic Bounce Handling
Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Inherit settings from application defaults
(Currently: Use standard LISTSERV server, see above)

No dedicated bounce server
(use standard LISTSERV server, see above)

Use dedicated server as follows:

LISTSERV Host: < default undefined >

Host Name for Return Path: ▾

LISTSERV TCPGUI Port: Default: 2306

LISTSERV Client Address: < default undefined >

LISTSERV Client Password: < default undefined >

Figure 29 LISTSERV Connection for a Single User without a Dedicated Bounce Server

Use the information on this line to determine which settings are being edited.
 Currently selected user: boss (Settings for component: LUI)

LISTSERV Connection

LISTSERV Connection
 Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

LISTSERV Host: Default: yourserver.company.com

Host Name for Return Path/List Addresses:

LISTSERV TCPGUI Port: Default: 2306

LISTSERV Client Address: Default: maestro@yourserver.company.com

LISTSERV Client Password: Default: *****

LISTSERV Connection for Automatic Bounce Handling
 Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Inherit settings from application defaults
 (Currently: Use standard LISTSERV server, see above)

No dedicated bounce server
 (use standard LISTSERV server, see above)

Use dedicated server
 (settings to be supplied when this option is selected)

Figure 30 LISTSERV Connection for a Group User

Currently selected user: jsmith (Settings for component: LUI)

LISTSERV Connection

LISTSERV Connection
 Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

LISTSERV Client Address: Default: maestro@yourserver.company.com

LISTSERV Client Password: Default: *****

- **Tracking URL** – Available only for single users and groups. Enter the Tracker URL for the user. Each user or group can have a different Tracker URL, although they all must lead back to the same tracker component. The domain name must resolve to an IP address on the server where the tracker component is installed.

Figure 31 Tracking URL

Tracking URL

Tracking URL
 Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Tracker Host: Default:

HTTP Port: Default: 9105

- **Size Limits** – Available for single users and groups, sets a size limit for e-mail messages. The size limit for an e-mail message applies to the total byte size of the

message (after all transfer encoding and MIME multipart wrappers have been applied). If the message exceeds the size limit, the delivery will fail.

Figure 32 Size Limits

Size Limits

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.
(Values without a suffix are interpreted as "Bytes". To specify a value in "Kilobytes" or "Megabytes", append a "K" or "M", respectively. (Samples: "150K" or "5M").

Maximum Message Size: Default: No Limit.

OK Cancel

- **Job ID Prefix** – Available for singles users or groups, a Job ID Prefix is an optional part of the Job ID. The prefix comes before the system generated Job ID and is separated by a hyphen. Allowing, disallowing, or presetting Job ID Prefixes for users takes place by selecting the corresponding option button and entering the prefix. For more information on job ID prefixes see the LISTSERV Maestro Users Guide, Section 3.1.



Use preset Job ID prefixes to easily identify jobs from different groups or users. For internal chargeback purposes, the Job ID can be extracted from the job name and base charges on records in LISTSERV's "system changelog". If no such identification is necessary, select "any job ID prefix allowed" to give users a way of grouping jobs.

Figure 33 Job ID Prefix

Job ID Prefix

Job ID Prefix Settings

Never use a job ID prefix

Any job ID prefix allowed

Use the following prefix for every job ID:

Only job ID prefixes from the following list are permitted:

temp
news
sale

Enter one prefix per row.

OK Cancel

- **Content Restrictions** – Available for single users or groups, defines restrictions for the content of e-mail messages. In the top section of the screen, select the option button to allow or disallow an AOL formatted alternative for HTML e-mail messages. For more information on HTML messages, see the LISTSERV Maestro User's Manual, Section 5.3.

In the bottom section of the screen, create a "positive list" of all files and/or URLs that will be available for drop-in content. If the list is left blank, no drop-in content in the form of files and/or URLs will be allowed. See the online help for more information on using this setting.

Figure 34 Drop-In Content Restrictions

Content Restrictions

Content Restrictions

Allow usage of AOL format alternative in HTML mail

Do not allow usage of AOL format alternative in HTML mail

Use the inherited setting: Do not allow usage of AOL format alternative in HTML mail

Drop-In Content Restrictions

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Security Issue: Drop-In content elements of type "file" and "URL" will access the files or URLs entered by the user in the context of the **server**. Therefore, in order to protect sensitive or other non-public information, you need to designate specific files, folders, and URLs that users will be able to access. See the help page for more information.

Prefix-Strings of files to which access is allowed: Default: No file access allowed

Prefix-Strings of URLs to which access is allowed: Default: No URL access allowed

OK Cancel

- **Recipients Restrictions** – Available for single users and groups. In the top section of the screen, set the type of recipients available for use for an e-mail job. If “*Disabled*” is selected, the option will appear grayed out in the Maestro User Interface, and the user will not be able to select it. If “*Hidden*” is selected, the recipient type will be disabled and will not appear at all in the Maestro User Interface.

In the lower section of the screen, set the recipient upload restrictions by entering a file name and path if the recipients will be taken from a file on the server "just-in-time" before the job is sent. If the list is left blank, no file access will be allowed. See the online help for more information on using this setting.

Figure 35 Recipients Restrictions

Recipients Restrictions

Recipients Type Restrictions

Define which recipients types are available to the user.
Select "Use Default" to inherit the default settings from application level.
Select "Enabled" to enable a recipients type.
Select "Disabled" to disable but still display a certain recipients type.
Select "Hidden" to disable and hide a certain recipients type.

Standard recipients types
Enable at least one of the following standard recipients types.

	Enabled	Disabled	Hidden	Use Default	
Upload a Recipients Text File	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Use Existing Recipients Target Group	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Select Recipients From a Database	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Send to an Existing LISTSERV List	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled
Let LISTSERV Select Recipients From a Database	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled

Advanced recipients type
You can additionally enable the following advanced recipients type.

	Enabled	Disabled	Hidden	Use Default	
Determine Recipients by Inspecting the Reaction on another Job	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default: Enabled

Recipients Upload Restrictions

Leave the fields empty to use the defaults, if defined, or enter a value to overwrite the default.

Security Issue: Recipient upload of type "file" will access the files entered by the user in the context of the **server**. Therefore, in order to protect sensitive or other non-public information, you need to designate specific files and folders that users will be able to access.
See the help page for more information.

Prefix-Strings of files to which access is allowed:

Default: No file access allowed

OK Cancel

To set component settings for a group, click on the group name. The "Group Settings" screen opens and will list the component settings:

- Default LISTSERV Connection
- Tracking URL
- Size Limits
- Job ID Prefix
- Content Restrictions
- Recipient Restrictions

The screens that configure these settings are very similar to the screens that configure single user settings. The difference is that settings configured at the group level will affect all members of the group whereas settings configured for the single user will only affect that user.

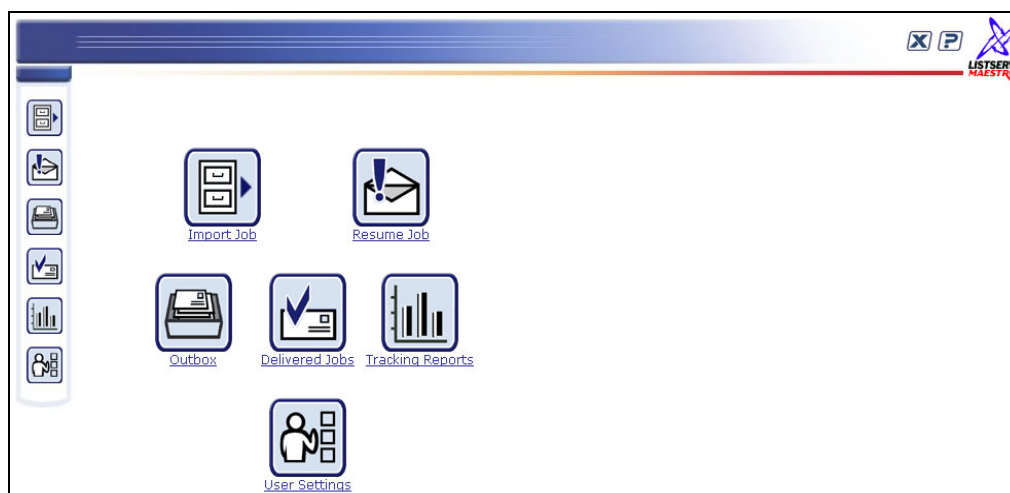
A variation to this rule is the group default LISTSERV Connection. If defined on the group level, the group settings will override the global default settings for that group. The settings will apply to all accounts in the group, except for the settings "LISTSERV Client Address" and "LISTSERV Client Password". These two settings may be configured individually for each account in the group (accounts in the group for which they are not configured will use the group's settings as the default). To set the LISTSERV Connection for an individual account, click on the user name from the user list. The screen that opens is different depending on whether the account is a group user or a single user. Single user accounts can have all LISTSERV Connection settings defined (see Figure 26). Group user accounts can only define the settings for "LISTSERV Client Address" and "LISTSERV Client Password" (see Figure 27).

Section 10 Special Administrative User Account

With every installation of LISTSERV Maestro, a special user account for the system administrator is available. From this account it is possible to archive delivered jobs and import jobs from the archive back into LISTSERV Maestro. The administrator can also change the ownership of a job, report, sender profile, drop-in content element, or recipients target group.

To access this account, log into the Maestro User Interface (LUI) as an administrator, using "admin" in the "User:" field and then typing in the administrator password that was configured in the Administrator Hub. The home page for the administrative user account is different than that of the home page for normal users.

Figure 36 Special Administrative User Account



10.1 Archiving Delivered Jobs

To save server space and shorten jobs listings within the Maestro User interface, administrators can archive delivered jobs and jobs that have been closed after a failed delivery. Archiving a delivered or failed job removes the job from the system and saves it in a single ZIP archive file stored in a special archive folder on the system. Archived jobs cannot be viewed because all their tracking events are deleted and they are removed from any report data sources. As a result, any existing reports referencing them in their data sources will not display correctly.

The default archive folder of a LISTSERV Maestro installation is located along a path similar to: `\Program Files\L-Soft\Application Server\lui\archive`. Although archived jobs

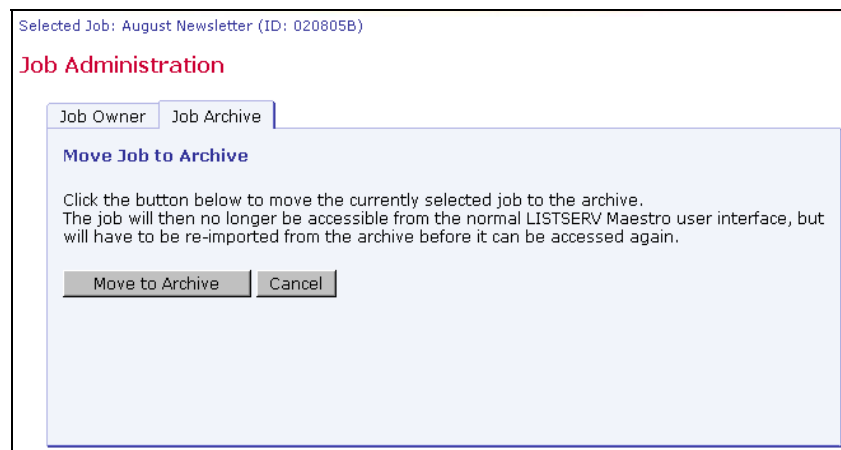
are saved as ZIP files, little space will be saved because the archive folder exists on the same server or disk as the application. To fully utilize saving disk space by archiving jobs, they need to be moved from the server or disk where LISTSERV Maestro is installed. This can be done two different ways.

The first way is to change the default archive folder in the Administration Hub to point to a folder that is located on a different disk. The disk could be another disk on the same server, a mapped network drive (Windows), or a mounted NFS drive (Linux) available on another server. By setting a different default folder for saving archived jobs within the Administration Hub, the list of archived jobs displayed under the **Import Job** icon remains intact. All archived jobs in the folder will display in this list and can be imported back into LISTSERV Maestro if necessary. To change the default archive folder, see Section 7 [Settings for the Maestro User Interface](#).

The second way to move archived jobs from the disk or server where LISTSERV Maestro is located is to do so manually. Open the default archive folder. All archive files are ZIP files and have the job ID in the file name. Select the files and move them to a secondary storage medium such as different disk, a tape, a CD-ROM or similar. Once the file has been removed from the default archive folder it will not appear in the list of archived files. Files removed from the archive folder can be moved back in it at any time to then will appear in the list of archived files. Once listed, the files will be available to import back into LISTSERV Maestro.

To archive a delivered or failed job, click on the **Delivered Jobs** icon from the home page of the administrative user account. The “*Delivered Jobs*” screen opens listing all the previously delivered jobs. Click on the Job ID link to select the job. The “*Job Administration*” screen opens. Click on the **Job Archive** tab. Next, click the **Move to Archive** button. Click the **Cancel** button to cancel the operation and return to the Delivered Jobs screen.

Figure 37 Job Administration - Job Archive



10.2 Importing an Archived Job

To restore an archived job to the system, click on the **Import Job** icon located on the home page. A listing of all the jobs currently present in the archive will appear. Click on the Job ID link to select the job to be restored. Imported archived jobs are in a “frozen” state. The status and the contents of the job will not change from the moment it was placed in the archive. Any tracking events that arrive after the moment the job is archived will be discarded, even if the job is later imported.

Imported jobs will have to be assigned a new Job Owner. Use the drop-down menu to select an owner for the imported archived job. Once restored, an imported job will be listed again in Delivered Jobs with its original Date and Time of Delivery (not the archived date). Imported archived jobs can be used by the job owner (and other group members if applicable) in tracking reports.

Figure 38 Archived Jobs

Job ID	Job Title	Job Owner	Archive Date/Time
DD-020826B	test	erlangen / robert	Aug. 26, 2002 02:56:38 AM
NEWS-020808A	Widget Company September Newsletter	landover / beth	Aug. 27, 2002 04:33:54 PM

10.3 Changing Job and Report Ownership

The user that initially creates a new job or report is the owner of that job or report. The owner is the only user with privileges (rights) to execute the following job or report related actions:

- Assign collaboration rights on the job to other group members
- Change the job information (job title and job ID-prefix)
- Delete the job
- Re-open, retry, or close a failed job in the Outbox
- Assign collaboration rights on the report to other group members
- Delete the report

No other user can be granted owner rights within the same e-mail job. Therefore, it is important that there is an owner for each job and each report, because only the owner can execute these actions.

Under normal conditions there will always be an owner because the initial creator will automatically become the owner. However, under certain circumstances, a job may lose its owner:

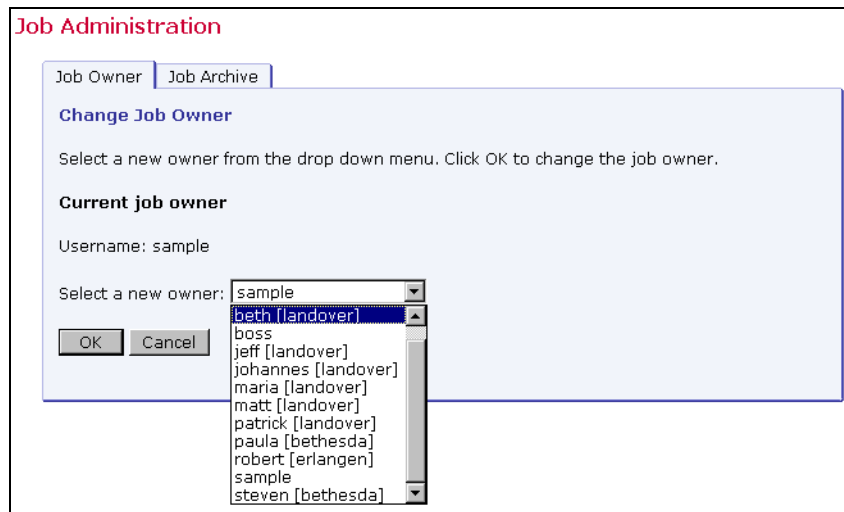
- If an account is deleted in the Administration Hub (and therefore also in the Maestro User Interface), then all jobs and reports that were owned by that account will be without an owner.
- If an account that was a member of one group is changed so that it becomes a member of another group, or not a member of any group at all, then all jobs and reports that were owned by that account will be without an owner.

To reassign a job, click on the appropriate icon to open the listing for that job. Click **Resume Job** for a listing of all the current jobs that have not been delivered yet, **Outbox** for all the jobs that have been authorized for delivery, or **Delivered Jobs** for all the jobs that have already been

delivered. To reassign a report, click the **Tracking Reports** icon for a listing of all the currently defined reports.

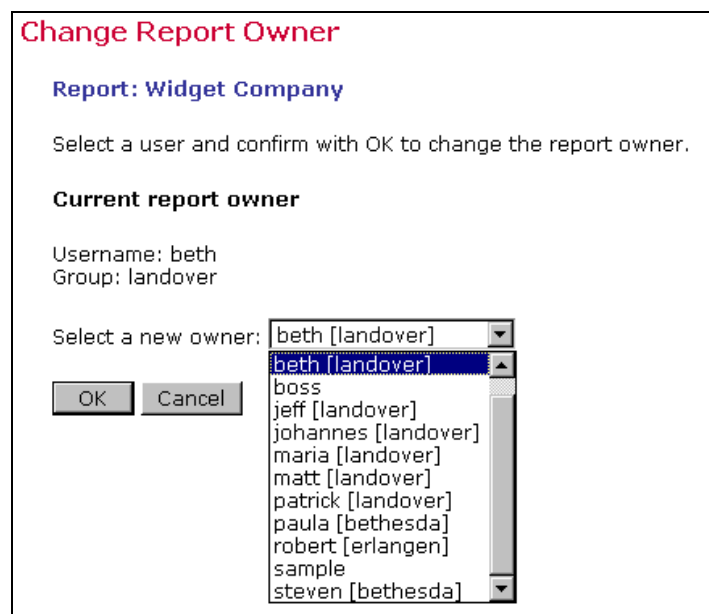
To select a job to reassign, click on the Job ID. The Job Administration screen opens. Click on the **Job Owner** tab (if necessary). Select a new owner for the job from the drop-down menu. Click **OK** to save the change, or **Cancel** to discard the change and return to the previous menu.

Figure 39 Change Job Owner



To select a report to reassign, click on the report title. The "Change Report Owner" screen opens. Select the new report owner from the drop-down menu. Click **OK** to save the change, or **Cancel** to discard the change and return to the previous screen.

Figure 40 Change Report Owner



When an account is changed or ownership of a job or report is transferred, job and report rights are affected.

