



LISTSERV Maestro Admin Tech Doc 7

Installing Behind a Firewall or Proxy

September 29, 2021 | © L-Soft Sweden AB
lsoft.com



This document is a LISTSERV Maestro Admin Tech Doc. Each admin tech doc documents a certain facet of the LISTSERV Maestro administration on a technical level. This document is number 7 of the collection of admin tech docs and explains the topic "Installing Behind a Firewall or Proxy".

Last updated for LISTSERV Maestro 10.0-1 on September 29, 2021. The information in this document also applies to later LISTSERV Maestro versions, unless a newer version of the document supersedes it.

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 Sweden AB 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 part of the document for the purposes of this copyright notice, and can be freely removed if present.

Copyright © 2003-2021, L-Soft Sweden AB
All Rights Reserved Worldwide.

LISTSERV is a registered trademark licensed to L-Soft international, Inc.

L-SOFT and LMail are trademarks of L-Soft international, Inc.

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

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

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

This product includes code licensed from RSA Security, Inc.

This product includes software developed by the Apache Software Foundation
(<http://www.apache.org/>).

All of L-Soft's manuals are also available at: <http://www.lsoft.com/manuals.html>

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

Table of Contents

1 Installing Behind a Firewall.....	1
2 Setup with Server Name Aliases / Proxy Setup	3

1 Installing Behind a Firewall

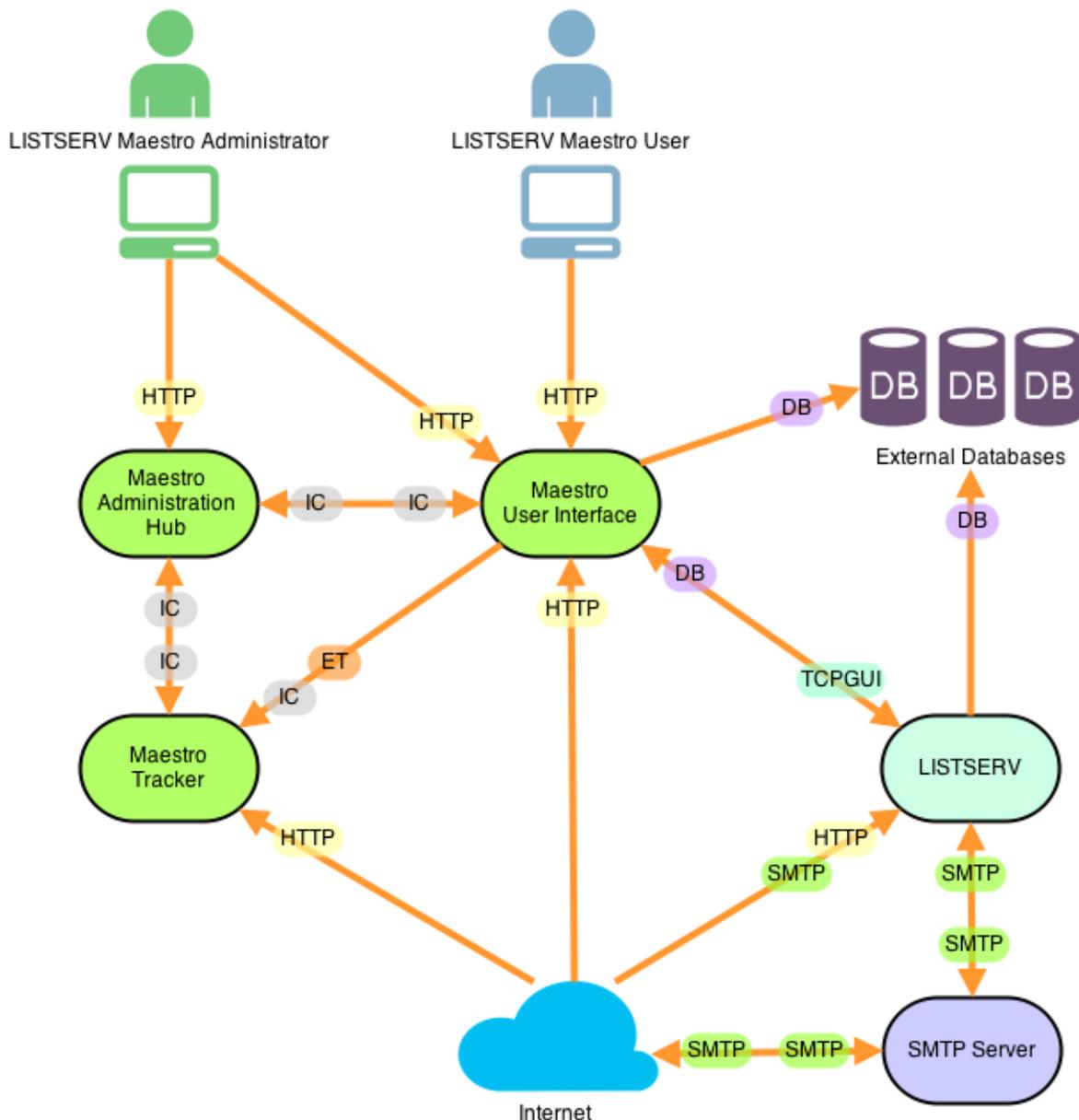
Any network that is connected to the internet usually is protected by some form of firewall, often in conjunction with different kinds of “demilitarized zones” and other security measures.