-
- **Account name is changed; account not in a group**
The account retains ownership of all jobs and reports. The account remains the owner of all previous jobs and reports. Since the account is not a member of a group, neither before nor after the change, team collaboration rights on the jobs and reports are not affected.
 - **Account name is changed; account member of a group**
The account retains ownership of all jobs and reports and the jobs and reports remain in the same group. The account retains ownership of all previous jobs and reports. The team collaboration rights on the jobs and reports are not affected. All members in the same group that had any job or report privileges before the change have the same privileges after the change.
 - **Group is added to a non-group account**
The account retains ownership of all jobs and reports and transfers them to the new group. The account remains owner of all previous jobs and reports. Since the account was not a member of a group before the change, no team collaboration rights on the jobs and reports are affected. However, after the change, since the account is now a member of a group, the owner of the account can assign team collaboration rights on any of the jobs or reports to any of the other members in the group.
 - **Group is removed from a group account**
The account loses ownership of all jobs and reports. Jobs and reports remain in the old group. All previous account privileges for any jobs or reports are removed. This means that the account loses all team collaboration rights on all jobs and reports that are owned by other members of the account's old group. The account also loses ownership of all jobs and reports that the user of the account created while the account was still a member of the old group. The team collaboration rights of other members of the old group are unaffected. However, these jobs no longer have an owner, since the old owner left the group. The administrator should set a new owner at this point.
 - **Group account becomes member of different group**
The account loses ownership of all jobs and reports. Jobs and reports remain in the old group. All previous account privileges for any jobs or reports are removed. This means that the account loses all team collaboration rights on all jobs and reports that are owned by other members of the account's old group. The account also loses ownership of all jobs and reports that the user of the account created while the account was still a member of the old group. As a result, the account joins the new group as a "fresh" member, without any team collaboration or job or report ownership rights. The jobs and reports that were created by the user of the account while still in the old group remain in the old group. The team collaboration rights that other members of the old group may have on those jobs and reports are unaffected. However, these jobs no longer have an owner, since the old owner left the group. The administrator needs to set a new owner at this point.
 - **Ownership of a job or report is transferred; previous owner not in a group**
The new account acquires all ownership rights on the job or report. The original owner loses all rights, including ownership.
 - **Ownership of a job or report is transferred; previous owner in a different group from new owner**
The new account acquires all ownership rights on the job or report. For all other

accounts (the previous owner and the members of the old group), ownership or team collaboration rights are removed.

- **Ownership of a job or report is transferred; previous owner in same group as new owner**

The new account acquires all ownership rights on the job or report. The original owner loses all rights, including ownership. However, any other accounts that may have team collaboration rights on the job or report do retain these rights – they are preserved.

10.4 Changing Sender Profile, Drop-In Content Element, and Recipients Target Group Ownership

Drop-in content elements, recipient target groups, and sender profiles are utility items in LISTSERV Maestro created for the convenience of the users. These items, if created by a user who is not part of a group, are owned by that single user and cannot be used by any one else. If a member of a group creates items, then everyone in that group can use them. In addition, users in that group who have the necessary right can create new items, and delete or modify existing items.

An item can lose its owner and become ownerless under certain circumstances:

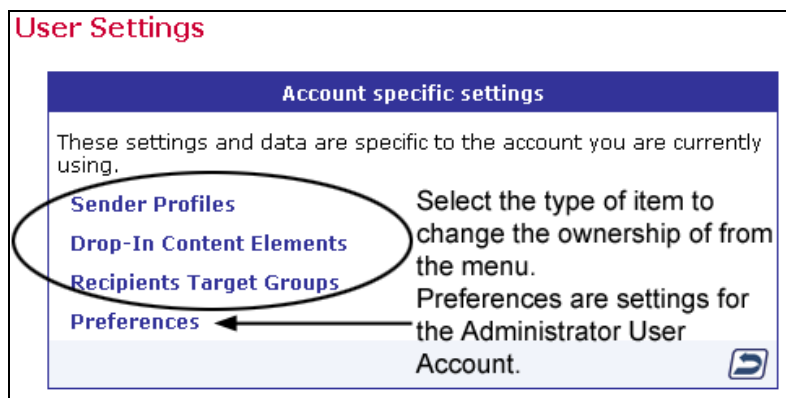
- If an item is owned by a non-group account, and that account is deleted.
- If a group owns an item, and the last account of that group is deleted or is moved out of the group (into another group or made into an account without a group).

The ownership of any item, whether it already has an owner or not, can be changed by the administrator using the special Administrator User Account. The administrator can also delete any item.

To change the ownership of a Sender Profile, Drop-in Content Element, or Recipients Target Group, click on the **User Settings** icon from the homepage. The “*User Settings*” screen opens. Select the item type to change from the menu.

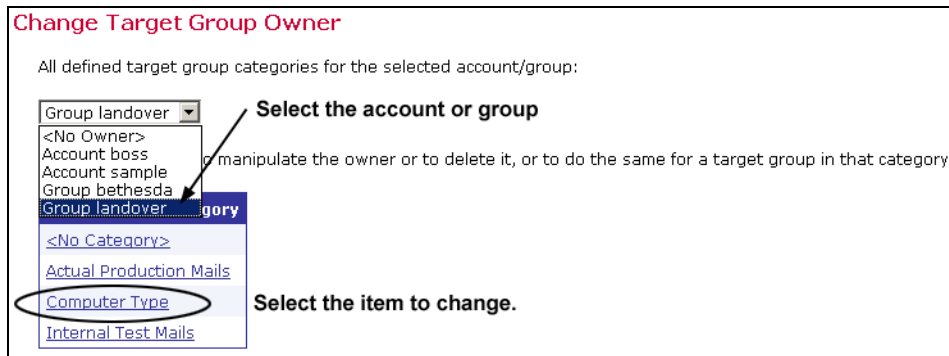
Note: The **Preferences** link on the menu is for setting the user preferences for the Administrator User Account, and has nothing to do with changing the settings or item ownership for other accounts.

Figure 41 Change Ownership



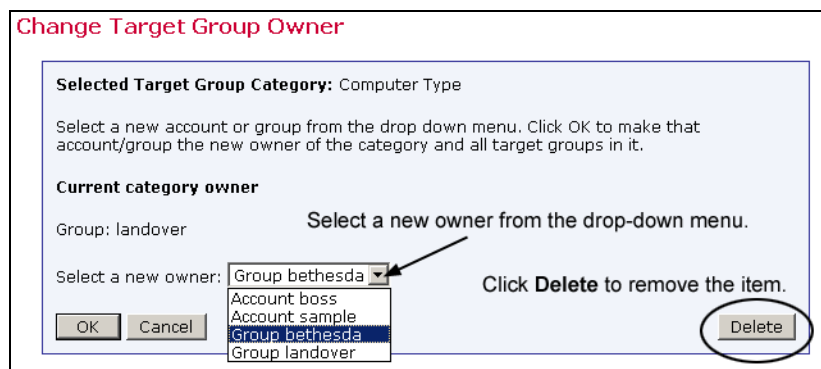
Clicking on any of the menu entries will open a list of the related items, grouped after their current owners. At the top of the list, a drop-down list with all available owners appears. The list includes all available non-group accounts, all available groups, and a special “<No Owner>” entry. Below the drop-down list is a table listing all items that are currently owned by the selected owner account or group.

Figure 42 Select Target Group and Item to Change Ownership



Click on an item to open a screen where a new owner can be selected, or where the item can be deleted.

Figure 43 Change Target Group Owner



If an item is moved to a new owner, and the new owner already has an item with the same name, the moved item is automatically renamed to give it a unique name. For example, if an item named “sample” is moved to an owner who already has an item with that name, the moved item is renamed “sample1”. If “sample1” is also in use, the moved item will be renamed “sample2”, and so on until a unique name is created.

Ownership of an item is affected when an account is changed in the following ways:

- **Account name is changed, account not in a group**

The account keeps ownership of all items of which it previously was the owner.

- **Account name is changed, account member of a group**

Since the items are owned by the account’s group anyway, ownership is not affected, meaning that they are still owned by the same group as before.

- **Group is added to a non-group account**

Ownership of all items previously owned by the account is transferred to the group that the account joins. All members in that group will then share ownership of these items. The account also gains ownership of all items that previously existed in the group it joins.

- **Group is removed from a group account**

Since the group owns the items, the account loses access to them. They stay in the old group. The account that no longer belongs to a group does not have ownership of any items until new ones are created with this account.

- **Group of a group account is changed – account becomes member of different group**

Since the old group owns the items, the account loses access to them. They stay in the old group. The account gains ownership of all items that previously existed in the new group it joins.

Section 11 Saving and Restoring a Backup

It is a standard best practice for any administrator to make regular backups of critical software and data. LISTSERV® Maestro archives a consistent backup of the data collected in the application so that it can be restored in the event of a system failure.

LISTSERV Maestro gives the Administration Hub component the responsibility of acting as backup master to avoid any problems that might arise from having different components that store data independently and reside on different servers. If different components initiate backups at different times, inconsistent data sets between components can result. If both backups were then to be restored, the data sets would be inconsistent, invalidating the backup.

The Administration Hub will centrally trigger a backup on all connected components (including itself) in order that the backup data saved by each component is consistent with the backup data of all other components. This backup is initiated based on the values entered in the Global Component settings for the Administration Hub.

11.1 Configuring the Backup Time

The application wide backup is triggered once per day. Each day at a certain time, the Administration Hub (backup master) will start a backup of each component. To assign backup settings, click the **Administration Hub** link. Set the time to start the backup master by entering the desired time of the daily backup in the form “*hh:mm*” with values from 00:00 to 23:59.

There may be times when it is necessary to create a backup immediately, for example just before any invasive procedure such as moving a component or applying a patch, or in the case of an emergency. To spawn a backup immediately, click the **Execute Backup Now** button.

Figure 44 General Component Settings for Administration Hub

General Component Settings for Administration Hub

Backup Settings

Time for daily backup: (hh:mm)
(This time is relative to the time zone of the server)

External processes to run after a backup completes:
(Your commands will be executed inside of a command shell with "cmd /c YOUR_COMMAND ARG1 ... ARGn".)

After backup success: [Test](#)
(Leave empty for default: "none".)

After backup failure: [Test](#)
(Leave empty for default: "none".)

Work folder for commands:
(Leave empty for default: "application home".)

[View list of currently active "after backup" processes.](#)

Backup folder:
(Leave empty for default: "backup".)

Number of previous backups to keep:

Execute Backup Now

Log Level

Only log severe messages.
 Log severe and standard operational messages.
 Log all messages.

Click **OK** to save settings and return to the Administer Component Settings screen.

11.2 Configuring External Post-Backup Processes

The administrator may define external processes that will be executed after a backup is completed. External processes may be used to execute additional backup tasks such as automatically moving the backup folders to a tape, copying backup folders to a network drive, notifying the administrator by e-mail if the backup was unsuccessful, and so on. Two different external processes can be defined, one to be executed after a successful backup and one after a backup failure.

Each process is specified in form of an external command that is executed by the Administration Hub when the backup completes. If it is necessary to execute more than one command, they can be written into a batch file (Windows) or shell script file (Unix/Linux). If this is the case, the name of that batch/script file is entered as the external command to be executed (with all necessary parameters). The administrator may also specify the work folder for the commands (same folder for both commands).

Clicking the **Test** link, located next to each command box, executes the command for a testing. A new window will pop up that shows the output of the command. In this window the external process can be stopped, if necessary. Closing the popup window before the process terminates, will not stop the process, it will continue running. To view the output of the test process again (if it is still running), or to terminate it (if it does not terminate by itself), access the process by using the **View list of currently active "after backup" processes** link.



Important: Commands should not define external processes that run indefinitely. Each external process should terminate itself when it has completed the action it is supposed to execute. Processes that run continuously over time slow the server down. Eventually this will cause a crash because each time a backup finishes, a new process will be started, tying up more system resources.

If several external processes are running using a batch/script file, make sure that all processes started by the batch/script file terminate themselves at some point. If you start an external process that does not terminate itself (because of a defect in the external process, or by mistake), click on the **View list of currently active "after backup" processes** link.

This screen displays a list of all currently active external processes started by the Administration Hub, either as an actual "after backup" process that was started when a backup was completed, or because the administrator clicked on one of the **Test** links. Only processes that are still running are shown in this list. Each process is shown with the date and time it was started, the command that was used to start it, and a link that opens a pop-up window. The pop-up window continuously shows the output of the external process (if any) and allows for the termination of that process while it is still running.

If any of the command fields are left empty, no external process will be started at the corresponding "after backup" condition. If the work folder is left empty, then the application home folder of the Administration Hub will be used as the work folder.

11.3 Configuring the Backup Location

Each component has a backup location. This is necessary because the components may reside on different servers. The backup default location is the folder "backup", which is in the home folder of the component in question (for example "\Program Files\L-Soft\Application Server\lui").

It is possible to use a different folder if desired. The folder configured may be either an absolute path, such as "C:\MyFolder\backup", or a relative path, such as "myFolder\backup", which is then interpreted as being relative to the home folder of the component. Enter the path name in the "*Backup folder:*" text box at each of the following locations:

- For the Administration Hub component, click the **Administration Hub** link to open the Administration Hub subsection.
- For the Maestro User Interface component, click the **Maestro User Interface** link to open the Maestro User Interface subsection. Next, click **General Settings**.
- For the Maestro Tracker component, click the **Maestro Tracker** link to open the Maestro Tracker subsection.

Click **OK** to save all entries.



Important: Do not configure different components to save backups into the same folder.

11.4 Configuring the Backup History

To lessen the risk of restoring a backup containing corrupted data, LISTSERV Maestro provides the opportunity for administrators to create a backup history. Each component can be configured to keep a number of previous backups. Each time a new backup is made, it is saved into the backup folder configured for the component (see Section 11.3 [Configuring the Backup Location](#)).

If the component is also configured to keep a number of previous backups, then the folders containing the older backups will be kept under names like “NAME1”, “NAME2” ... “NAME_n”, where “NAME” is the name of the standard backup folder and “n” is the number of previous backups that the component is set to keep.

For example, if a component is configured to keep three previous backups, then the backup history of each day will look like this:

Table 2 Backup History

Day 1	backup – contains backup of day 1
Day 2	backup – contains backup of day 2 backup1 – contains backup of day 1
Day 3	backup – contains backup of day 3 backup1 – contains backup of day 2 backup2 – contains backup of day 1
Day 4	backup – contains backup of day 4 backup1 – contains backup of day 3 backup2 – contains backup of day 2 backup3 – contains backup of day 1
Day 5	backup – contains backup of day 5 backup1 – contains backup of day 4 backup2 – contains backup of day 3 backup3 – contains backup of day 2

Keeping a backup history can help ensure against corrupted backup data. However, as the amount of application data grows, it may not be possible to keep many old backups, which take up space on the disk. Also, keeping older backups on the same disk does not ensure against failure of the disk itself (head crash for example). Always save the backup to an external backup medium as described in Section 11.5 [Saving a Backup to an External Medium](#).

Note: if daily backups are saved to an external medium routinely, it is acceptable to set the number of old backups to “0”.

11.5 Saving a Backup to an External Medium

Once LISTSERV Maestro has completed its backup, the configured backup folder of each component contains the data that is required to restore this component to the state of the moment when the backup was triggered. To prevent catastrophic loss of data, save these folders to an external backup medium such as a backup tape or other storage device.

To avoid a potential partial backup problem, use the automatically triggered external post-backup process that is outlined in Section 11.2 [Configuring External Post-Backup Processes](#) to ensure that the backup tool does not start its work until after the completion of the internal backup. Use whatever standard backup tool is used by the organization to configure a daily backup of the designated folders. Schedule this daily backup to occur at a time after the time when the Administration Hub itself triggers and completes the backup of each component. There should be a long enough period between the backup triggered inside of LISTSERV Maestro and the backup to the external medium triggered by the backup tool to ensure that all components have enough time to complete their backups. Otherwise, partial data would be backed up to the external medium.

For small installations, the backup inside LISTSERV Maestro will not take more than a few minutes. However, as the data in the LISTSERV Maestro installation accumulates over time, backup will naturally take longer. If post-backup triggers are not being used, periodically check the backup logs to see how long the backup actually takes and schedule the external backup accordingly, at a safe time after the LISTSERV Maestro backup is completed.

Remember that the external post-backup command or backup tool must be configured such that it backs up all backup folders of all components. A LISTSERV Maestro installation will have three backups to save to an external medium, one for the Administration Hub, one for the Maestro User Interface, and one for Maestro Tracker. These folders may also reside on different servers, depending on the installation.

11.6 Identifying the Backup: The Backup ID

Because the LISTSERV Maestro components store their backup data into separate folders, it is necessary to know which of the folders belong together, in case a backup history is kept or it is necessary to retrieve a backup from an external medium. This is done using the backup ID. Each backup gets a unique ID that is shared by all components participating in the backup. Each component also writes a “`readme.txt`” file into the backup folder. Stored in this text file is the ID of the backup that saved the data in the particular backup folder, together with output about backup start time, end time and its success or error state.

11.7 Restoring a Backup

In the unfortunate event of having to restore a backup, follow the procedure described in this section. There are several steps that need to be executed to successfully restore a backup. Please review each step carefully. Some steps have lengthy descriptions or sub-steps. Do not skip steps, or do them out of order or the restoration will not succeed.

1. Identify the backup that is to be restored

This usually is the most recent backup, but it also must be a successful backup. If there were errors during the most recent backup, revert to the next most recent backup, which may have to be retrieved from an external medium.

-
- To find out if a backup was successful check the backup log in the folder:

```
\Program Files\L-Soft\Application Server\hub\logs
```

For each backup triggered by the Administration Hub, a report named “backupReport_ID.txt”, where “ID” is replaced with the ID of the backup in question, is saved into this folder. The IDs are assigned in alphanumeric order; the most recent backups have higher order IDs (in an alphanumeric sense). Use the file date of the report file to locate the most recent backup.

If the backup was successful, an entry like this will appear at the end of the file:

```
“The backup was completed successfully  
Final completion date: <date here>”
```

If the backup was unsuccessful for any reason, then the report will contain entries detailing the errors that occurred.

If the “logs” folder cannot be accessed (because a disk crash destroyed the disk of the Administration Hub installation, for example), it is still possible to locate the most recent successful backup by opening the “readme.txt” file in the backup folder of each component. The “readme.txt” file lists the backup ID and the success state of that particular backup. If no errors are reported in that file, then the backup of this component was successful. If successful backups with the same ID of all the other components are located, then a complete and successful backup set exists and can be restored.

2. Find the backup folders from all components that belong to the same backup set

Once the backup to be restored has been identified and the backup ID is determined, the next step is to find all the backup folders of the individual components that contain data for this backup. Check the “readme.txt” in the backup folder of each component. If it contains the same ID, the right backup folder for this component has been located.

3. Copy the backup folders and save them in a safe location

These folders will have to be copied back into the system in a later step, and need to be saved in a location that will not be affected by the next step, which is to make a fresh installation.

4. Make a fresh installation of all components

This includes uninstalling old versions (if necessary) and installing the components on the servers where needed. Do not start the components after installation.

5. Restore all three components

- **To restore the Administration Hub**

Remove the existing versions of the file “hub.ini” and the folders “accountreg” and “hubreg”, including their contents, from the Administration Hub home folder:

```
\Program Files\L-Soft\Application Server\hub
```

Replace them with the versions from the backup folder of the Administration Hub component that was saved in step 3.

- **To restore the Maestro User Interface**

Remove the existing versions of the files “lui.ini” and “my.ini” and the folders “luidata” and “registry”, including their contents, from the Maestro User Interface home folder:

```
\Program Files\L-Soft\Application Server\lui
```

Replace them with the versions from the backup folder of the Maestro User Interface component that was saved in step 3. Next, add a new entry into the “lui.ini” file like the example below:

```
RestoreBackup=path_to_backup_folder
```

The “*path_to_backup_folder*” is replaced with the path name that leads to the backup folder from which the files and folders, as described above, were copied.

This path name may either be a full path name including driver letter, or it may be an absolute path without driver letter starting with “\” or “/”, which is then interpreted as being absolute on the drive/root where the application server is installed (for example, in the default case, the same drive where “\Program Files\L-Soft\Application Server” is located). Or a relative path without a driver letter may be used, and not starting with either “\” or “/”, which is then interpreted as being relative to the home folder of the Maestro User Interface component (for example, in the default case, that would be the folder “\Program Files\L-Soft\Application Server\lui”).

Forward slashes “/” or backslashes “\” may be used as the filename separator. However, if backslashes are used, then use double backslashes.

Example, either write:

```
C:/Sample/MyFolder/backup
```

or

```
C:\\Sample\\MyFolder\\backup
```

This entry to the “lui.ini” file will be automatically removed during the first startup of the component. It is only present to signal to the component that it should restore all required data from the given folder, which happens automatically during the next startup, whenever this INI file entry is present. For more information on editing INI files, see Section 19 [Editing LISTSERV Maestro INI Files](#).

- **To restore Maestro Tracker**

Remove all “*.dat” files from the folder called “data” inside the Maestro Tracker home folder:

```
\Program Files\L-Soft\Application Server\trk\data
```

Replace them with the “*.dat” files from the backup folder of the Maestro Tracker component that was saved in step 3. Also replace the file “tracker.ini” in the Maestro Tracker home folder, (not into the “data” folder) with the same file from the backup folder.

6. Edit respective INI files if necessary

If components are being restored on different servers or a different combination of servers than the original backup was taken from, it may be necessary to edit the respective “*.ini” files of the components. This would include restoring a backup to a server with a different name, using a different port number, or changing how the components are grouped on a server or servers. For example, if components that were all originally on the same server are moving to different servers, or taking components that were originally on different servers and moving them to the same server.

7. Start all components

Monitor the log files of the components to check if they start up correctly. If yes, the backup restoration is complete. If any component does not start up correctly, this may be because of differences in the configuration of the backed up system and the restored system. In that case, it may be necessary to adjust further INI file settings (see previous step) or to log into the Administration Hub and configure the necessary settings accordingly. Then restart and again monitor the startup log entries. If necessary, repeat this until the system starts up normally.

Section 12 Maestro Logs

LISTSERV Maestro has three levels of logging. In the Administrator User Interface, it is possible to choose the level of logging for each component. Click the option button adjacent to the level of logging desired.

- “*Only log severe messages*” – Logs only unexpected problems and errors.
- “*Log severe and standard operational messages*” – Logs all severe messages and general informational messages about normal operations such as logins, or new jobs.
- “*Log all messages*” – Logs all severe messages, all operational messages and additional detailed messages to describe the ongoing processes such as databases opened and closed, or files created or deleted. These messages are usually used for debugging, or finding problems.

LISTSERV Maestro log files are located in two places. Log files having to do with specific LISTSERV Maestro components are kept in a directory configured like the example below:

```
x:\Program Files\L-Soft\Application Server\XXX\log
```

“x:” is the drive where LISTSERV Maestro is installed and “XXX” is the component, either HUB, LUI, or TRK.

Log files for third party components like Tomcat are kept in a directory configured like the example below:

```
x:\Program Files\L-Soft\Application Server\logs
```

“x:” is the drive where Maestro is installed.

12.1 Remote Log Access

The three main LISTSERV Maestro components all write their own log files. These files can be found in the “logs” subfolder of each component’s home folder inside of the “Application Server” installation folder. In some situations the administrator may not have access to these folders, but still needs to access the log files. To solve this, LISTSERV® Maestro offers remote log file access. The remote access allows an administrator to download the log files from the server, directly in the Web browser.

Before accessing the log files of a component, configure the component for remote log access first. To do so, edit the INI file of the component and add the following entry:

RemoteAdminPassword=PASSWORD

Replace “PASSWORD” with a password only known to authorized administrators. For security reasons, do not use the normal admin password from the Administration Hub. Because this password will later be used as a parameter in a URL, use only URL-safe characters in the password (alphanumeric characters).

Remember; add this entry to each component’s INI file; to `lui.ini`, `hub.ini` and `tracker.ini`. For information on how to edit INI files, see Section 19 [Editing LISTSERV Maestro INI Files](#). If the entry is not added to one of the INI files, then it will not be possible to access the log files of that component (but it will still be possible to access logs of the other components where the entry has been added). To disable remote log access, simply remove the entry from the INI file(s) or comment it out. Whenever this entry is changed, the change will be effective immediately – The component will not have to restart.

Once the component(s) have been configured for remote log access, access their log files from any Web browser on any computer that has HTTP access to the particular component. The only requirements for access are the “PASSWORD” configured in the INI file(s) and the day of the log file to access.

- To download a Maestro User Interface log file, access the following URL:
`http://HOST:PORT/lui/downloadLog?pw=PASSWORD&day=DATE`
- To download a Administration Hub log file, access the following URL:
`http://HOST:PORT/hub/downloadLog?pw=PASSWORD&day=DATE`
- To download a Maestro Tracker log file, access the following URL:
`http://HOST:PORT/trk/downloadLog?pw=PASSWORD&day=DATE`

Replace “HOST” with the host name of the server running the component to be accessed, “PORT” with the HTTP port on that server (“:PORT” can be left out if the HTTP-port is “80”), “PASSWORD” with the password configured in the INI file, and “DATE” with the date of the day of the log file to download. The date is formatted as “YYYYMMDD”, where “YYYY” is the year with 4 digits, “MM” is the month with 2 digits and “DD” is the day of the month with 2 digits.

Section 13 Using Non-Standard Ports

The components of LISTSERV® Maestro use a number of ports to communicate with each other and with the external world. The ports used are standard ports and will work well under most circumstances. Under certain conditions it may be desirable to change one or several of the ports to other ports, for example, if another application installed on the same server already uses one of the ports LISTSERV Maestro is set to use. Changing ports may require editing certain INI files. For more information on editing LISTSERV Maestro INI files, see Section 19 [Editing LISTSERV Maestro INI Files](#).

13.1 Ports Used by LISTSERV Maestro

This list contains the individual ports used by each of the LISTSERV Maestro components.

13.1.1 Ports used by the Administration Hub

The Administration Hub uses three different ports:

- For HTTP access to the Administration Hub user interface (using a Web browser), the Administration Hub uses the standard HTTP port **80**.
- For internal communication with the other components, the Administration Hub uses port **1099**.
- For shutdown of the application server, the Administration Hub uses port **8007**.

13.1.2 Ports used by the Maestro User Interface

The Maestro User Interface uses four different ports:

- For HTTP access to the Maestro User Interface (using a Web browser), the Maestro User Interface uses the standard HTTP port **80**.
- For internal communication with the Administration Hub, the Maestro User Interface uses port **1099**.
- For the internal database connection (only available in Windows), the Maestro User Interface uses port **3306**.
- For shutdown of the application server, the Maestro User Interface uses port **8007**.

13.1.3 Ports used by Maestro Tracker

Maestro Tracker uses four different ports:

- To collect the tracking events from mailings sent with the Maestro User Interface, Maestro Tracker uses the standard HTTP port **80**.
- For internal communication with the Administration Hub, the Maestro User Interface uses port **1099**.
- To transfer the tracking events to the Maestro User Interface, Maestro Tracker, uses port **7000**.
- For shutdown of the application server, Maestro Tracker uses port **8007**.

13.2 Configuring Port Usage

If any of the ports described in the previous sections are already in use on the server where the LISTSERV Maestro component is installed, it is possible to change the use of this port. Note that some components make use of the same port as other components. This is not a problem between the different components of LISTSERV Maestro. If there are several components on the same server, then these components share usage of these ports (port 80 for HTTP access and port 1099 for internal communication for example). It is not necessary or even possible to configure one component to use a different port than the other while the components are on the same server.

13.2.1 Configuring the HTTP Port

To configure the HTTP port, edit the following file:

```
\Program Files\L-Soft\Application Server\conf\server.xml
```

In this file there is an XML-entry for the “Normal HTTP” connector (this is close to the end of the file, immediately following the “<!-- ===== Connectors ===== -->” header). An example of this entry is in Figure 45.

Figure 45 XML Entry for Normal HTTP

```
<!-- Normal HTTP -->
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
  <Parameter name="handler"
    value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
  <Parameter name="port" value="80"/>
</Connector>
```

The standard HTTP port “80” is used. Simply change this value to any port not currently in use by another application.

If there are several LISTSERV Maestro components installed on the same server, then they will all be affected by this change. It is not possible to use different HTTP ports for each of the components if the components are installed on the same server. However, if the components are installed on different servers, they can use different HTTP ports. It is important to note that these changes will only be effective after a restart of the component in question.

When changing the HTTP port, there are a few issues to be aware of:

- If the HTTP port is changed on a particular server where it affects the Maestro Tracker component (where this component is installed), then it is also necessary to change the Tracking URL – HTTP Port settings in the Administration Hub, either by editing the global component settings or on the group or single user level.
- If the HTTP port is changed on the server where it affects the Administration Hub component, then it is necessary to edit the Maestro User Interface INI file. On the server where the Maestro User Interface component is installed edit the file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit or add the entry “HubHTTPPort” (if the entry is not present or is commented out, it defaults to port 80). For example: HubHTTPPort=8080.” or similar.

- The Maestro User Interface and the Administration Hub User Interface are both accessed via this HTTP port. This implies that if this port were to be changed, it would no longer be possible to access these interfaces by entering their plain URL into the location field of a browser. Instead, it is necessary to add the port number (with a colon “:”) to the URL. For example, if the HTTP port is changed to 8080, then the access URL will need to include the port number as shown below:

```
“http://your_host:8080/lui”.
```

-
- The shortcuts to access the Maestro User Interface and the Administration Hub User Interface that are installed in the Windows start menu do not include any port information. They expect the user interfaces to be accessible on the standard port 80. If this port is changed, then it is necessary to edit these shortcuts and add “:yourPort” to the URL, as described above.
 - Changing the HTTP port also affects the “CompileAll” command (this command is a tool to pre-compile all pages before first use – see the Installation Manual for details). Usually this command is only executed once, right after installation. However, if “CompileAll” needs to be run again (for example after an upgrade installation), and the HTTP access port has been changed for the LISTSERV Maestro installation, the following files must be edited:

```
\Program Files\L-Soft\Application Server\commands\compile\hub.host
```

```
\Program Files\L-Soft\Application Server\commands\compile\lui.host
```

Note that the “hub.host” file is located on the server where the Administration Hub component is installed, while the “lui.host” file is located on the server where the Maestro User Interface component is installed. If both components are on the same server, then the two files will be as well.

The file can be edited with any text editor. It contains a single line, comprised of the access-URL (including host-name and port) for the Administration Hub and the Maestro User Interface component, respectively. Change it so that it contains the new HTTP port with a colon “:” after the host name (or leave out port and colon if the port is the standard port 80). For example, if the HTTP port was changed to “8888”, then the Maestro User Interface entry must look like this:

```
http://yourhost.domain.etc:8888/lui
```

The entry for the Administration Hub will look similar, only with “/hub” at the end.

If the port is changed back to the standard 80, then either include “:80” instead of the “:8888” shown above, or just leave out the port and the colon

```
http://yourhost.domain.etc/lui
```

- If LISTSERV Maestro is installed behind a firewall (which is advisable) and the Maestro User Interface and/or the Administration Hub User Interface needs to be accessible from a computer outside the firewall, the firewall must be configured to allow access on the configured port instead of the standard HTTP port.
- Similarly, if the Maestro Tracker component is installed behind a firewall, then the firewall must be configured to give all outside users access to the server where Maestro Tracker is installed on the port that is configured for HTTP access. This is normally port 80, but can be a different port if the port was changed as described above.

The whole tracking mechanism of LISTSERV Maestro will not work if the Maestro Tracker component is installed behind a firewall in a way such that outside clients do not have access to its configured HTTP port.



Important: Maestro Tracker will work most effectively if set to port 80. Many sites have firewalls that prevent their users from connecting to other ports for HTTP connections, which would not only prevent them from being tracked, but from reaching the URLs that are being tracked.

13.2.2 Configuring the Internal Communication Port

This port can be configured independently for each component. However, if the components are installed on the same server, then they must all use the same internal communications port.

- To configure the communication port for the **Administration Hub component**, edit the following file:

```
\Program Files\L-Soft\Application Server\hub\hub.ini
```

Edit or add the entry “RMIPort”. If the entry is not present or is commented out, the component defaults to port 1099. For example: RMIPort=5310

In addition, it is necessary to edit the INI-file of each component that works together with this Administration Hub component. This is usually one Maestro User Interface and one Maestro Tracker component.

For the Maestro User Interface component, edit the file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit the entry “HubRMIPort” (if this entry is not present or is commented out, it defaults to port 1099).

For the Maestro Tracker component, edit the file:

```
\Program Files\L-Soft\Application Server\trk\tracker.ini
```

Similarly, in this example, edit the entry “HubRMIPort” in the same way as described above for the Maestro User Interface component.

- To configure the communication port for the **Maestro User Interface**, edit the following file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit or add the entry “RMIPort”. If the entry is not present or is commented out, the component defaults to port 1099. Example: RMIPort=5310

- To configure the communication port for **Maestro Tracker**, edit the following file:

```
\Program Files\L-Soft\Application Server\trk\tracker.ini
```

Edit or add the entry “RMIPort”. If the entry is not present or is commented out, the component defaults to port 1099. Example: RMIPort=5310

In addition, edit the Maestro User Interface INI file that communicates with the Maestro Tracker component. On the server where the Maestro User Interface is installed, edit the file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit or add the entry "TrackerRMIPort"

13.2.3 Configuring the Tracker Communications Port

This port is only used by the Maestro User Interface (LUI) to communicate with Maestro Tracker component (TRK). It can easily be configured using the Administration Hub. Simply enter the Administration Hub and click the **Global Component Settings** link, then the **Maestro Tracker** link. Edit the port number from here. Click **OK** to save. The change will be effective immediately.

13.2.4 Configuring the Internal System Database Connection Port

LISTSERV Maestro installations on Windows come with an internal database that can be used as the system database when configured to use this internal database. The port is only used by the Maestro User Interface component. To configure it, edit the following file:

```
\Program Files\L-Soft\Application Server\lui\my.ini
```

In this file, find the entry "port" both in the "[client]" and "[mysqld]" sections. Edit the value of both of these entries to change the database connection port. In addition, edit the following file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit the "MySQLDriverPlugin.databasePort" entry to point to the same port number. These changes will only be effective after restarting the Maestro User Interface component.

13.2.5 Configuring the Application Server Shutdown Port

To configure the application server shutdown port, edit the following file:

```
\Program Files\L-Soft\Application Server\conf\server.xml
```

This file contains an XML-entry similar to the following example, close to the end of the file.

Figure 46 Example of XML File

```
<!-- Apache AJP12 support. This is also used to shut down tomcat. -->
<>Connector className="org.apache.tomcat.service.PoolTcpConnector">
  <Parameter name="handler"
    value="org.apache.tomcat.service.connector.Ajp12ConnectionHandler"/>
  <Parameter name="port" value="8007"/>
</Connector>
```

If port 8007 is already in use on the system, set the port number to a different value in this file. These changes will only be effective after restarting the Maestro User Interface component.

Section 14 Defining IP Addresses

By default, LISTSERV Maestro binds the HTTP port on all IP addresses of the server it is running on. If the server has several addresses, then a client will be able to access the Maestro

User Interface, the Administration Hub, and Maestro Tracker (depending on which components are installed) on the HTTP port by using any of the server's addresses.

No changes to the LISTSERV Maestro configuration are required if this default behavior is satisfactory. However, to make LISTSERV Maestro bind to only a single IP address on the server, the following file needs to be edited:

```
\Program Files\L-Soft\Application Server\conf\server.xml
```

In this file, an XML-entry for the “Normal HTTP” connector occurs close to the end of the file, right after the “<!-- ===== Connectors ===== -->” header. This entry looks similar to Figure 47.

Figure 47 XML Entry for Normal HTTP

```
<!-- Normal HTTP -->
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
  <Parameter name="handler"
    value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
  <Parameter name="port" value="80"/>
</Connector>
```

Add another “<Parameter>” item to that entry, with the name “inet”, and a “value” that corresponds to the IP address to be used. For example, to use the address “192.168.1.1”, the resulting entry would look like Figure 48 (emphasis added for readability).

Figure 48 XML Entry for IP Address

```
<!-- Normal HTTP -->
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
  <Parameter name="handler"
    value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
  <Parameter name="port" value="80"/>
  <Parameter name="inet" value="192.168.1.1"/>
</Connector>
```

Note: If you have several LISTSERV Maestro components installed on the same server, then all of them will be affected by this change. It is not possible to use different bindings for each of the components if the components are installed on the same server. However, if the components are installed on different servers, they can use different bindings.



Important: This change will only be effective after a restart of the component in question.

Section 15 Installing Behind a Firewall

Any network that is connected to the Internet is usually protected by some form of firewall, often in conjunction with different kinds of “demilitarized zones” and other security measures. If there is a desire to install the components of LISTSERV® Maestro behind a firewall, or in different protection zones so that some are behind and others are in front of the firewall, it is necessary to take into account the communication channels between the separate components.

Communication happens exclusively using ports (see the Section 13 [Using Non-Standard Ports](#) for more information). If the components are installed behind, in front of, or around a firewall, the firewall needs to be configured to let communication through on certain ports between certain servers. Figure 38 shows LISTSERV Maestro components and all other players (the Maestro Administrator, the Maestro User, and the Internet, which represents the messages recipients) and their interconnections.

At each communication line, a labeled arrow illustrates the direction of the communication between the two components, and the port used for this communication. The communication can either go in one direction or both directions. However, if the communication goes in both directions, then an open port is required on both sides.