If you want 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, you need to take into account the communication channels between the separate components.

Communication happens exclusively via ports (see also “LMA Admin Tech Doc 6 – IP Addresses and Ports”).

So if you install the components behind, in front of, or around a firewall, you need to configure the firewall to let through communication on certain ports between certain servers.

The following figure shows the LISTSERV Maestro components and all other players (like the Maestro Administrator and Maestro User, or the Internet, which stands for the set of mails sent to their recipients) and their interconnections:



The arrows between the components indicate the direction of communication and the bubbles at the arrow heads indicate the port that is used for this communication. Note, that sometimes the communication goes in both directions (requiring an open port on both sides) and sometimes it only goes in one direction.

The port labels have the following meaning:

- **HTTP:** Used for standard HTTP access, via a web-browser. This is also used to transfer the tracking events from the internet (e.g. from the mails that were sent) to the Maestro Tracker component.

The standard HTTP-Port is **80**.

If you are using HTTPS access to the Administration Hub and/or the Maestro User Interface component (see "LMA Admin Tech Doc 9 - Securing Access with HTTPS"), then you should substitute 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 with the **HTTPS** port, for which the standard is **443**.

- **SMTP:** Used for standard SMTP communication, during the sending and receiving of mails.

The standard SMTP-Port is **25**.

- **IC (Internal Communication Port):** Used for communication between the separate LISTSERV Maestro components.

The standard Internal Communication Port is **1099**.

- **ET: (Event Transfer 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.

The standard Event Transfer Port is **7000**.

- **TCPGUI:** Used by the Maestro User Interface component to access the LISTSERV component.

The standard TCPGUI Port is **2306**.

- **DB:** Used by the Maestro User Interface and/or LISTSERV component to access the external database component (if used) and/or by the LISTSERV component to access the internal system database on the Maestro User Interface server (if used).

The standard database port depends on the database you use.

(See also "LMA Admin Tech Doc 6 – IP Addresses and Ports" for more information about the ports).

All the nodes shown in the diagram (except for the "Internet" and "Maestro Admin" and "Maestro User", of course) may reside on a single server, or may be distributed over different servers, up to the maximum distribution of having a dedicated server for each of the components shown (see also "LMA Admin Tech Doc 5 – Multi Server Installation").