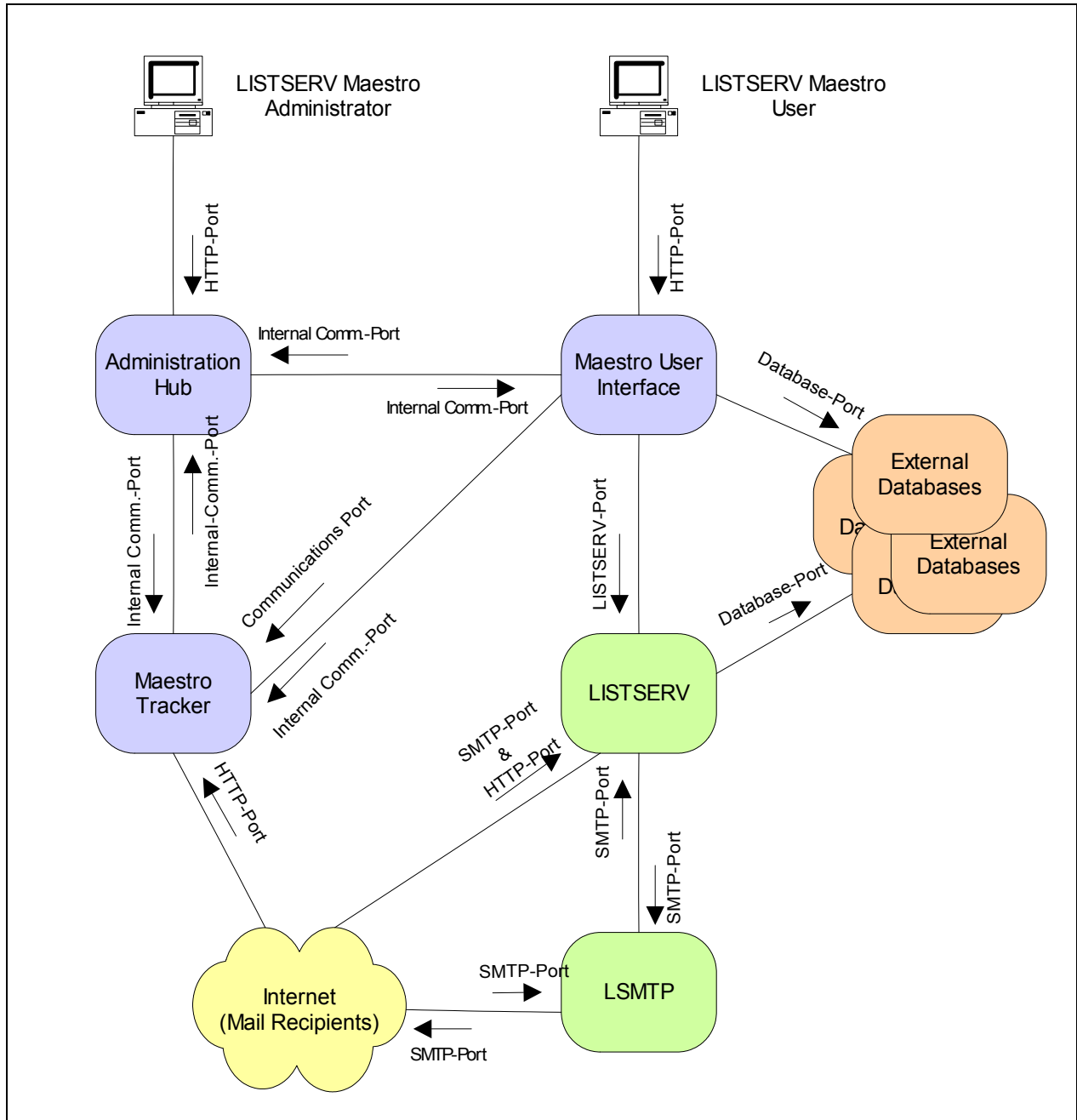
The port label definitions are:

- **HTTP Port** – Used for standard HTTP access, using a Web browser. This is also used to transfer the tracking events from the Internet (from the e-mail messages that were sent) to the Maestro Tracker component. The standard HTTP Port is **80**.

If HTTPS access to the Administration Hub and/or the Maestro User Interface component is being used, then the HTTP Port from the Maestro Administrator to the Administration Hub and/or the HTTP Port from the Maestro User to the Maestro User Interface should be substituted with the **HTTPS Port**, for which the standard is **443**. (This does not apply for the HTTP Port between the Internet and Maestro Tracker, which can never be replaced by the HTTPS Port).

- **SMTP Port** – Used for standard SMTP communication, during the sending and receiving of e-mail. The standard SMTP Port is **25**.
- **Internal Communication Port** – Used for communication between the separate LISTSERV Maestro components and the Administration Hub. The standard Internal Communication Port is **1099**.
- **Communications Port** – Used for special communication between the Maestro User Interface and the Maestro Tracker component to transfer tracking events to the Maestro User Interface component (for reports). The standard Communication Port is **7000**.
- **LISTSERV Port** – Used by the Maestro User Interface component to access the external LISTSERV component. The standard LISTSERV Port is **2306**.
- **Database Port** – Used by the Maestro User Interface component to access the external database component. The standard Database Port depends on the database used.

Figure 49 Component Communication Pathways



All the components shown in the figure (except for the “Internet”, “Maestro Admin” and “Maestro User”) may reside on a single server or may be distributed over different servers, up to the maximum distribution of a dedicated server for each of the components shown.

When two components are installed on the same server, a firewall will not stop the communication between the two (except if the firewall is installed on the same server, where the firewall closes the ports the components use to communicate). However, if some components are installed on separate servers, a firewall may sit between the two. Most commonly a firewall

will separate the “Internet” from the other components. The other components may also be installed in a way that has a firewall between them.

Imagine the firewall as sitting “on top” of the connection between two components.

If that is the case, then the firewall must be configured so that it allows communication between the two components, as specified by the arrow(s) associated with the connection the firewall guards. The direction of the arrow shows the direction the port should be opened, and the label of the arrow defines which port needs to be open.

For most components, the safest method will be to open the firewall for only the required port(s) in the required direction(s), and between the IP addresses of the servers where the components reside.

For example, if there is a firewall between the Maestro Tracker and the Maestro User Interface component, open the “Communications Port” and the “Internal Communications Port” only in the direction from the Maestro User Interface host to the Maestro Tracker host. Open both ports only for the IP address involved. This limits the possible security breaches in the case of an unauthorized person gaining access to one of the component servers.

There are some exceptions:

- If there is a firewall that separates the Internet from the other components (as is advisable), open the HTTP and SMTP ports from the Internet to the respective components as shown in the diagram, and open them for all incoming IP addresses, not just for a specific one. Also, it is necessary to open the SMTP port for outgoing communication originating from the LISTSERV[®] and LSMTP[®] servers.
- Similarly, if there is a firewall separating the Internet from the other components as described above, and both the Maestro Administrator and the Maestro User need to be able to connect to LISTSERV Maestro from the Internet as well as the local intranet behind the firewall, then the HTTP port to the Administration Hub and Maestro User Interface components for all incoming IP-addresses must also open. In this case, LISTSERV Maestro’s login security will be relied upon to disallow unauthorized access to these components.

Allowing the Application Server Shutdown Port, (default 8007) access through the firewall is not a concern, as this port is only ever used locally for communication between two processes on the same server. If there is a firewall on the server itself, this port might also have to be opened. Simply check if the “L-Soft Tomcat” server still reacts to the “Stop” command. If not, then the port needs to be opened.

Section 16 Restricting Access to Components

The administrator can restrict access to LISTSERV Maestro in two different ways. The first way of restricting access is based on the IP address of the computer where the browser is running that is used to access the component. The second way of restricting access is to disallow concurrent access with the same user account. This will limit users from logging in twice with the same user account at the same time.

16.1 IP Address Restrictions

Each of the LISTSERV Maestro components (Administration Hub, Maestro User Interface, and Maestro Tracker) can be configured to restrict access based upon the IP address of the computer where the browser/e-mail-client is running that is used to access the component. This means that it is possible, for example, to define that everyone (all IP addresses) is allowed to access the Maestro Tracker component, but only certain IP addresses (a local subnet, perhaps) are allowed to access the Maestro User Interface and Administration Hub components. If access is not allowed for a certain address, then a client from that address will receive a “403: Forbidden” error when attempting to access the restricted component.

By default, no component access restrictions are in effect. To add access restrictions, it is necessary to add a new `<RequestInterceptor>` entry into the file:

```
\Program Files\Application Server\conf\server.xml
```

This entry must appear the same as Figure 50 below.

Figure 50 Request Interceptor Entry

```
<RequestInterceptor  
  className="com.lsoft.lib.servlet.SourceIPInterceptor"  
  allowedSubnets="SUBNETS_HERE"/>
```

Replace "SUBNETS_HERE" with the component name, IP address of the subnet, and the subnet mask in the exact form described below.

Add this new entry at the end of the `server.xml` file, just before the closing `</ContextManager>` tag.

Stop and restart LISTSERV Maestro after editing the `server.xml`, to make the changes effective.

If the `RequestInterceptor` is not present in the `server.xml`, then access to all LISTSERV Maestro components is unrestricted, except for password input. This is the default after installation. If the `RequestInterceptor` is present, then access to the LISTSERV Maestro components is restricted (in addition to normal password input).

To set up restrictions in the `RequestInterceptor`, replace “SUBNETS_HERE” as shown in Figure 47, with a description of each subnet and what components it will have access to. The listing of the subnets and accessible components must adhere exactly to the following rules:

- No spaces or other white space (including line breaks) is allowed anywhere in the list.
- A component/subnet definition has exactly three parts, of the form “COMPONENT:NETWORK/MASK”, where:
 - “COMPONENT” is the name of the component, in lower case, either “hub”, “lui” or “trk”.
 - “NETWORK” is the dot-separated IP address of the subnet (such as “192.168.1.0”).

-
- “MASK” is the dot-separated subnet-mask for that subnet (such as “255.255.255.0”).

This example, “lui:192.168.1.0/255.255.255.0” would grant access to the Maestro User Interface component to all computers with IP addresses 192.168.6.0 through 192.168.6.255.

- It is possible to have several component and/or subnets defined, but they must be separated by comma “,”.

Any component/subnet definition that is not present in SUBNETS_HERE will not have access to any component. On any server where RequestInterceptor exists in the server.xml, at least one subnet/mask for each component that is running on that server must be specified. Otherwise, the component will be totally inaccessible.



Important: Because of the way it functions (by accepting tracking events from e-mail sent all over the Internet), the Maestro Tracker component should be accessible to everyone. If access is restricted on the server where the Maestro Tracker component is running, then always include “trk:0.0.0.0/0.0.0.0” in SUBNETS_HERE, which will grant access to Maestro Tracker to every address.

Each component may appear several times if it is necessary to grant access to that component to several subnets.

Here are some examples:

To grant access to the Maestro User Interface and Administration Hub for just the computers on a subnet 192.168.1.0 with mask 255.255.255.0, while granting access to Maestro Tracker for everyone, the RequestInterceptor would look similar to Figure 51.

Figure 51 Request Interceptor Example

```
<RequestInterceptor
  className="com.lsoft.lib.servlet.SourceIPInterceptor"
  allowedSubnets="lui:192.168.1.0/255.255.255.0,
  hub:192.168.1.0/255.255.255.0,trk:0.0.0.0/0.0.0.0"
/>
```

Note: In a real RequestInterceptor no white space or line breaks are allowed.

To grant everyone access to the Maestro User Interface and Maestro Tracker, but only grant access to the Administration Hub to two specific machines with the IP addresses 1.2.3.4 and 5.6.7.8, the `RequestInterceptor` would look similar to Figure 52:

Figure 52 Request Interceptor Example

```
<RequestInterceptor
className="com.lsoft.lib.servlet.SourceIPInterceptor"
allowedSubnets="lui:0.0.0.0/0.0.0.0, hub:1.2.3.4/255.255.255.255,
hub:5.6.7.8/255.255.255.255, trk:0.0.0.0/0.0.0.0"
/>
```

Note: In a real `RequestInterceptor` no white space or line breaks are allowed.

After the modified `server.xml` has been saved, stop and restart LISTSERV Maestro to put the changes into effect.

Note: If components of LISTSERV Maestro are distributed on several servers, then it may be necessary to include the `RequestInterceptor` entry in the `server.xml` file of several of these servers, depending on which components are being restricted. For example, if all three components are installed on separate servers, typically a `RequestInterceptor` would not be added on the Maestro Tracker server (since Maestro Tracker needs to be accessible to all), but the Administration Hub and the Maestro User Interface server might have `RequestInterceptors` added to the `server.xml` to restrict access.

16.2 Disallowing Concurrent Access with the Same User Account

The administrator has the option of allowing or disallowing users to log in twice with the same user account at the same time. The default setting does allow concurrent access. To change the default to disallow concurrent access, go to the “*General Administration*” section of the Maestro User Interface, in the Administration Hub and check the corresponding option.

Figure 53 Multiple Logins

General Administration of Maestro User Interface

General Settings

Backup folder: (Leave empty for default: "backup".)

Number of previous backups to keep:

Event transfer interval (from Maestro Tracker): min.

Job archive folder: (Leave empty for default: "archive".)

Log Level

Only log severe messages.

Log severe and standard operational messages.

Log all messages.

Runtime Administration

Multiple Logins: Disallow multiple logins with the same user account. **Check this box to disallow multiple logins from the same user account**

Outbox: Sending is disabled.

Login Access: LISTSERV Maestro User Interface is locked.

Message that will be shown instead of login page while login is locked:

Message that will be shown at top of each page while login is locked:

OK Cancel

Disallowing concurrent access will affect the behavior of the Maestro User Interface. If a user logs in with a certain account, and another user is already logged in with the same account, the system will not accept the second login right away, but will instead do the following:

- If the second login attempt comes from a different workstation, the user attempting the second login is given the message “Logion failed: *Someone is already logged in with the given account from a different workstation. Please use a different account for login.*” The user is not logged in. However, the user may still use a different account (which is not currently in use) to log in.
- If the second login attempt comes from the same workstation, the user is informed that a previous session is already active from the same workstation. The user is then asked whether to cancel the second login, or proceed with the second login and log out of the previous session. If the user cancels the second login, the previous session will be unaffected, but the second login attempt will fail. If the user does not cancel the second login, the previous session will be logged out and the second session will log in.

A second login attempt from the same workstation may happen in situations similar to these:

- A user has one browser window open, in which the first login session is active. The user opens a second window and tries to log in again with the same account. In this case, the user will be notified that there still is a session open from the workstation and that proceeding with the second login will log out that first session. Most users will probably cancel the second login instead and continue using the first session.
- A user has been using a first login session in a browser and has closed the browser without logging out properly. Since the system has no way of knowing that the user has closed the browser, it will still keep the user’s login session active. And since the browser is closed already, the user has no way of “going back” to that session to log out properly.

This is usually not a problem, since the system will log out the session automatically after a certain timeout period has passed (usually 90 minutes). However, if in the meantime the user opens a new browser window and tries to log in again with the same account, the user will be notified that there is already a session logged in from the workstation, and that proceeding with the second login will automatically log out that first session. Since the first session is the one that the user no longer has access to, the user will proceed with the second login.

The determination if a second login attempt comes from the same or from a different workstation is made by looking at the IP address of the workstation used to make that attempt.

This approach has some caveats to be aware of:

- If a group of users are accessing the Maestro User Interface using a local subnet with local addresses, and a router with NAT (Network Address Translation) or some other method of address mapping is used to connect to the Internet, and the Maestro User Interface is on the “other” side of that router, then to the Maestro User Interface, all users will appear to be using the same workstation, since they will all have the same IP address, namely that of the router.

In this case, the Maestro User Interface will handle all login attempts as if they were originating from the same workstation, which may result in the following confusing or even harmful

situation. One user is logged in with an account from workstation A. Now another user tries to log in with the same account, only from workstation B. Both workstations will appear to the Maestro User Interface as one and the same, since both will be using the same IP address externally. The result is that the second user will be notified that there is another session already active from the workstation with the same account. The user will have the option of proceeding with the login and canceling the “previous” login. This other session would in fact be the session of the first user and by logging in, the second user would log out the first user, disrupting the workflow.

To work around this situation, make sure that all users are using different accounts, and that the passwords are kept secret, so that no other user can use a colleague’s account to log in from a different computer and thus log out that colleague.

- If a user is connected to the Internet with a dial-up modem connection as provided by most ISPs, the workstation’s IP address is usually assigned dynamically each time the user connects, meaning a different IP address will be assigned each time a connection is made. This may cause the following situation to happen:

The user opens a browser and logs into the Maestro User Interface with a certain account. The user then closes the browser without logging out properly, so that the session will continue to be active until the timeout has expired. The user then disconnects the Internet connection. Shortly thereafter, the user reconnects to the Internet, opens another browser, and tries to log in with the same account. This time, the user is very likely to be assigned a different IP address from the previous connection. The Maestro User Interface will interpret this as a different workstation logging in to the same account. As a result, the Maestro User Interface will report that the account is currently in use from a different workstation and will not accept a login with that account.

The user now has no choice but to wait for the 90 minutes timeout to expire, before logging in again with the same account. To cancel the previous login, the user would have to access the Maestro User Interface using the same IP address as before, which is extremely unlikely with this kind of dynamic address assignment. To avoid this problem, the user should always remember to log out properly. If the browser is closed accidentally without logging out, but before the modem is disconnected, a new browser session should be opened so that the user can log in again, canceling the previous session, and then log out properly.

To moderate this problem, the administrator may configure the session timeout of the Maestro User Interface to be shorter than the default of 90 minutes, so that in the worst case, the user does not have to wait for that long to log back in.

The timeout for the Maestro User Interface is configured in the following file:

```
\Program Files\L-Soft\webapps\lui\WEB-INF\web.xml
```

Figure 54 XML Entry for the Session Timeout

```
<!-- 1.5 hrs session timeout -->
<session-config>
  <session-timeout>90</session-timeout>
</session-config>
```

The value of "90" determines the session timeout in minutes. Set it to a suitable value, save the file and restart the Maestro User Interface.

The same setting can be changed for the Administration Hub by editing the file

```
\Program Files\L-Soft\webapps\hub\WEB-INF\web.xml
```

Section 17 Securing Access With SSL

As described in the section regarding the use of non-standard ports and installing behind a firewall, the LISTSERV[®] Maestro components can be configured in a way that users and/or administrators can access the Maestro User Interface and/or the Administration Hub with a Web browser from anywhere on the Internet. This feature allows, for example, LISTSERV Maestro to be set up in an ASP-environment, where the customers access the application over the Internet.

Providing access to users from the Internet exposes the risk of unauthorized access. LISTSERV Maestro uses password authentication as a first barrier against intruders. However, network traffic is a public affair. Anyone with the right knowledge and access to certain nodes in the network may eavesdrop on the communication between the user's browser and the LISTSERV Maestro server. Intruders may gain knowledge about the data that is sent to the user's browser (for display) and sent back to the server (to trigger a certain action or to submit settings the user made). Even more dangerous, the intruder could find out the user name and password that the user or administrator employs for login, and could then log him/herself in with the same account.

If security is a concern, consider securing access to the LISTSERV Maestro servers with encrypted communication, so that intruders cannot listen in on the communication between browser and server, and cannot gain knowledge about the data exchanged or spy out passwords. All standard browsers support encrypted communication using Secure Sockets Layer (SSL), and the HTTPS protocol to access Web pages, instead of the normal HTTP protocol.

LISTSERV Maestro also offers the possibility of using SSL for communication with the Administration Hub and/or the Maestro User Interface components. Since topics such as encryption, server certificates, and trusted authorities are so complex, an introduction is presented in Section 17.1 [Introduction to Secure Communication](#) to assist understanding the concepts involved, making the execution of the required steps easier. Implementation instructions start in Section 17.2 [Which Components Should Be Secured?](#)

Securing access with SSL (HTTPS) as described in this section is a separate issue from authenticating and encrypting communication between the components of LISTSERV Maestro, even though the two have many similarities and can even be combined. To authenticate and encrypt the communication between the separate components of LISTSERV Maestro please contact L-Soft Support and request the white paper "Authenticating and Encrypting Communication Between LISTSERV Maestro Components".

17.1 Introduction to Secure Communication

This section is intended to provide a short introduction about the basics of secure communication. Please see the many publications about this topic for more details.

Basically, for successful encrypted communication to take place one partner holding an “encryption key” encrypts the data. It is transferred to the second partner and decrypted using the same “key”. One requirement is that both communication partners know the encryption key, so that the receiving partner may decrypt the data that was encrypted by the sending partner.

With online communication, however, this is more complex. Both partners (the browser and the server) are most likely communicating with each other for the first time, and do not have a common encryption key that is known only to them. So, when the connection is first established, the two partners must secretly decide at the spur of the moment on an encryption key that will be used for the rest of the communication (this is a simplified view of the matter, but it explains the basics).

Assuming that both partners have decided what key to use, they can now communicate in an encrypted manner. There is still the problem of being sure that each partner is actually communicating with the partner they think they are communicating with. An analogy to this problem can be found in real life. Let’s say that two employees of two partner companies meet in a hotel to exchange confidential information. The two have never met each other, but they know each other’s names and home addresses. How can each of them be sure that the other person they meet in the lobby of the hotel is actually the person they are supposed to meet and not an impostor?

An impostor could act as a “man-in-the-middle”. He meets with employee A of corporation A-Corp in the lobby and poses as employee B of corporation B-Corp. Thus, he gains confidential information from A and goes into the bar where he meets the real employee B. Here he poses as employee A from A-Corp, gives the confidential information from the “real” A to B and receives similar information back from B. Finally he goes back into the lobby relays the information he received from B to the “real” employee A. On his way from the lobby to the bar and back, he made copies of the information he was carrying. In the end, both employee A and B are unaware that they did not talk to their “real” counterparts, but to an impostor that acted as a “man-in-the-middle”, and the impostor goes back to his employer C-Corp with the confidential information he gained from their competitors.

On a network, this “man-in-the-middle” attack is even easier to mount. The only thing that a server and a client know of each other is their network addresses, which can easily be forged. In real life, the two employees of A-Corp and B-Corp would probably request to see some picture ID with name and home address of their communication partner. They would then compare the picture on the ID with the person they are talking to and verify that the name and address on the ID matches the ones they have previously been told. If the ID matches the person, they would be confident that they are talking to the right person.

But, in doing so, they actually implicitly trust a third party that has not yet been involved. This would be the agency that issued the picture ID. By accepting the ID, they trust that the agency has created an ID that it is hard to forge. They also trust that this agency has, in turn, verified that the person they issued the ID to really is the person he claims to be. If employee A had tried to use his library card for identification, then employee B would probably have rejected it as improper identification, because she would not trust either that the clerk in the library responsible for issuing the ID really did a thorough check of A’s identity, or she did not trust the security features of the ID, (these days anyone can create an authentic looking ID with the help of a color laser printer). Instead she would probably request a “proper” ID like a passport or driver’s license.

With online communication, the problem of identifying the communication partner is solved very similarly. The role of a “picture ID” in real life is fulfilled by “certificates” in the online world. A certificate asserts that the owner of the certificate is, in fact, the entity it claims to be. For example, a certificate could assert that the server with the host name “`host.somecorp.com`” actually is a server that belongs to SomeCorp, and that it is not an impostor’s server.

How can such credibility problems be solved? Simply falsifying a file that states, “Yes, the server ‘`host.somecorp.com`’ is indeed a server belonging to the SomeCorp Corporation,” would not be cumbersome for an imposter. To guard against this, the certificate is digitally signed by a trustworthy authority, so that it now reads, “Yes, the server ‘`host.somecorp.com`’ is a server belonging to the SomeCorp corporation, and we, the people from TrustCorp have verified that this is indeed so.”

The digital signature is very useful because it prevents anyone from tampering with the certificate. If even a single letter (or byte) in the text of the certificate is changed, the signature will no longer match and the certificate will be invalid. However, a last problem remains: how to test the validity of the signature? The digital signature of the certificate was created using a signature key. The signature key consists of two parts, a private key and a public key. The signer (the signing authority) uses both parts to create the signature. The private key is held secret by the signer so that only the signer is able to use it to create a signature and a signature cannot be created with the public key alone.

The public key on the other hand is made public. It can be used by anyone who desires to test the validity of a digital signature that is supposed to come from the owner of the public key. With a certain algorithm, the signature is tested against the public key, producing a result that states (if the signature was valid): “Yes, the data signed by this signature has not been tampered with and it was signed with a private/public key pair, where the public key matches the public key that was used to test the signature.”

If the signature was not valid, the result could be, “The data was tampered with since it was signed,” in which case the data seen by the recipient is not the original data that the signer saw. Or, the result could be, “The data was signed with a private/public key pair, where the public key does not match the public key used to test the signature.” In this case the data was signed by someone else than the owner of the public key the recipient has. In both cases the signature is invalid.

It is not possible to simply use any public key that is found anywhere (or given by any one), because who would then guarantee that the public key received really is a key from the entity it supposedly belongs to? The origin of the public key that is used to verify the digital signature of a certificate has to be very reliable, otherwise, the “man-in-the-middle” would still have a chance to spy. The intruder would create his own public/private keys with a forged name of “TrustCorp” and his own certificate with a forged host name of SomeCorp. Then he would use his own private key to sign the certificate and would give others the public key claiming, “This is the public key of TrustCorp”. If this public key were used to check the validity of the forged certificate, a match would be made leading to the belief that the forged certificate is legitimate. As a result, the attacker would receive the communication and not the server of TrustCorp.

To verify a public key of the signing authority, most Web browsers, like Microsoft® Internet Explorer, are already equipped with a list of trusted so called “root certificates.” It is not necessary to verify that these certificates indeed come from the entity they claim to, because the browser vendor has already verified this.

The full trust-chain when a browser is used to access a secured is described as follows:

- The browser vendor receives root certificates from the signing authorities, verifying their validity.
- The browser vendor trusts that the root certificates are genuine.
- The browser trusts any signed certificate with a genuine certificate traceable to one of the trusted root certificates. This can be a very short chain such as, for example, “a certificate signed with a root certificate” or a long chain such as for example, “a certificate signed with a certificate that was signed with a certificate ... etc. ... that was signed with a root certificate.”
- The browser trusts any server that has a browser-trusted certificate.

In the real life example, employees A and B both needed picture IDs to verify each other. With online communication, this verification is often only one-sided. For most purposes it is enough that the client is certain about the server it communicates with. It is usually not required that the server is also certain about the client. Therefore, usually only the server has a certificate (which is, down the trust chain, signed by a trusted root certificate) and the client does not.

There are also real-world examples of this. If a car were purchased privately from its former owner, the buyer would most likely request to see a picture ID of the owner during the transaction. Otherwise she would risk unknowingly buying a stolen car. On the other hand, it is not a requirement for the former owner to see the buyer's ID.

To summarize the concepts introduced:

- **Server Certificate** – This certificate asserts that a certain server (with the given host name) actually belongs to a certain organization, so that the server can be trusted and confidential data can be safely communicated. This certificate is digitally signed to prevent tampering and falsification.
- **Trusted Root Certificate** – The trusted root certificate is used to sign the actual server certificate (or another certificate down the trust-chain is used to sign the actual server certificate). Usually the fact that a root certificate is installed together with trusted software (like the browser) already makes it a trusted root certificate. A root certificate can be received by other means (by e-mail, for example). In that case, first verify the certificate before it is rated as “trusted.” To do this, compare the fingerprints on both the sent and received certificates.
- **Encrypted Communication** – This is made possible with the help of an encryption key, which is secretly generated when the communication first begins. Verifying that there is no “man-in-the-middle” while negotiating the encryption key is achieved by verifying the communication partner's certificate and matching its digital signature, to one of the trusted root certificates, further down the trust-chain.

17.2 Which Components Should Be Secured?

Only the Maestro User Interface and/or the Administration Hub component should be secured with SSL - never the Maestro Tracker component. The Maestro Tracker component always requires use of normal HTTP; it cannot be configured to use HTTPS (because the collection of the tracking events needs to be fast, HTTPS is too slow for this).

As all components installed on one server share the same access method, it is necessary to select the access method for all components simultaneously. Therefore, if it is desired to secure the Administration Hub and/or Maestro User Interface components with SSL, they must be installed on a separate server (or separate servers) from the Maestro Tracker component (however, both may be on the same server, as long as they are both secured). Similarly, if only one component is to be secured (either the Administration Hub or the Maestro User Interface), then each component has to be secured on a separate server. This will permit security of one independent of the other.

17.3 Obtaining and Installing a Server Certificate

To enable LISTSERV Maestro to use HTTPS via SSL, obtain a signed server certificate for the server to be secured. It is not possible to simply obtain any server certificate and use it on any server. The certificate is always bound to the explicit server name that was chosen when the certificate was created. If the LISTSERV Maestro component is moved to a different server (with a different name), or the server is renamed, then a new certificate for the new name would have to be obtained.

Obtaining a server certificate involves three basic steps:

- Create an unsigned certificate with the name of the server being secured.
- Create a certificate-signing request (CSR) from that certificate and send it to a certification authority (CA). The CA first verifies that the requester is genuine, and then returns a signed version of the certificate to him/her.
- Replace the unsigned certificate with the signed certificate returned by the CA.

Certificate administration happens with a command line tool called “`keytool`”, that is installed together with Java. For more information about this tool, and further discussion about certificates and secure communication, see the relevant documentation at Sun’s Web site:

<http://java.sun.com/j2se/1.4/docs/tooldocs/win32/keytool.html>

17.3.1 Securing the Trusted Root Certificate Keystore

As a first step when starting to use certificates, be sure to secure the default keystore for trusted root certificates that is shipped with Java. The Java version that is installed together with LISTSERV Maestro includes a keystore that already contains trusted root certificates from some CAs (for example VeriSign and Thawte) This keystore is initially protected with the default password “`changeit`”, which should be changed as soon as possible after the installation of LISTSERV Maestro.

To change the password of the default keystore, execute the following command:

```
HOME\j2sdk1.4.0_01\jre\bin\keytool -storepasswd  
-keystore HOME\j2sdk1.4.0_01\jre\lib\security\cacerts
```

with the following replacement:

HOME: The installation folder of your LISTSERV Maestro, usually something like “\Program Files\L-Soft\Application Server”. (Note, that “*HOME*” needs to be replaced twice in the command shown above.)

You will be queried first for the old password (which is “changeit” if it has not been changed since installation of LISTSERV Maestro), and then twice for the new password. You need to enter a new password with at least six characters, but longer and complex passwords are safer.

17.3.2 Creating an Unsigned Server Certificate

In Java, all certificates are stored in a “keystore,” which is usually a special file protected with a password.

To add a certificate to a keystore, execute the following command:

```
HOME\j2sdk1.4.0_01\jre\bin\keytool -genkey -alias NAME -validity DAYS
-keystore KEYFILE -keyalg RSA
```

with the following replacements:

HOME: The installation folder of LISTSERV Maestro, usually something similar to:

“\Program Files\L-Soft\Application Server”.

NAME: The name of the certificate. Can be any name that is not already in use in the keystore file specified (see below), but choose an informative name that helps in recognition of the certificate at a later time.

DAYS: Limits the validity of the certificate. The certificate will expire so many days after the day it was created. Can be any number of days. Usually, when the signing service from the CA is purchased, only a limited period during which the certificate shall be valid is paid for. Choose a number of days for this parameter, which is no shorter than the period purchased from the CA (a little padding here is probably a good idea, to be on the safe side). It is also possible to create a certificate that has a very long validity period (several years), if desired.

KEYFILE: The keystore file to which the certificate shall be added. Can either be a relative or a full path name. If the file doesn’t exist, it is created. If it already exists, a certificate with the given “*NAME*” is added to it.

Choose a suitable location and file name for the keystore file that takes into account the special security considerations for this file as outlined below.

Be very careful with the keystore file into which the certificate has been created. Protect this file in two respects:

- Do not “lose” or accidentally delete this file, as it contains the certificates. New certificates would have to be purchased in this event. Keep a backup at a safe location.
- Protect the file against unauthorized access. Even though the file is password protected, passwords can always be cracked, and an attacker could thus gain access to the certificates.

The tool will first prompt for the entry of the password with which the keystore is protected. If an existing keystore is being used, enter its password. If a filename of a keystore that does not yet exist is given, then a new keystore will be created and it will be protected with the password that was entered at the first prompt (choose a password with at least six characters, remembering that longer and more complex passwords are safer).

Next, the tool will prompt for the following information values. Press `RETURN` each time to simply accept the default value "Unknown". However, some values must be entered for the certificate to work and some CAs require other values are filled out. So it is generally a good idea to fill out all values with whatever fits best in each case (see below):

"What is your first and last name?"

Here, the host name of the server to be secured with the certificate being created must be entered. Yes, even though the question reads "your first and last name," it is necessary to enter the host name of the computer instead! This should be the same host name that will be used in the URLs to access the server. For example, if the URL is "http://maestro.mycorp.com/lu1", then enter the host name "maestro.mycorp.com" (without the quotes).

"What is the name of your organizational unit?"

"What is the name of your organization?"

"What is the name of your City or Locality?"

"What is the name of your State or Province?"

"What is the two-letter country code for this unit?"

Use the two-letter code that fits the country where the server is deployed, like US, DE, SE, CH, and so on.

After the last question is answered, a summary of the input and a request for confirmation will appear. Type "yes" and `RETURN` to accept the input, or "no" and `RETURN` (or simply `RETURN`) to reject it (in this case enter the values again until they are satisfactory). After the input is confirmed, the tool takes a few seconds to generate the certificate. When it is done, enter a password at the prompt to protect the certificate. Although generally any password is usable, for the certificate to be usable with LISTSERV Maestro, the same password chosen for the keystore itself must be used. To do so, simply press `RETURN` without entering anything, so that the default is accepted.

At this point, the certificate has been created, but it is as yet unsigned.

17.3.3 Performing a Certificate Signing Request (CSR)

Once an unsigned certificate has been created, generate a certificate-signing request (CSR) from it, which can then be submitted to a certification authority (CA), for example VeriSign.

To generate a CSR for a certificate in the keystore, execute the following command:

```
HOME\j2sdk1.4.0_01\jre\bin\keytool -certreq -alias NAME -file OUTFILE  
-keystore KEYFILE
```

with the following replacements:

HOME: The installation folder of LISTSERV Maestro, usually something similar to: “\Program Files\L-Soft\Application Server”.

NAME: The name of the certificate. This must be the name of the certificate that the CSR is created for (the same name that was specified when the certificate was created).

OUTFILE: The file into which the CSR will be written. If the file already exists, it will be replaced with the new file. Can either be a relative or a full path name.

KEYFILE: The keystore file in which the certificate is stored. Can either be a relative or a full path name.

The command will request the password of the keystore. After it is entered, the file specified as “*OUTFILE*” will be written. This file is a text file that contains the CSR in Base64-encoded form. An example of this file is shown in Figure 55.

Figure 55 Example of Base64 Encoded Outfile

```
-----BEGIN NEW CERTIFICATE REQUEST-----
tPnJhsLOuocsBYAmyM11qiZ5BEVWAnJfZ6kyN/Xft5NFxGIy9Uynz5kODfBwFUgiu98iQKWyMK
C/bGFuZ2VuMQ8wDQYDVQQKEwZMLVNVZnQxEDAObgNVBAsTB1Vua25vd24xDzANBgNVBAMTBnRl
cHBp6E7Zyl9wkPyVpn1qbnbtXQGAablJIInE9/LruaJ1NX1f/NVJgL4vPiDKsU4laGvJHBNhdj+
F0uVb3SIb3DQEBBAUAA4GBAB6XqdfJvhy7dThijsHjw+c4ELQFI/TkHBvgp5NaCccQoNwwW9ln
IeOikDb2lwWg56G6LiYfpVBss5+OOW2jXlq9CdNw1KLSDQ+kMtZjdVr8+iQ9gsqxvskCAwEAAa
AAMA0GCSqGMIIBpjCCAQ8CAQAwZjELMAkGA1UEBhMCREUxEDAObgNVBAGTB0d1cm1hbnkxETAP
BgNVBAcTCEVYyZCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAz+hQRsqDWRLvmV4YD5+JaQ
EXn5qqJeyzkfg2PQoU2VPgHID0VnyTpt8r/t4uFk8p1NxjYkC4
-----END NEW CERTIFICATE REQUEST-----
```

Now submit this CSR to the desired CA. For example, VeriSign offers an online order form that contains a field into which the text from the CSR can be simply pasted. Other CAs may do this differently – please ask the CA for help if there is any question, or if anything is unclear. After the CA has received the CSR, it will first verify that the requester or company is indeed genuine, that is if the content of the certificate can or cannot be trusted. This usually happens using methods such as making phone calls, checking company registrations, or other types of research, and may take a few days. Once the CA has verified the validity of the certificate, it will either be returned as a signed certificate, or instructions on how to obtain the signed certificate will be supplied.

17.3.4 Installing the Signed Server Certificate

The signed certificate received back from the CA must be in X.509 format, either in binary or Base64 encoded form (please contact the CA if the certificate received does not match either of these formats). Once the certificate has been received, store it into a file (usually “*.cer”). Then execute the following command:

```
HOME\j2sdk1.4.0_01\jre\bin\keytool -import -alias NAME -file INFILE -
keystore KEYFILE -trustcacerts
```

with the following replacements:

HOME: The installation folder of LISTSERV Maestro, usually something similar to: “\Program Files\L-Soft\Application Server”.

NAME: The name of the certificate. This must be the name of the certificate that the CSR was made for (the same name that was specified when the certificate and the CSR were created).

INFILE: The file that contains the reply from the CA with the signed certificate.

KEYFILE: The keystore file in which the certificate is stored. Can either be a relative or a full path name.

The command will load the certificate from the given file, check the signature of the signer (the CA) against a trusted root certificate of the CA and, if the signature matches, replace the unsigned version of the certificate that was in the keystore with the signed version.

There is one critical moment here – when the tool tries to check the signature against a trusted root certificate of the CA: If this check cannot be made because such a trusted root certificate of the CA cannot be found, the tool will abort with an error message. In this case, obtain a trusted root certificate from the CA first (see Section 17.3.5. [Installing the Trusted Root Certificate](#) for more details) and then repeat the import step described above. Java is already shipped with trusted root certificates of certain CAs, like VeriSign and Thawte. For other CAs, obtain and install a root certificate first.

17.3.5 Installing a Trusted Root Certificate

This step is only required if the signed server certificate was obtained from a CA for which a trusted root certificate is not already shipped with Java. An error message during the import of the signed certificate will occur if this is the case. The required root certificate should be available from the CA. The certificate must be stored in a file, either in “DER encoded binary X.509” or “Base-64 encoded X.509” format. If there is access to such a certificate file, import it into the keystore with the trusted root certificates by executing the following command:

```
HOME\j2sdk1.4.0_01\jre\bin\keytool -import -alias NAME -file INFILE  
-keystore HOME\j2sdk1.4.0_01\jre\lib\security\cacerts
```

with the following replacements:

HOME: The installation folder of LISTSERV Maestro, usually something similar to: “\Program Files\L-Soft\Application Server”. The replacement folder name and path needs to be entered twice – once for each occurrence of *HOME*.

NAME: The name to be given to the certificate in the keystore. This name is not really important for anything, except for recognition at a later time. Also this name must not yet be in use in the keystore.

INFILE: The file in which the X.509 certificate from the CA is stored.

The password of the default keystore file will be queried for, which should have been set to something other than its default “changeit” earlier. See Section 17.3.1 [Securing the Trusted Root Certificate Keystore](#) for more information. The command will present the details of the certificate to be imported in a way similar to Figure 56.