Whenever two components are installed on the same server, you do not have to worry about a firewall stopping the communication between the two (except of course, if you have a firewall 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, than you may have to deal with a firewall sitting between the two. Most commonly you will for example have a firewall separating the

“Internet” from the other components, but also the other components may be installed in a way, that they have a firewall between them.

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

If that is the case, then you must configure the firewall so, that it lets through communication between the two components, as specified by the arrow associated with the connection the firewall guards: The direction of the arrow shows you in which direction you have to open the port, and the label of the arrow tells you which port you need to open (see port list above).

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

For example, if you have a firewall between the Maestro Tracker and the Maestro User Interface component, then you should open the “Event Transfer Port” and the “Internal Communication Port” **only** in the direction from the Maestro User Interface host to the Maestro Tracker host, and both **only** for the involved IP address. Thus you limit possible security breaches in case any unauthorized person gains access to one of the component servers.

If you have a firewall that separates the Internet from the other components (as is advisable), then you need to open the HTTP and SMTP ports from the internet to the respective components as shown in the diagram, and you need to open them for all incoming IP-addresses, not only for a specific one. And of course you need to open the SMTP port for outgoing communication originating from the LISTSERV and SMTP servers.

You do not have to worry about letting the Application Server Shutdown Port [default: 8007] through the firewall, since this port is only ever used locally for communication between two processes on the same server. Of course, if you have installed a firewall on the server itself, then you might have to open this port too. Simply check if the “L-Soft Tomcat” server still reacts to the “Stop” command. If not, then you need to open the port.

2 Setup with Server Name Aliases / Proxy Setup

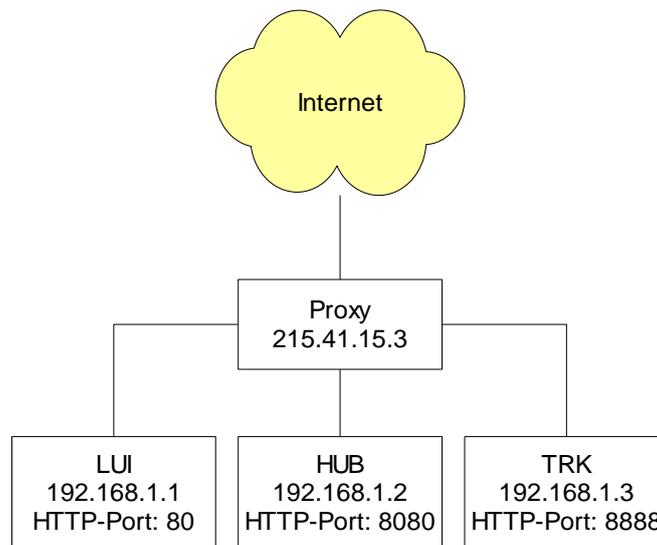
In any given installation of LISTSERV Maestro, the components of LISTSERV Maestro will be installed on one or more servers, where each server has its own host name. Components on separate servers use the other server’s name to access the component(s) there.

Similarly, the “outside” world (e.g. users as well as mails that are tracked) access the components with their server names too.

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 the “outside” world access. In this case, setup is quite forward 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 only known in the local network, with no DNS names assigned. Or the hosts are, for security reasons, not supposed to be accessed directly from the outside and instead there is a proxy (or other kind of “forwarder”) which sits between the local network and the outside world in a way, 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).

The following figure 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 below), while the LISTSERV Maestro servers have only local names and addresses.



Example 1:

We assume that the proxy shown in the figure has a single DNS-name “maestro.sample.com”. So 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 like “`http://maestro.sample.com:9001/loi`”.

Users accessing the Administration Hub would use “`http://maestro.sample.com:9002/hub`”.

And the tracking URLs would contain the URL “`http://maestro.sample.com:9003/trk`”.

Example 2:

As a second example, we assume that the proxy has three DNS names “`lui.sample.com`”, “`hub.sample.com`” and “`trk.sample.com`” assigned, 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”.