Figure 56 Imported Certificate

```
Owner: OU=For VeriSign authorized testing only. No assurances (C)VS1997,
OU=www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.,
O="VeriSign, Inc"
Issuer: OU=For VeriSign authorized testing only. No assurances (C)VS1997,
OU=www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.,
O="VeriSign, Inc"
Serial number: 52a9f424da674c9daf4f537852abef6e
Valid from: Sun Jun 07 02:00:00 GMT+02:00 1998 until: Wed Jun 07 01:59:59
GMT+02:00 2006
Certificate fingerprints:
    MD5: 40:06:53:11:FD:B3:3E:88:0A:6F:7D:D1:4E:22:91:87
    SHA1: 93:71:C9:EE:57:09:92:5D:0A:8E:FA:02:0B:E2:F5:E6:98:6C:60:DE
Trust this certificate? [no]:
```

The presentation contains details about the certificate, but these could have been forged. It also contains the certificate's fingerprints, which can be used to verify that the certificate has not been falsified. For example, if the certificate was e-mailed (thus giving a potential attacker the possibility to "catch" the e-mail before it reaches its destination, and replacing the certificate therein with his own certificate for a future "man-in-the-middle" attack), then it is advisable to call the responsible person from the CA, to verify the fingerprint of the certificate over the phone.

Once the certificate is believed to be genuine, answer "yes" and RETURN to the question "Trust this certificate?" After this is done, the certificate is installed as a new trusted root certificate in the default Java root certificate store, and can now be used to import server certificates signed by the CA from which the root certificate was obtained, as described in Section 17.3.4 [Installing the Signed Server Certificate](#).



Internet Explorer comes (as many browsers do) with an extensive list of trusted root certificates. It also allows for those certificates to be exported to a file in the X.509 format required for import by "keytool". Therefore, if a CA is chosen to sign the server certificate for which there is no trusted root certificate already in the Java default keystore, it is very easy to locate a root certificate by exporting it from Internet Explorer as described below. This description is for IE 5.0, 5.5 and 6.0; other versions may vary.

Go to "Tools → Internet Options... → Content tab → Certificates... → Trusted Root Certification Authorities tab" and look for a matching root certificate (many CAs have several of these). This might have to be done by trial-and-error until a matching certificate is found. Select the certificate and click on "Export..." In the export wizard, choose either "DER encoded binary X.509 (.CER)" or "Base-64 encoded X.509 (.CER)" and supply a suitable filename. Next, complete the export. The file that is exported can then be imported into Java's default keystore as described above.

17.3.6 Making LISTSERV Maestro Aware of the Server Certificate

Once the signed server certificate is imported into the keystore file, the LISTSERV Maestro server needs to be aware of this certificate. This is the last step to securing the server.

On the server to be secured with SSL, edit the file "server.xml" in the LISTSERV Maestro installation folder:

\Program Files\L-Soft\Application Server\conf\server.xml

Near the end of the file there is a section labeled “HTTPS (SSL)”. This section contains a connector for HTTPS connections, which is initially commented out (with braces “<!--” and “-->”). Remove the comment-braces around the connector, not around the explanatory comment-text that precedes the connector, to activate it.

Figure 57 Editing the Server.XML File to Remove the HTTP Connector

```
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
  <Parameter name="handler"
    value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
  <Parameter name="port" value="443"/>
  <Parameter name="socketFactory"
value="org.apache.tomcat.net.SSLSocketFactory" />
  <Parameter name="clientAuth" value="false" />
  <Parameter name="keystore" value="TODO:Set path to keystore file!" />
  <Parameter name="keypass" value="TODO:Set to password of keystore
file!" />
</Connector>
```

It is also necessary to edit the values of the parameters “keystore” and “keypass”, which currently contain only “TODO” comments:

- As the value of “keystore”, enter the absolute path to the keystore file (including drive letter) in which the signed certificate can be found. A relative path name cannot be used; the full path to the file must be supplied. The keystore file itself can be stored in any place that seems appropriate, but the “Application Server\commands” folder would be a good choice.
- As the value of “keypass”, enter the password that was used for the keystore (as explained earlier, the same password must also have been used for the certificate).



Important Security Issue: The password to the keystore and the certificate therein are included as plain text in this file. This can be a security breach, if unauthorized persons have access to this file. Therefore, employ the appropriate operating system or file system security measures so that only authorized persons can access this file. This should previously have been done, as this file is integral to the functioning of the server. Tampering with this file, or other files in the “Application Server” folder, may prevent LISTSERV Maestro from working.

The HTTPS-connector is pre-configured to use port **443**, which is the standard port for HTTPS (in comparison to port 80, which is the standard port for normal HTTP). If this port cannot be used, then it is possible to change the port to any other value that is not in use on the server. However, in this case the users will have to enter a URL like “https://server.domain.com:yourPort/lu1” instead, (just as with standard HTTP, if the standard HTTP port had been changed to something other than 80). Finally, comment out or simply remove the normal HTTP connector in the “server.xml” file. Either simply delete it or enclose it in comment braces.

Figure 58 Editing the Server.XML File to Remove the HTTP Connector

```
<!--  
<Connector className="org.apache.tomcat.service.PoolTcpConnector">  
  <Parameter name="handler"  
    value="org.apache.tomcat.service.http.HttpConnectionHandler"/>  
  <Parameter name="port" value="80"/>  
</Connector>  
-->
```

This is necessary so that the server is no longer accessible using normal HTTP. If this is not done, then users could use both HTTPS and HTTP URLs to access the server. As most users are not familiar with the HTTPS availability, most would probably default to the normal HTTP, and all communication would once again be unencrypted – which defeats the purpose of securing the server. Therefore, it is safer to remove/comment out the standard HTTP connector to prevent users from accessing the server with normal HTTP and remind them to use HTTPS instead.

This also explains why it is not possible to secure a server that is running the Maestro Tracker component with SSL: The Maestro Tracker component always requires use of normal HTTP. It cannot be configured to use HTTPS (because the collection of the tracking events needs to be fast, and HTTPS is too slow for this).

As all components installed on one server share the same connectors, a connector type is enabled/disabled for all components simultaneously. Therefore, if it is desirable to secure the Administration Hub and/or Maestro User Interface components with SSL, they must be installed on a separate server from the Maestro Tracker component (however, both components may be on the same server, as long as they both are to be secured).

LISTSERV Maestro is now prepared for SSL access. Start or re-start LISTSERV Maestro and access it normally, except now it is necessary to use HTTPS: URLs instead of the standard HTTP: URLs.

Section 18 Tracking and Recipient Profiles

Among the four tracking types, LISTSERV® Maestro offers two types that involve recipient profiles: personal tracking and anonymous tracking. With personal tracking, each recipient is identified uniquely by a recipient ID that can be traced back to the data associated with this recipient, (the recipient's profile). With anonymous tracking, each recipient is identified with an anonymous ID that cannot be traced back to the actual recipient data, but only to an anonymous profile. This is usually a subset of the actual recipient data that contains only anonymous data, no personal data like name or address is included.

When anonymous tracking is chosen, LISTSERV Maestro always creates and stores an anonymous profile for each recipient. For higher efficiency, if several recipients have the same anonymous profile, only one profile entry is created and this is shared by all of the recipients. The anonymous ID is then included in the tracking data and maps to one of these anonymous profiles stored in LISTSERV Maestro.

The storage of personal profiles is very similar. For each recipient, a profile entry with this recipient's data is created. Usually there will be one entry for each recipient, but should several recipients happen to have exactly the same profile, only one profile entry will be generated and

this will be shared by those recipients. Both anonymous and personal profiles are stored in the Maestro System database. See Section 4 [The System Database](#) for additional information.

Anonymous profiles always need to be created and stored by LISTSERV Maestro, because they simply do not exist anywhere else. However, with personal profiles, this is usually different. The personal profile of a recipient contains the full set of data associated with that recipient. It maps to one row in the uploaded recipients file (in CSV format), or to one row in the result set that was selected from the database. Each column in the row constitutes one field of the profile data, where the column headers from the uploaded file or the database table are the labels of these fields.

For personal tracking, the recipient data must also contain one column with a unique recipient ID – a column with values that can be used to uniquely identify the recipient from all other recipients.

More often than not, the recipient data already comes from some type of database. Either it was exported from the database and then uploaded as a recipients file, or the Maestro User Interface selected it directly from the database (possibly by using a database backed target group). In both cases, there is already a table in a database that contains the full recipients profiles, including the unique recipient IDs. In some cases, when the Maestro User Interface is used with an external system database, and that database happens to be the same database as the one where the recipients originally came from (either by an export or an explicit select in the Maestro User Interface), the original recipient profiles exist in the same database where the Maestro User Interface will store them. So, under certain circumstances, it seems redundant to allow the Maestro User Interface store personal profile information in its database, when the same information already exists in another database (or even in the same database, if the database is shared as explained above).

To avoid this circumstance, the Maestro User Interface offers an option to switch off the storing of personal profiles in the Maestro System Database. To do this, edit the following file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Add this entry:

```
CreatePersonalProfileTables=false
```

If the entry is set to “false”, then the Maestro User Interface will not write personal profiles into its system database. If it is set to “true” (or missing, which is the default after installation), then the Maestro User Interface will create personal profiles. Restart the Maestro User Interface after the change to make the entry effective.

The actual difference between permitting and not permitting the Maestro User Interface to create personal profiles is that if the Maestro User Interface creates personal profiles, then the match between the recipient ID that is collected with the tracking event and the corresponding recipient (that recipient’s profile) can be made directly in the Maestro User Interface.

If the report type “Details Report” is run, the resulting table will have one entry for each recipient for which one of the events selected was registered. Optionally, with a count that details the amount of these events that were registered. One row per recipient is generated, including the recipient’s profile as values in the row, as shown in Figure 59.

Figure 59 Example of Recipients Profile Data Table

```
"Count", "ID", "Name", "EMail", "Age", "ZIP"  
"5", "fred1", "Fred", "fred@flintstone.com", "52", "12345"  
"2", "wilma1", "Wilma", "wilma@flintstone.com", "45", "12345"  
etc...
```

The “count” column is optional.

With this table, it is immediately apparent which recipients reacted to the message (and how often, if the “count” column is included), as the details of each recipient are included in the form of a profile.

If the version of this table without the “count” column is chosen, the same table can also be used, without any modifications, to upload the recipients list for another job (for example to send a follow-up mail to all recipients that reacted to the previous mail). The data is already in the CSV-format that the Maestro User Interface understands, and since all recipient profiles are already in the Maestro User Interface database, the profiles will not be recreated, but instead the existing profiles are reused.

In contrast, if the Maestro User Interface does not create personal profiles, then it is necessary to make the match between the recipient IDs and the actual recipients behind them with a tool outside of LISTSERV Maestro, because the Maestro User Interface does not contain the information to do so itself. To help make this match, the Maestro User Interface will output a table with the recipient IDs in question when the “Details Report” is run. The result is one row per recipient with the recipient’s ID as the value in the row, as shown in Figure 60.

Figure 60 Example of Recipients ID in Data Table

```
"Count", "ID"  
"5", "fred1"  
"2", "wilma1"  
etc...
```

Again, the column “count” is optional.

Here, only the ID’s of the recipients that reacted (and how often, if the “count” column was included) are apparent, but any further details regarding the recipients are not.

This data would have to be brought into context with the original source of the recipients, by whatever reporting or analysis tool preferred to discover more details about the users.

The type of handling of the personal profiles depends on the requirements of the feedback desired:

- If immediate and simple-to-get feedback is desired about those recipients who trigger the events, and there is not much concern about saving storage space (for example keeping possible redundant versions of the profiles in different databases – or even the same database), then choose the option of permitting the Maestro User Interface to create personal profile entries (set the INI-file entry to “true” or leave it out, which is the default after installation).

-
- If there is not much concern about receiving feedback on the identity of the recipients quickly, because the tracking information will be imported into some other tool or database anyway, keeping redundant sets of data is not desired, and there is concern about saving disk space, then choose the option of not storing profile entries in the Maestro System Database (set the INI-file entry to “false”).

The choice between allowing and not allowing the Maestro User Interface to store personal profiles in the system database is really an advanced administration feature. If there is any concern about this choice, keep the default of letting the Maestro User Interface store the profiles. Only change this setting after thoughtful consideration of the requirements and the impact this will have.

Section 19 Editing LISTSERV Maestro INI Files

The following rules apply to the INI-files “lui.ini”, “hub.ini” and “tracker.ini”, which are the configuration files for the Maestro User Interface, Administration Hub and Maestro Tracker components, respectively (the “my.ini” configuration file of the internal MySQL database follows different rules, because it is a third party product. See the MySQL documentation for details):

- All INI-files are text files and assumed to be encoded in the default encoding for the platform being used. For most English/European installations that would be ISO-8859-1 [Latin 1 – Western European].
- In the files, every parameter occupies one line. Each line must be terminated by a line terminator (LF, CR, or CRLF). All lines in the file are processed.
- A line that contains only white space or whose first non-white space character is an ASCII “#” or “!” is regarded as a comment, and its content is ignored.
- Every line other than a blank line or a comment line describes one parameter (except if a line ends with a backslash “\”, then the following line, if it exists, is treated as a continuation line, as described below).
- A parameter always consists of a key and a value. Keys and values are separated by white space or “=” or “:”. Any white space around the separation character is also ignored.
- All remaining characters on the line become part of the associated value. Some characters which otherwise have special meanings, need to be escaped with a backslash. The ASCII escape sequences “\t”(TAB), “\n”(LF), “\r”(CR), “\\”(backslash), “\””(quotation mark), “\'”(apostrophe), “\ ”(space), and “\uXXXX” (where “XXXX” is the Unicode-value of the required character, expressed in hexadecimal format) are recognized and converted to single characters.
- In the case that the last character on a line is a “\”, then the next line is treated as a continuation of the current line; the “\” and line terminator is simply discarded, and any leading white space characters on the continuation line are also discarded and are not part of the parameter value.

Examples:

Each of the following four lines specifies the key "Truth" and the associated value "Beauty":

```
Truth = Beauty
Truth:Beauty
Truth           :Beauty
Truth Beauty
```

The following three lines specify a single parameter:

```
fruits           apple, banana, pear, \
                  cantaloupe, watermelon, \
                  kiwi, mango
```

The key is "fruits" and the associated value is:

```
"apple, banana, pear, cantaloupe, watermelon, kiwi, mango"
```

Note that a space appears before each "\ " so that a space will appear after each comma in the final result; the "\ ", the line terminator and leading white space on the continuation line are discarded and are not replaced by one or more other characters.

As a last example, the line:

```
cheeses
```

specifies that the key is "cheeses" and the associated value is the empty string.

19.1 Maestro User Interface INI-File Entries

The following table shows all possible entries of the "lui.ini" file for the Maestro User Interface component. For any entry that is missing in the INI-file, the corresponding default value is assumed. Changes in INI files requires a restart of the affected component to take effect.

Table 3 Maestro User Interface INI-File Entries

Entry Key	Description
AllowCharsetChoice	<p>Defines if the user is allowed to change the content charset on a job-by-job basis, or if he has to accept the default charset (see “DefaultMailCharset”).</p> <p>Default: true</p> <p>See Section 23.1 Defining the Default Mail Charset</p>
AllowISO-i-Mails	<p>Defines if in out going mail the special bi-directional charsets”ISO-8859-6-i” and “ISO-8859-8-i” will be used instead of their normal Iso-8859 counterparts.</p> <p>Default: true</p> <p>See Section 23.2 Allowing or Disallowing Bi-Directional Character Sets</p>
ClickThroughURL	<p>Path-part of the click-through tracking URL used for URLs without passing of merged parameters.</p> <p>Default: /trk/click</p>
ClickThroughPPURL	<p>Path-part of the click-through tracking URL used for URLs with passing of merged parameters.</p> <p>Default: /trk/clickp</p>
CreatePersonalProfileTables	<p>Defines if full personal profiles should be stored in the system database, when personal tracking is used.</p> <p>Default: true</p> <p>See Section 18 Tracking and Recipient Profiles</p>
DefaultMailCharset	<p>Defines the charset that is to be used as the charset of the content for newly created jobs that are not copies of existing jobs. May or may not be changed by user (see “AllowCharsetChoice”).</p> <p>Default: ISO-8859-1</p> <p>See Section 23.1 Defining the Default Mail Charset</p>

Entry Key	Description
ExternalHostName	<p>Host name and HTTP-port of the Maestro User Interface server as seen by external clients, in the format “host:port” where “:port” can be left out if standard port “80”. To be used if the external host name or HTTP-port of the server is different than the actual host name or port (for example behind a proxy).</p> <p>Default: <i>none</i> (normal host name and port 80 used)</p> <p>See Section 20.3 Setup with Server Name Aliases or Proxy Setup</p>
ExternalHubHostName	<p>Host name and HTTP-port of the Administration Hub server as seen by external clients, in the format “host:port” where “:port” can be left out if standard port “80”. To be used if the external host name or HTTP-port of the server is different than the actual host name or port (for example behind a proxy).</p> <p>Default: <i>none</i> (normal host name and port 80 used)</p> <p>See Section 20.3 Setup with Server Name Aliases or Proxy Setup</p>
Home	<p>Home folder in which work-files are kept.</p> <p>Default: subfolder “lui” in installation folder</p>
HubContext	<p>Context-path part of the user interface access URLs for the Administration Hub component.</p> <p>Default: hub</p>
HubHTTPPort	<p>HTTP-Port of the Administration Hub server.</p> <p>Default: 80</p> <p>See Section 13.2.1 Configuring the HTTP Port</p>
HubRMIPort	<p>Internal communication port (RMI-Port) of the Administration Hub server.</p> <p>Default: 1099</p> <p>See Section 13.2.2 Configuring the Internal Communication Port</p>
MaintenanceMode	<p>Defines if the Maestro User Interface component will run in maintenance mode or not.</p> <p>Default: <i>false</i></p> <p>See Section 8.3 Runtime Administration and System Shutdown</p>
OpenUpURL	<p>Path-part of the open-up tracking URL.</p> <p>Default: /trk/open</p>
RegistryDomain	<p>The domain name with which the Maestro User Interface component stores its settings in the Administration Hub registry.</p> <p>Default: LUI</p>

Entry Key	Description
RegistryHubHost	<p>Host name of the server with the Administration Hub component. Default: localhost See Section 20.2.2 Moving the Administration Hub Component to Another Server</p>
RemoteAdminPassword	<p>Password for remote log file access. Default: none (no remote log file access allowed) See Section 12.1 Remote Log Access</p>
RestoreBackup	<p>Path name of the folder containing the backup that shall be restored during the next startup. Note: This key will be automatically removed from the INI-file during the next startup. Default: none See Section 11.7 Restoring a Backup</p>
RMIPort	<p>Internal communication port (RMI-Port) of the Maestro User Interface server. Default: 1099 See Section 13.2.2 Configuring the Internal Communication Port</p>
TrackerHost	<p>Host name of the server with the Maestro Tracker component. Default: localhost See Section 20.2.3 Moving the Maestro Tracker Component to Another Server</p>
TrackerRMIPort	<p>Internal communications port (RMI-Port) of the Maestro Tracker server Default: 1099 See Section 13.2.2 Configuring the Internal Communication Port</p>

19.2 Administration Hub INI-File Entries

The following table shows all possible entries of the “hub.ini” file for the Administration Hub component. For any entry that is missing in the INI-file, the corresponding default value is assumed. Changes in INI files requires a restart of the affected component to take effect.

Table 4 Administration Hub INI-File Entries

Entry Key	Description
Home	Home folder in which work-files are kept. Default: subfolder “hub” in installation folder
RegistryDomain	The domain name with which the Administration Hub component stores its settings in its own registry. Default: HUB
RemoteAdminPassword	Password for remote log file access. Default: <i>none</i> (no remote log file access allowed) See Section 12.1 Remote Log Access
RMIPort	Internal communication port (RMI-Port) of the Administration Hub server. Default: 1099 See Section 13.2.2 Configuring the Internal Communication Port

19.3 Maestro Tracker INI-File Entries

The following table shows all possible entries of the “tracker.ini” file for the Maestro Tracker component. For any entry that is missing in the INI-file, the corresponding default value is assumed. Changes in INI files requires a restart of the affected component to take effect.

Table 5 Maestro Tracker INI-File Entries

Entry Key	Description
Home	Home folder in which work-files are kept. Default: subfolder “trk” in installation folder
HubRMIPort	Internal communication port (RMI-Port) of the Administration Hub server. Default: 1099 See Section 13.2.2 Configuring the Internal Communication Port
RegistryDomain	The domain name with which the Maestro Tracker component stores its settings in the Administration Hub registry. Default: TRK
RegistryHubHost	Host name of the server with the Administration Hub component. Default: localhost

Entry Key	Description
RemoteAdminPassword	Password for remote log file access. Default: <i>none</i> (no remote log file access allowed) See Section 12.1 Remote Log Access
RMIPort	Internal communication port (RMI-Port) of the Maestro Tracker server. Default: 1099 See Section 13.2.2 Configuring the Internal Communication Port

Section 20 Distributed Components

The three LISTSERV Maestro components, the two external components (LISTSERV and LSMTP), and the optional (for Windows installations) database may be installed on any combination of hosts, from one single host shared by all components to six dedicated hosts, one for each component. If different components are installed on separate servers, it is not necessary that all of the servers have the same operating system. It is possible to install the Maestro User Interface and Administration Hub components on a Windows server and at the same time the Maestro Tracker component on a Linux server (or other combinations). For more information on host restrictions, installing LISTSERV Maestro, and starting and stopping the LISTSERV Maestro service, see the LISTSERV Maestro Installation Manual.

Distributing components has several advantages:

- **Load Distribution** – Processor and disk load is shared between several servers, giving each component more “room” to operate.
- **Separate Maintenance** – All components do not have to be shut down or re-started whenever a maintenance task on one of them requires it. The other components may continue running (of course, when a component that other components rely on is shut down, this is no longer entirely true, since the other components can not run properly while the one component is down).

The Maestro Tracker component has very rigid uptime requirements. This component should constantly be running to be able to collect the tracking data from the messages that are sent. It can only do so while it is running and connected to the Internet. Therefore it is not a good idea to shut down the server on which the Maestro Tracker component is running – this should only be done as a last resort. Other components do not have these strict uptime requirements. To minimize Tracker downtime in the event of maintenance on the tracker components, it is a good idea to have the Maestro Tracker component on a separate server.

For optimal performance for a high-volume installation, a component distribution on five servers is recommended:

- **User-Interface and Hub Server** – Contains the LISTSERV Maestro components Maestro User Interface and Administration Hub.
- **Tracker Server** – Contains the Maestro Tracker component.
- **Database Server** – Contains the Maestro System Database component.
- **LISTSERV Server** – Contains the LISTSERV[®] external component.
- **LSMTP Server** – Contains the LSMTP[®] external component.

20.1 Fresh Installation with Distributed Components

A fresh installation with distributed components is a straightforward operation. To install any of the three LISTSERV Maestro components, simply run the LISTSERV Maestro setup on the server where the component(s) will be installed and then select the required components from the list, while leaving all components to be installed on other servers unchecked. The other external components (database, LISTSERV, and LSMTP) have separate installation kits. Simply execute each application setup on the respective server(s).

20.2 Moving Components to Another Server

It is also possible to move an already running installation or several of its components to other servers. This also applies (in slightly different form) if it is necessary to change the host name of the server where the components are installed.

20.2.1 Moving the Maestro User Interface Component to Another Server

Follow these steps to move the Maestro User Interface Component to another server:

1. As a preparation for moving the Maestro User Interface component, determine which kind of system database you are using:
 - If LISTSERV Maestro is currently using an **external system database**, make sure that the new server will also be able to contact this external database over the network. Also, remember to add the database driver file(s) for that external database to the fresh installation of your Maestro User Interface on the new server (see step 3 and Section 5 [Defining External Database Connections](#) for the driver file(s) needed). In step3, remember to follow the description for the case with an external system database.
 - If LISTSERV Maestro is currently using the **internal system database**, decide if on the new server will continue using the internal system database (which is only available on a Windows server) or if it will to switch to an external system database instead.

To remain using the internal system database, continue with the procedure described here. In step 3, remember to follow the description for the case with an internal system database.

If you decide to switch to an external database, then, abandon the procedure described here and first switch to the new database, as described in Section 4.1 [Configuring the](#)

[External System Database](#). Afterwards, return to here, and proceed as described in the bullet above.

2. Shut down the existing LISTSERV Maestro installation on all servers where components of it are running.
3. For servers that have no existing LISTSERV Maestro components, execute a fresh installation as described in the LISTSERV Maestro installation manual for the server's operating system. During installation select the Maestro User Interface when queried for which components to install. After installation, do not start LISTSERV Maestro.

For servers that already have the Administration Hub and/or the Tracker component installed, start the installation package for the server's operating system as if doing a fresh installation. The installation package will recognize any existing components and present an option to add new components. Select the Maestro User Interface component to add, and proceed with the installation. Install the Maestro User Interface component on the new server. After installation, do not start LISTSERV Maestro.

4. If you are using the internal database, copy the following files and folders (including all files and subfolders) to the new server:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
\Program Files\L-Soft\Application Server\lui\my.ini
\Program Files\L-Soft\Application Server\lui\database
\Program Files\L-Soft\Application Server\lui\luidata
\Program Files\L-Soft\Application Server\lui\registry
```

If an external system database is being used, copy only the following files and folders:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
\Program Files\L-Soft\Application Server\lui\luidata
\Program Files\L-Soft\Application Server\lui\registry
```

This will overwrite some files and folders on the new server. Depending on the installation, these paths may be slightly different on one or both of the servers.

4. If the component is being moved together with the internal database and the installation path on the new server is different than the one on the old server, it will be necessary to edit the file `my.ini` on the new server.

In the "[mysqld]" section of the file, make sure that the following entries correctly point to the equivalent folders on the new server that corresponds with the ones they pointed to on the old server:

```
basedir=...
datadir=...
innodb_data_home_dir=...
innodb_log_group_home_dir=...
innodb_log_arch_dir=...
```

Remember that this step is only required if the component is being moved with the internal database.

On the old server, remove the previous installation of LISTSERV Maestro.

For a server with Windows, use Windows' "Add/Remove Programs" panel to start the maintenance setup of LISTSERV Maestro. In the setup, choose "Modify" and deselect the Maestro User Interface component, so that it is uninstalled.

For a server with Linux, start the installation package the same way as if performing a fresh installation. The installation package will recognize the existing components. Select the Maestro User Interface component to be removed and proceed with the uninstallation.

Start LISTSERV Maestro on all servers

20.2.2 Moving the Administration Hub Component to Another Server

Follow these steps to move the Administration Hub to another server:

Shut down the LISTSERV Maestro installation on all servers where components are installed.

For servers that have no existing LISTSERV Maestro components, execute a fresh installation as described in the LISTSERV Maestro installation manual for the server's operating system. During installation select the Administration Hub when queried for which components to install. After installation, do not start LISTSERV Maestro.

For servers that already have the Maestro User Interface and/or the Tracker component installed, start the installation package for the server's operating system as if doing a fresh installation. The installation package will recognize any existing components and present an option to add new components. Select the Administration Hub component to add, and proceed with the installation. After installation, do not start LISTSERV Maestro.

Copy the following files and folders (including all files and subfolders) to the new server:

```
\Program Files\L-Soft\Application Server\hub\hub.ini
\Program Files\L-Soft\Application Server\hub\accountreg
\Program Files\L-Soft\Application Server\hub\hubreg
```

This will overwrite some files and folders on the new server. Depending on the installation, these paths may be slightly different on one or both of the servers.

Edit the following file of the Maestro User Interface component, which may be installed on a different server:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

In the file, edit the “RegistryHubHost” entry so that it contains the host name of the new server where the Administration Hub will be running.

Edit the following file of the Maestro Tracker component, which may also be installed on a different server:

```
\Program Files\L-Soft\Application Server\trk\tracker.ini
```

In the file edit the “RegistryHubHost” entry so that it contains the host name of the new server where the Administration Hub will be running.

On the old server, remove the previous installation of LISTERV Maestro.

For a server with Windows, use Windows' “Add/Remove Programs” panel to start the maintenance setup of LISTSERV Maestro. In the setup, choose “Modify” and deselect the Maestro User Interface component, so that it is uninstalled.

For a server with Linux, start the installation package the same way as if performing a fresh installation. The installation package will recognize the existing components. Select the Maestro User Interface component to be removed and proceed with the uninstallation.

Start LISTSERV Maestro on all servers

20.2.3 Moving the Maestro Tracker Component to Another Server

Moving the Maestro Tracker component to a different server must be well thought out and planned. The problem is that all messages that have been sent while the Maestro Tracker component was still installed on the old server include message tracking code with the old server name. If the Maestro Tracker component is shut down and de-installed on that old server, all tracking events from those messages will be lost.

Even worse, click-through tracking links will no longer work. If a recipient clicks on a click-through tracked link that is connected to the old Maestro Tracker component's host name, then the recipient will receive a “Host not found” or “Page not found” error – it will appear like a broken link – instead of being routed to the actual link target. Therefore be very careful when moving the Maestro Tracker component to a different server.

Under normal production conditions, this should never be done. But if necessary, move the component only if the last tracked e-mail job has occurred some time in the past and there is no more concern for tracking events that get lost and result in broken links. Of course changing the DNS registration of the host name can also solve this problem. For example, if the host name for the Maestro Tracker component was previously DNS-registered to point to the IP address of the old server, then change the registration and let it point to the address of the new server instead. To users accessing links this will appear as if there was no change at all. Keep in mind, however, that the propagation of a DNS change always takes a few days, so in the interim period, the averse effects of moving the component may still happen.

If it really becomes necessary to move the Maestro Tracker component follow these steps:

-
1. Shut down the LISTSERV Maestro installation on all servers where components are installed.
 2. For servers that have no existing LISTSERV Maestro components, execute a fresh installation as described in the LISTSERV Maestro installation manual for the server's operating system. During installation select the Maestro Tracker when queried for which components to install. After installation, do not start LISTSERV Maestro.

For servers that already have the Maestro User Interface and/or the Administration Hub component installed, start the installation package for the server's operating system as if doing a fresh installation. The installation package will recognize any existing components and present an option to add new components. Select the Maestro Tracker component to add, and proceed with the installation. After installation, do not start LISTSERV Maestro.

3. Copy the following files and folders (including all files and subfolders) to the new server:

```
\Program Files\L-Soft\Application Server\trk\tracker.ini
```

```
\Program Files\L-Soft\Application Server\trk\data
```

This will overwrite some files and folders on the new server. Depending on the installation, these paths may be slightly different on one or both of the servers.

4. Edit the following file of the Maestro User Interface component, which may be installed on a different server.

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

In the file edit the "TrackerHost" entry so that it contains the host name of the new server where Maestro Tracker will be running. If the DNS registration of the old host name also changed to point to the new server, then this is not a necessary change, since the actual host name is not changed – it only points to a different server.

5. On the old server, remove the previous installation of LISTSERV Maestro.

For a server with Windows, use Windows' "Add/Remove Programs" panel to start the maintenance setup of LISTSERV Maestro. In the setup, choose "Modify" and deselect the Maestro User Interface component, so that it is uninstalled.

For a server with Linux, start the installation package the same way as if performing a fresh installation. The installation package will recognize the existing components. Select the Maestro User Interface component to be removed and proceed with the uninstallation.

6. Start LISTSERV Maestro on all servers.

20.2.4 Moving the Database External Component to Another Server

Install the database software on the new server and start the program. Follow the instructions in Section 4.1 [Configuring the External System Database](#) with the exception that instead of moving from one type of database to a different one, move between two databases that are on different servers. These may actually be the same type of database (the database vendor, version, and such).

20.3 Server Name Aliases and Proxies

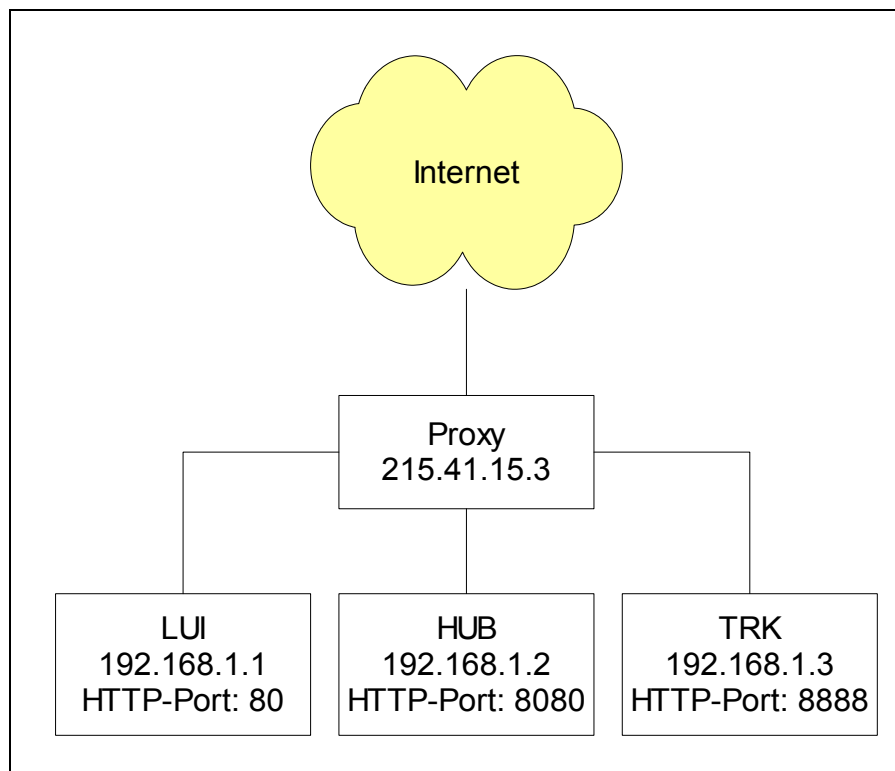
With any given installation of LISTSERV Maestro, the components of LISTSERV Maestro are installed on one or more servers, where each server has its own host name. Components on separate servers use the other server or servers' name(s) to access the component(s) there. Similarly, the "outside" world (users and e-mail messages that are being tracked) access the components with their server names as well.

In the simplest setup, each server hosting a LISTSERV Maestro component will have a DNS name that can be used both for the inter-component communication as well as for "outside" world access. In this case, setup is straightforward and no extra measures have to be taken.

However, there are configurations in which the host names of the LISTSERV Maestro component servers are names known only in the local network, with no DNS names assigned. Or the hosts are, for security reasons, not accessible directly from the outside. Instead, there is a proxy (or other kind of "forwarder") that sits between the local network and the outside world so that the outside only ever knows the host name (and IP address) of the proxy, but never the names and addresses of the servers behind it (which also may be addresses from a local range, like the 192.168.0.0 subnet).

Figure 61 shows such a setup, where only the proxy has a valid non-local IP address and a registered DNS name (or several names, see examples following the figure), while the LISTSERV Maestro servers have only local names and addresses.

Figure 61 Sample Proxy Setup



Example 1

Assume that the proxy shown in Figure 58 has a single DNS name “maestro.sample.com”. It could be configured to:

- Forward access on
maestro.sample.com:9001
to local host LUI (192.168.1.1), port 80
- Forward access on
maestro.sample.com:9002
to local host HUB (192.168.1.2), port 8080
- Forward access on
maestro.sample.com:9003
to local host TRK (192.168.1.3), port 8888

This example shows how a single DNS name can be “split” to proxy for three different servers, by employing different ports (9001-9003), which are mapped to different hosts (LUI, HUB, TRK) and their corresponding ports (80, 8080, 8888). Users wanting to access the Maestro User Interface would have to use a URL similar to: “http://maestro.sample.com:9001/lui”.

Users accessing the Administration Hub would use: “http://maestro.sample.com:9002/hub”

The tracking URLs would contain the URL `http://maestro.sample.com:9003/trk`

Example 2

As a second example, assume that the proxy has three assigned DNS names “lui.sample.com”, “hub.sample.com” and “trk.sample.com”, which are used to decide which local host to access, so the proxy could be configured to do the following:

- Forward access on
lui.sample.com:80
to local host LUI (192.168.1.1), port 80
- Forward access on
hub.sample.com:80
to local host HUB (192.168.1.2), port 8080
- Forward access on
trk.sample.com:80
to local host TRK (192.168.1.3), port 8888

In this example the “splitting” is realized by using three different host names, all assigned to the same server, where access on the standard HTTP-port 80 is mapped to the different local hosts (LUI, HUB, TRK) and their corresponding ports (80, 8080, 8888) depending on the DNS name used to access the proxy. Users wanting to access the Maestro User Interface would have to use a URL like “http://lui.sample.com/lui”. Users accessing the Administration Hub would use “http://hub.sample.com/hub” and the tracking URLs would contain the URL “http://trk.sample.com/trk”.

The example demonstrates that the host names of the servers hosting the LISTSERV Maestro components may differ when viewed locally or from the “outside” world. Internally, the LISTSERV Maestro components always use the local names to communicate. When setting host names in INI files (or during the setup), use the names that are locally valid (which can also be externally valid names, only if the names work for local access too). Whenever the local names are different from the external names (usually because some sort of proxying or forwarding is involved), the administrator needs to perform some additional configuration steps to make LISTSERV Maestro aware of the differences.

20.3.1 Configuring LISTSERV Maestro components with Server Name Aliases or Proxies

If the local name or HTTP port of a host differs from the externally known name or port the following files must be edited:

- If the **Maestro User Interface** component’s server has a local host name or port that is different from the external name, edit the file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Add or edit the entry “ExternalHostName” to read

```
“ExternalHostName=HOST:PORT”
```

where “HOST” is replaced with the external name of the server running the Maestro User Interface component and “PORT” with its external HTTP port (if the external HTTP port is the default “80”, leave out “:PORT” and only write “ExternalHostName=HOST”).

- If the **Administration Hub** component’s server has a local host name or port that is different from the external name, edit the file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Add or edit the entry “ExternalHubHostName” to read:

```
“ExternalHubHostName=HOST:PORT”
```

where “HOST” is replaced with the external host name of the server running the Administration Hub component and “PORT” with its external HTTP port (if the external HTTP port is the default “80”, leave out “:PORT” and only write “ExternalHubHostName=HOST”).



Important: This entry has to go into the “lui.ini”, not into the “hub.ini”.

- If the **Maestro Tracker** component’s server has a local host name or port that is different from the external name, set the external host name and/or port in the “Tracking URL” settings in the Administration Hub. Please see Section 7.1 [Setting the Default Tracking URL](#) for more details.