When looking at the example, it becomes obvious 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. E.g. when setting host names in INI-files (or during the setup), you should use the names that are locally valid (which can of course also be externally valid names, if only the names work for local access too).

Whenever the local names are different from the external names (usually because some sort of proxy or forwarding is involved), the administrator needs to perform some additional configuration steps to make LISTSERV Maestro aware of the differences, as described on the following pages.

The following list describes what to do if the host name, protocol or HTTP-port as used by external clients differs from the default values:

- External **host name** or **protocol** or **port** of the **Maestro User Interface (LUI)**:

The default host name is the value of the “HostName” setting in the `lui.ini`, or, if not present, the canonical host name of the server running the Maestro User Interface component. The default protocol is HTTP. The default port is “80” for HTTP and “443” for HTTPS.

If **any** of these values as used by external clients is different than these defaults, then you have to edit the “LUI Access URL for Users” setting in the Administration Hub, to reflect this.

This may affect the “Default LUI Access URL for Users” under **Main Menu → LUI Settings → Application Default Settings → URL Settings** and/or the individual “LUI Access URL for Users” setting on group or user level.

You may also have to change the “LUI Access URL for Admin” setting (on default level) and/or the “URL for Recipients, Subscribers and Others” setting (on group or user level), if these settings do not inherit the “LUI Access URL for Users” setting.

Additionally, you need to configure the protocol, host and port that the *proxy* uses to access the Maestro User Interface in the `lui.ini`, with the following setting:

```
AccessURLBehindProxy=PROTOCOL://HOST:PORT
```

- External **host name** or **protocol** or **port** of the **Administration Hub (HUB)**:

The default host name is the value of the “HostName” setting in the `hub.ini`, or, if not present, the canonical host name of the server running the Administration Hub component. The default protocol is HTTP. The default port is “80” for HTTP and “443” for HTTPS.

If **any** of these values as used by external clients is different than these defaults, then you have to edit the “HUB Access URL for Admin” setting in the Administration Hub, to reflect this.

See “HUB Access URL for Admin” under **Main Menu → LUI Settings → Application Default Settings → URL Settings**.

- External **host name** or **protocol** or **port** of **Maestro Tracker (TRK)**:

The default host name is the value of the “HostName” setting in the `tracker.ini`, or, if not present, the canonical host name of the server running the Maestro Tracker component. The default protocol is HTTP. The default port is “80” for HTTP and “443” for HTTPS.

If **any** of these values as used by external clients is different than these defaults, then you have to edit the “Tracking URL” setting in the Administration Hub, to reflect this.

This may affect the “Default Tracking URL” under **Main Menu → LUI Settings → Application Default Settings → URL Settings** and/or the individual “Tracking URL” setting on group or user level.

If we wanted to implement the two examples of above, we would have to make the following administration settings (assuming that we configure this as application defaults in the HUB):

For Example 1, we would have to supply the following URL Settings:

Default LUI Access URL for Users:	<code>http://maestro.sample.com:9001</code>
Default HUB Access URL for Admin:	<code>http://maestro.sample.com:9002</code>
Default Tracking URL:	<code>http://maestro.sample.com:9003</code>
In <code>lui.ini</code> :	<code>AccessURLBehindProxy=http://192.168.1.1</code>

For Example 2, we would have to supply the following URL Settings:

Default LUI Access URL for Users:	<code>http://lui.sample.com</code>
Default HUB Access URL for Admin:	<code>http://hub.sample.com</code>
Default Tracking URL:	<code>http://trk.sample.com</code>
In <code>lui.ini</code> :	<code>AccessURLBehindProxy=http://192.168.1.1</code>

(And then of course we would also have to configure the proxy accordingly, so that it indeed does the transparent forwarding of the requests as described above – but this depends on the proxy software used and is not part of the LISTSERV Maestro setup.)