To actualize the examples above, the following changes to the administration settings would have to be made:

For **Example 1**, two `lui.ini` entries are required:

```
ExternalHostName=maestro.sample.com:9001
```

```
ExternalHubHostName=maestro.sample.com:9002
```

Also, the Administration Hub would be used to configure the tracking URL to use a “Tracker Host” of “maestro.sample.com” and a “HTTP Port” of “9003”.

For **Example 2**, two `lui.ini` entries are required:

```
ExternalHostName=lui.sample.com
```

```
ExternalHubHostName=hub.sample.com
```

Also, the Administration Hub would be used to configure the tracking URL to use a “Tracker Host” of “trk.sample.com” and a “HTTP Port” of “80”. Next, it would be necessary to configure the proxy accordingly, so that it transparently forwards the requests as described above – but this depends on the proxy software used and is not part of the LISTSERV® Maestro setup.

Section 21 User Interface Branding

The Maestro User Interface and the Administration Hub components permit limited user interface branding by allowing the administrator the choice of using institutional or company logo images instead of the LISTSERV® Maestro logos, and by adding a few text strings at prominent locations, like in the header and footer of each page.

To do this, the administrator must create a text file called “`custom.properties`” that must be located in the folder

```
\Program Files\L-Soft\Application Server\lui
```

to customize the Maestro User Interface component and/or

```
\Program Files\L-Soft\Application Server\hub
```

to customize the Administration Hub component.

This file must be a text file that follows the rules of LISTSERV Maestro INI files (see Section 19 [Editing LISTSERV Maestro INI Files](#) for more information). This means that the file must consist of entries of the form “`key=value`”, with which the administrator can define customized text strings or point to customized logo image files.

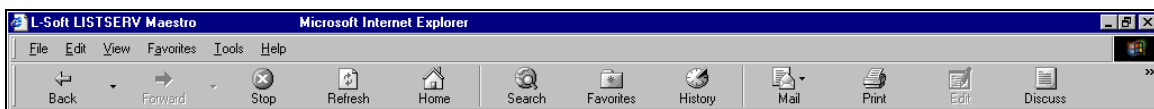
21.1 Adding Custom Text Strings

Each custom text string consists of a “key=value” pair, where the key is as listed below, and the value is the text that is supposed to appear in the user interface (and follows the INI file rules). The following text string keys are currently available for customization:

- `app.title.companyName=YOUR_TEXT`

Sets “YOUR_TEXT” to be used in the window title bar of each browser window that is used to access the Maestro User Interface or the Administration Hub component. The text will appear as the first text in the title bar, before the application name. If this key is not included, the text “L-Soft” will be shown. Supply an empty value “`app.title.companyName=`” to not show any text before the application name.

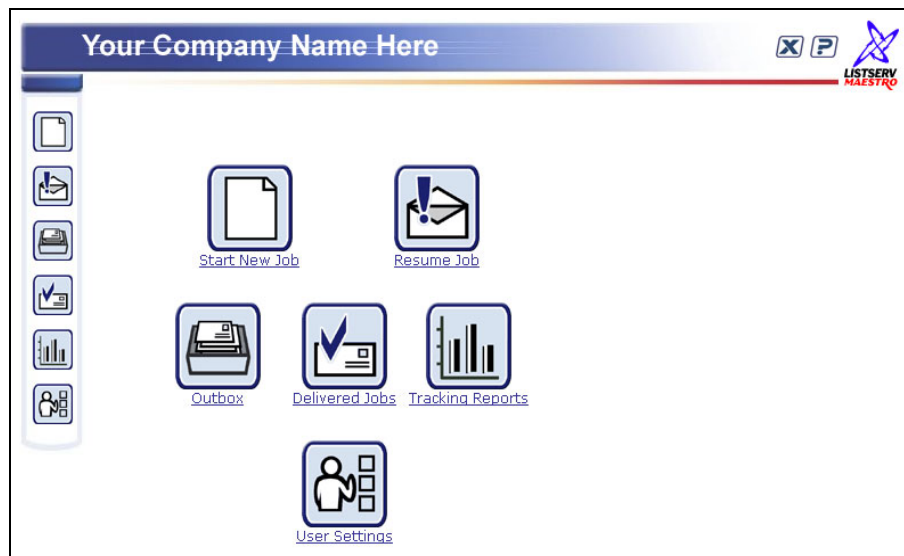
Figure 62 Browser Window Branding



- `app.msg.headerText=YOUR_TEXT`

Adds “YOUR_TEXT” as a header text at the top of the page. The header text will be drawn so that it will appear on top of the blue header bar that is shown at the top of each page so that the blue header bar will be the background behind the text, which is drawn with a white, bold faced font, about as large as the page headers that appear on each page right below the header bar. If this key is not included, no text will be shown.

Figure 63 LISTSERV Maestro Header Branding



- `app.msg.footerText=YOUR_TEXT`

Adds “YOUR_TEXT” as a footer text at the bottom of the page. The footer text will be drawn in the bottom left corner of each page where it will appear to the left of the “Protected by F-Secure” message (in the Maestro User Interface). It will be drawn in the

same small standard page font as the F-Secure message. If this key is not included, no text will be shown.

Figure 64 LISTSERV Maestro Footer Branding



- `app.url.companyURL=YOUR_URL`

Uses “YOUR_URL” (must be a valid “http://...” URL) as the target link of the logo that appears at the top-right of each page. This logo is set to the LISTSERV Maestro logo with a target URL of “http://www.lsoft.com”. Customizing the logo’s target URL is the most effective when used together with exchanging the LISTSERV Maestro logo with a customized institutional or company logo (see below). If this key is not included the URL will point to “http://www.lsoft.com”.

21.2 Exchanging Logo Images

In order to replace the LISTSERV Maestro logo image files, prepare the customized image files and save them in either GIF or JPG format. There are size restrictions for the files, which are detailed below. Create a folder named “custom” in the directories below. Save the image files in these “custom” folders so that the files are accessible to LISTSERV Maestro and so that the files will not be changed or deleted by LISTSERV Maestro’s upgrade routine (although the folders may be deleted during a full de-installation of LISTSERV Maestro).

For the Maestro User Interface component, create a “custom” folder so that the path to save the image files reads:

```
\Program Files\L-Soft\Application Server\webapps\lui\custom
```

For the Administration Hub component, a “custom” folder so that the path to save the image files reads:

```
\Program Files\L-Soft\Application Server\webapps\hub\custom
```

Storing image files anywhere else will either have the effect that LISTSERV Maestro will not be able to find them, or they may be lost during an upgrade.

Once the images are saved in the “custom” folder, LISTSERV Maestro needs to know about them. Do so with the same sort of “key=value” entries in the “custom.properties” file(s) as described above. Each key’s value must be a relative filename starting with a forward slash “/” and including the name of the “custom” folder itself as the first path element, using the forward slash as the separator (not backslash).

For example: “/custom/myImage.gif”.

The following image file keys are currently available:

- `app.img.titleBarLogo=/custom/FILENAME`

Uses the image file with the name “FILENAME” from the “custom” folder to replace the LISTSERV Maestro logo image that is shown at the right of the header bar that appears at the top of each page. This logo is also a clickable link that may be customized. Set the target URL with the “app.url.companyURL” key (see above). This image must be 60 x 60 pixels in size. If this key is not included, the LISTSERV® Maestro logo will be used.

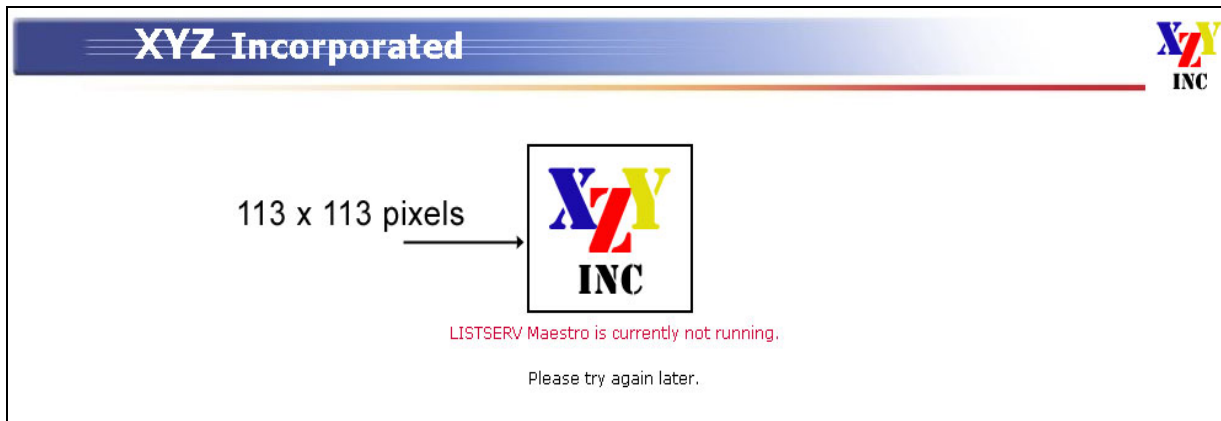
Figure 65 Right Logo Branding



- `app.img.appLogo=/custom/FILENAME`

Uses the file with the name “FILENAME” from the “custom” folder to replace the LISTSERV Maestro logo image that is shown on the login page when the Maestro User Interface or Administration Hub is not accessible: Under normal conditions, the login page only shows the image in the header bar, plus the edit fields for the login. However, if the Maestro User Interface or Administration Hub is locked by the administrator or is for other reasons not correctly running, the login page displays this logo and a short message text, instead of the login edit fields. This logo image should be about 113 x 113 pixels in size, but the size may vary (within reasonable limits). If you do not include this key, a version of the LISTSERV Maestro logo will be used.

Figure 66 Error Screen Logo Branding



Section 22 LISTSERV Maestro in Evaluation Mode

In order to function in normal mode, LISTSERV Maestro needs to be connected to a fully licensed instance of LISTSERV. LISTSERV Maestro connects to the configured LISTSERV instance to check if there is a MAESTRO scope and a suitably recent maintenance license in the LISTSERV license key (LAK). A “suitably recent” maintenance key is one that expires after the release date of the given LISTSERV Maestro version. If not, then LISTSERV Maestro will run in evaluation mode for all users and groups that are configured to use this LISTSERV instance.

In evaluation mode, actual delivery of a job is only simulated. When the scheduled send time of an authorized job has been reached, the job is transferred into the “delivered” state without actually sending any messages to any recipients. Operating in this fashion, a user can evaluate

all aspects of LISTSERV Maestro, including job definition, authorization, and viewing delivered jobs, without actually being able to use LISTSERV Maestro for real deliveries.

Test delivery, which is a workflow step that precedes the authorization step, is possible even in evaluation mode. However, with the restriction that an evaluation message is added to the top of all messages that are sent during test delivery with LISTSERV Maestro in evaluation mode.

In addition, for test delivery in evaluation mode to function, the following condition must be fulfilled: Either LISTSERV's SMTP listener or an instance of LSMTP that is connected to LISTSERV must be installed on the same server that the LISTSERV instance used for delivery is running on. And, this SMTP listener/LSMTP must be listening for STMP requests on the standard SMTP port 25.

Section 23 Using International Character Sets

Each e-mail job that is created in LISTSERV Maestro has a character set (charset) associated with its content. This charset is used to encode the content for sending. When a job is first created as a new job (not as a copy of an existing job), the job is initially created with the default charset. LISTSERV Maestro defaults to the ISO-8859-1 (Latin 1) character set for encoding e-mail messages unless the administrator has defined a different default setting.

23.1 Defining the Default Mail Charset

To define the default charset, edit the following in the Maestro User Interface INI-file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit or add the key "DefaultMailCharset" and set it to the name of one of the charsets supported by LISTSERV Maestro.

Table 6 Supported Charsets

Charset Name:	Description:
US-ASCII	US ASCII
ISO-8859-1	West European, Latin 1
ISO-8859-2	East European, Latin 2
ISO-8859-3	South European, Latin 3
ISO-8859-4	North European, Latin 4
ISO-8859-5	Cyrillic
ISO-8859-6	Arabic
ISO-8859-7	Greek
ISO-8859-8	Hebrew
ISO-8859-9	Turkish, Latin 5
ISO-8859-15	Similar as ISO-8859-1 but with Euro currency symbol
UTF-8	International Unicode, encoded in UTF-8 format
AUTO-NO-UTF-8	LISTSERV Maestro will choose either US-ASCII or any of the ISO-8859 charsets (but <u>not</u> UTF-8), depending on the characters that are actually used in the content. If possible, ASCII is favored over any ISO-8859, so an ISO-8859 set is only chosen if ASCII is not able to display all characters in

Charset Name:	Description:
	<p>the content.</p> <p>Of the ISO-8859 sets, the one where the number of non-displayable characters is minimized is chosen. If two sets have an equal number of non-displayable characters, then lower ISO-8859 sets are favored over higher sets (for example, ISO-8859-1 over ISO-8859-2, over ISO-8859-3, and so on).</p>
<p>AUTO-YES- UTF-8</p>	<p>LISTSERV Maestro will choose either US-ASCII or any of the ISO-8859 or even UTF-8, depending on the characters that are actually used in the content. If possible, ASCII is favored over any ISO-8859 and the ISO-8859 sets are favored over UTF-8.</p> <p>The step to the next “higher” set is only made if the “lower” set is not able to display all characters in the content. If several ISO-8859 sets are able to display all characters, then lower ISO-8859 sets are favored over higher sets (for example ISO-8859-1 over ISO-8859-2, over ISO-8859-3, and so on.).</p>

The default charset is only initially assigned to the e-mail job. It may be changed by the user on the content definition page.

If the administrator wants to prevent the users from changing the default charset (and force the users to always accept the default charset already set), another entry in the same INI-file needs to be edited:

Edit or add the key “AllowCharsetChoice”. Set to “true” to allow the users to change the charset of a job (to be able to assign different charsets to each job) or to “false” to disallow changing of the charset. The default if the key is not present in the INI-file is “true.”

23.2 Allowing or Disallowing Bi-Directional Character Sets

Of the ISO-8859 charset family, there are two charsets that contain letters from languages that have a standard reading direction of right-to-left. These are the charsets ISO-8859-6 (Arabic) and ISO8-859-8 (Hebrew), both of which are supported by LISTSERV Maestro.

Actually, LISTSERV Maestro will not use the charsets with the names ISO-8859-6 and ISO-8859-8 when it recognizes Arabic or Hebrew characters, but will instead use the special bi-directional versions ISO-8859-6-i and ISO-8859-8-i. These charsets contain the same characters as their non-i-suffix counterparts, but the “-i” suffix tells the receiving mail client that the text should be displayed with right-to-left reading direction. Without the “-i” suffix in the charset name, many e-mail clients would probably display the correct characters, but in the (for that language) incorrect left-to-right reading direction.

Even with the "-i" suffix, the recipient might need a special mail client version (or even a special mail client) that is prepared to display text with right-to-left reading direction properly and is also able to properly display bi-directional text (text that mixes characters with left-to-right and characters with right-to-left reading direction, in the case of a Hebrew text that contains English names, for example). Some clients may only display the characters with the right direction, but still left-align each line of text, instead of the correct right-alignment (occurrences such as this are subject to the mail client itself, and are outside of the scope of LISTSERV Maestro).

It is possible, however, to disallow the charsets with the "-i" suffix and use the "normal" counterparts, ISO-8859-6 and ISO-8859-8 instead. To do so, edit the following file:

```
\Program Files\L-Soft\Application Server\lui\lui.ini
```

Edit or add the key "AllowISO-i-Mails=false" to disallow the bi-directional charsets. (If the key from the INI-file is removed, commented out, or set to "...=true", then the bi-directional charsets will be allowed as is the default).

This INI-file setting will affect all mail sent, with any user account. Please note that changing this setting requires a restart of the Maestro User Interface component to take effect.

Glossary of Terms

Administration Hub (HUB) – A component of the LISTSERV Maestro program that allows the administrator to create user accounts, and assign and change settings for the entire application.

Click-Through Event – A trackable occurrence available with text and HTML e-mail messages that records each time a URL contained in the message is clicked.

Column – A vertical set of data, as in a table or spreadsheet.

Database – A large collection of data organized with inter-related data tables for rapid search and retrieval, managed as an entity by a DBMS.

Database Plugin – A feature that allows LISTSERV Maestro to connect to a driver for a particular DBMS.

Database Server – A single server running a DBMS to manage one or more databases.

DBMS – Database Management System: a software product for the management of databases. Examples are: DB2, MySQL, Oracle, SQL Server.

Delimiter – The character or symbol that is used to separate one item from another. In text files imported into databases, commas are often used as delimiters. A delimiter is the same as a separator character.

Driver – A program installed on a workstation or server to allow programs on that system to interact with a DBMS.

E-mail Merge – Placing variables that are extracted from a database into an e-mail message template. This operation permits individual personalization of otherwise bulk e-mail messages.

Encoding – Is the transformation of data into digital form. With text encoding, different character sets encode text files differently based on language and other variables. If a special character set was used to encode a text file, that same encoding scheme needs to be used to interpret the data correctly. LISTSERV® Maestro allows for the selection of encoding based upon the original encoding scheme of the uploaded text file. For example, if special encoding was used to initially create (and save) the text file (e.g. ISO-7 encoding for a file with Greek characters, or a Unicode encoding), the same encoding will have to be selected in LISTSERV® Maestro so that the system interprets the uploaded data in the same way it was saved.

Header – A special row of data that defines and labels the columns in a text file.

Maestro Tracker (TRK) – A component of the LISTSERV Maestro program that receives and compiles tracking data from delivered e-mail messages.

Maestro User Interface (LUI) – A component of the LISTSERV Maestro program that allows regular users to create e-mail jobs and tracking reports.

Open-Up Event – A trackable occurrence available with HTML e-mail messages that records each time a message is opened by a recipient.

Quote character – In a SQL statement: a character (usually the single quote) used to enclose string literals, to set them off from the rest of the SQL statement.

In a text file (CSV-file) containing data: a character or symbol used to surround the value of a column if the value contains the separator character in the actual data. This is necessary to ensure that the appearance of the separator character in the data is not interpreted as an actual separation. For example, if a comma (,) is used as the separator character in a database file, all the fields of data are separated by a comma. If the comma is also used within a field, the quote character must be used to surround the entire field. If the quote character is used in a field, it must be used twice, or “escaped.”

Select Statement – A SQL statement in form of a query that is issued to a database to retrieve data.

Separator Character – A character or symbol used to separate one item from another. In text files exported from databases, commas are often used as separator characters. A separator character is the same as a delimiter.

SQL – Abbreviation of Structured Query Language. SQL is a standardized query language for requesting information from a database.

SQL Statement – A statement written in SQL that is issued to a database to retrieve data or to create, insert, update, or delete data in the database.

Appendix A LISTSERV Maestro Standard Default Ports

Ports Used by the Administrative Hub

Port Number	Function
80	HTTP access
1099	Internal communication with other LISTSERV Maestro Components
8007	Shut down of the application server

Ports Used by the Maestro User Interface

Port Number	Function
80	HTTP access
1099	Internal communication with other LISTSERV Maestro components
8007	Shut down of the application server
3306	Internal system database connection (Windows only)

Ports Used by Maestro Tracker

Port Number	Function
80	HTTP access
1099	Internal communication with other LISTSERV Maestro components
7000	Communications Port transfers tracking data to the Maestro User Interface
8007	Shut down of the application server

This page intentionally left blank.